ERRORES HUMANOS LATENTES: LA ESTRATEGIA DIRECTIVA Y SU CAUSALIDAD EN LOS ACCIDENTES GRAVES

JAMES REASON

Cátedra de Psicología. Universidad de Manchester

El presente artículo es la traducción de la comunicación presentada por el autor en el Seminario sobre Riesgo y Sociedad, organizado por la Asociación de Ginebra y celebrado en Londres (Inglaterra) en enero del presente año.

La tecnificación de procesos complejos produce el efecto de separar dichos procesos del ser humano. Cada vez es más difícil un control directo sobre los sistemas o procesos tecnológicos. Un alto porcentaje de accidentes graves se produce por fallos humanos «latentes», es decir, por acciones no directas sobre la instalación o sistema fallido. El autor plantea una reflexión sobre esta importante paradoja, presente en muchos accidentes que, por su importancia, han sido actualidad mundial.

A la hora de considerar la contribución humana a la causalidad de los accidentes catastróficos en los sistemas tecnológicos, cabe distinguir dos tipos de errores: los activos, cuyos efectos se evidencian prácticamente de inmediato; y los latentes, cuyas consecuencias adversas pueden permanecer ocultas durante cierto tiempo, manifestándose únicamente al combinarse con otros factores para agredir las defensas del sistema (cfr. RASMUSSEN y PEDERSEN, 1984). En general, los errores activos se asocian con la actividad de operadores de «primera línea de explotación de un sistema»: pilotos, oficiales de buques, controladores aéreos, etc. Por el contrario, los errores latentes subyacen normalmente a actividades disociadas (tanto espacial como temporalmente) de la labor directa de control: ingenieros de diseño, operarios y técnicos, personal de mantenimiento y directivos.

Los errores latentes entrañan la mayor amenaza para la seguridad de un sistema complejo.

El análisis detallado de algunos accidentes recientemente acaecidos (y reflejados posteriormente en este artículo) evidencia significativamente el hecho de que los errores latentes entrañan la mayor amenaza para la seguridad de un sistema complejo. Hasta ahora, los análisis de fiabilidad y las investigaciones sobre accidentes tendían a centrar su atención en los errores de los operadores y en los fallos de los equipos. Si bien es cierto que los operadores pueden (y suelen) cometer errores al intentar recuperar situaciones no toleradas por un cierto sistema, también es cierto que la mayoría de las causas que subyacen a la emergencia se encontraban ya en el sistema mucho antes de que estos errores activos fuesen cometidos.

El papel de los operadores, más que el de principales causantes de un accidente, es el de heredar las taras del sistema causadas por la baja calidad del diseño, defectos de instalación, escasa competencia de los técnicos de mantenimiento y arbitrariedad en las decisiones de la dirección. Los operadores son —en realidad— el condimento final a un guiso que llevaba largo tiempo ya cocinándose.

Existe una creencia cada vez más firme, entre los investigadores del tema (cfr. BATSTONE, 1987; RASMUSSEN, 1988), de que los intentos por descubrir y neutralizar estos errores latentes incrementarían la seguridad del sistema por encima de las cotas alcanzables mediante esfuerzos individuales por minimizar los errores activos. Hasta la fecha, el trabajo de los especialistas en factores humanos se ha dirigido fundamentalmente a la mejora del punto de encuentro entre el sistema y el operador (la interfaz hombre-sistema, es decir, la sala de la torre de control o la cabina de los pilotos). Sin negar la trascendencia de estas investigaciones, es preciso recordar que se restringen a una pequeña parte del problema de la seguridad total, al estar enfocadas a reducir el «error activo» (que apenas representa la punta del iceberg de la causalidad). La experiencia de los pasados años enseña que, en materia de seguridad, el término «factores humanos» abarca un espectro de individuos y actividades mucho más amplio que el conjunto de personas en «primera línea de explotación» de un sistema. De hecho, uno de los temas centrales de este artículo es que cuanto más alejados están los individuos de estas actividades de primera línea (e, incidentalmente, de los riesgos directos), mayor es su peligro potencial para el sistema.

Existen también intentos típicamente «reactivos» por minimizar errores: se pretende en estos casos eliminar la recurrencia de determinados fallos activos identificados a posteriori por los investigadores de accidentes. De manera similar, si bien es conveniente aprender lo máximo posible acerca de los accidentes ocurridos en el pasado, también debe considerarse que tales sucesos suelen ser provocados por una conjunción singular de diversos factores necesarios, pero por sí solos insuficientes. Si se tiene en cuenta la improbabilidad de que tal combinación de causas vuelva a repetirse, los esfuerzos por evitar que se produzcan dichos errores activos apenas influirán en la seguridad total del sistema. En el peor de los casos, la inutilidad del esfuerzo es equiparable a la de encontrar el mejor método de asegurar la puerta de un establo cuyo caballo ya se ha escapado.

En este artículo se considera la contribución de los errores latentes al fallo catastrófico de una serie de sistemas complejos. Puesto que la noción de error latente está íntimamente ligada a la idiosincrasia de la tecnología contemporánea, comenzaré por describir brevemente algunas de las modificaciones más significativas introducidas durante las últimas décadas en el control de los sistemas de alto riesgo.

1. DESARROLLOS TECNOLOGICOS

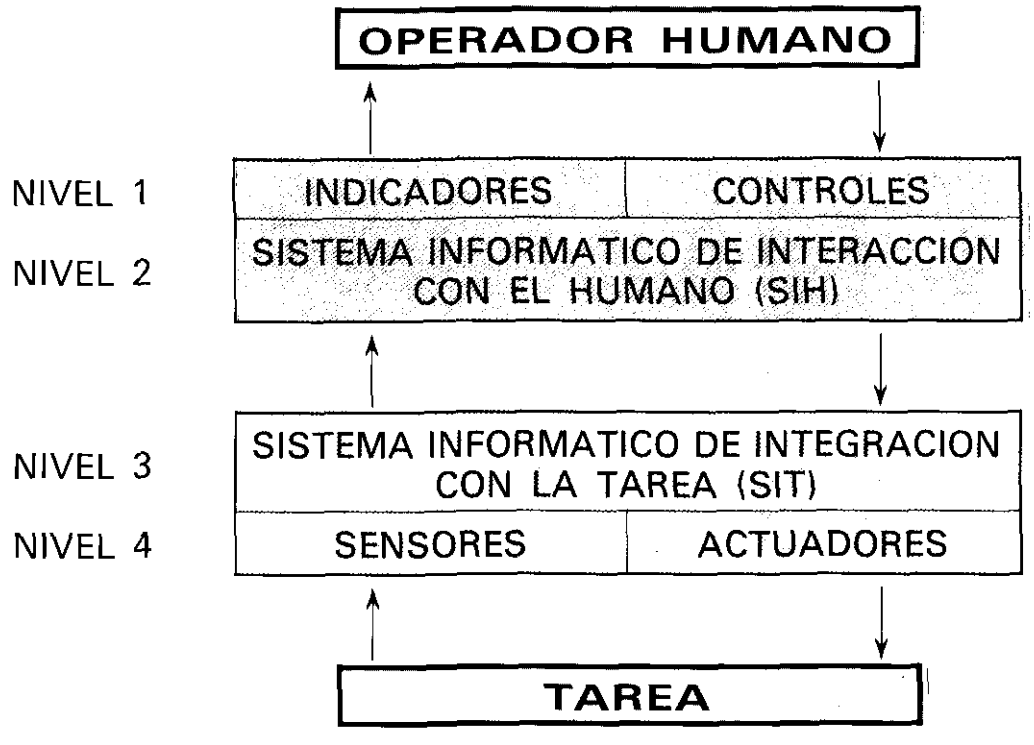
Los últimos 30 ó 40 años han sido testigos de una auténtica revolución tecnológica en el di-

seño y control de los sistemas de alto riesgo. A su vez, esta revolución ha desatado cambios radicales (y todavía poco comprendidos) en las tareas destinadas a los humanos.

1.1. Los sistemas están cada vez más automatizados

Uno de los adelantos más significativos de los últimos años ha sido la separación física entre los operadores (las personas situadas en el interfaz hombre-sistema) y los procesos sobre los que ejercen su control. Se han introducido máquinas de creciente complejidad que intervienen entre el humano y la tarea física.

Al principio, los operadores empleaban métodos directos de actuación y captación: veían y tocaban lo que producían o controlaban. Después llegaron los dispositivos de actuación y control remotos, que se introdujeron cuando el proceso resultaba demasido peligroso o demasiado sensible para ser tratado directamente, cuando resultaba necesario superar la potencia del músculo humano, o cuando los sentidos del operador resultaban incapaces de detectar ciertos cambios físicos significativos.



Elementos básicos del control de supervisión (MORAY, 1986)

Pero los cambios más profundos llegaron con el advenimiento de la potencia informática a bajo precio. Ahora, el operador puede ser separado del proceso al menos por dos barreras informáticas: en el nivel inferior, uno o varios ordenadores controlan los diversos aspectos detallados de la operación (SIT); por otra parte, interviniendo entre los operadores y los ordenadores de interacción con la tarea se sitúa la interfaz hombre-sistema, con otro ordenador (SIH) que —generalmente— apenas permite un nivel de interacción muy limitado entre los humanos y el proceso (que se convierte así en remoto).

Hemos pasado de un estadio en el que el individuo era el actor principal, y el ordenador su esclavo, a otro en el que los papeles se han invertido.

Esta situación se denomina «control de supervisión», que definió SHERIDAN (1984) como «... procesos de inicialización, monitorización y ajuste en sistemas que, por lo demás, están controlados automáticamente».

Tal sistema de control ha devengado un profundo cambio en la relación hombre-sistema. Como explica MORAY (1986):

«Existe un cierto sentido en decir que el actor principal es más el ordenador que el individuo. La mayor parte del tiempo, el ordenador decide cómo se debe ejercer el control y qué se debe informar o preguntar al operador. Este puede tomar el control o aceptar lo que el ordenador le propone pero, normalmente, a pesar de que es el individuo quien define la tarea que ha de realizar el ordenador, es este último el que ejerce el control. El ordenador se convierte así en el corazón del sistema».

Por tanto, hemos pasado de un estadio en el que el individuo era el actor principal, y el ordenador su esclavo, a otro en el que los papeles se han invertido. Durante la mayor parte del tiempo, la tarea del operador se reduce a supervisar el correcto funcionamiento del sistema, y a que éste funcione dentro de los límites normales. La cognición humana, con sus fortalezas y debilidades, se muestra poco adecuada para este tipo de actividad.

1.2. Los sistemas son cada vez más complejos y peligrosos

Una de las consecuencias de la creciente informatización antes descrita ha sido que los sistemas de alto riesgo (tales como plantas nucleares o de procesos químicos) han aumentado en tamaño y complejidad. Esto significa que cada vez mayores cantidades de materiales potencialmente peligrosos se concentran en centros de trabajo únicos bajo el control centralizado de un elenco cada día menor de operadores. Un fallo catastrófico de estos sistemas supone una seria amenaza no sólo para el personal de la planta, sino también para el público pedáneo (en plantas nucleares y de armamento, este riesgo se extiende más allá del área circundante).

1.3. Los sistemas poseen mayores defensas contra los fallos

Debido a las cada vez más catastróficas consecuencias derivadas de un posible fallo, y gracias a la disponibilidad cada vez mayor de hardware «inteligente», los diseñadores se han concentrado en incluir dispositivos automáticos de seguridad (DAS) suficientes para proteger el sistema contra cualquiera «escenario» conocido de fallo. **«Cuanto más complicada es una planta o mayor la interacción de sus elementos, mayor atención se presta a disminuir la eventualidad de los fallos ...»** (PERROW, 1984, pág. 43).

Así, el diseño de una planta nuclear moderna, por ejemplo, se basa en la filosofía de «defensa exhaustiva»: para que ocurra una catástrofe, durante la secuencia del accidente debe producirse una combinación de eventos aparentemente improbables (cfr. RASMUSSEN y PEDERSEN, 1984). En primer lugar, los dispositivos automáticos de seguridad tendrían que ser incapaces de restablecer el estado de seguridad del sistema; además, los métodos de confinamiento de materiales tóxicos tendrían que ser inútiles. Sin embargo, tales desastres todavía ocurren. Una de las razones más obvias reside en la susceptibilidad de estos sistemas de seguridad a los errores humanos y —en especial— a los latentes. Nos enfrentamos por tanto a una paradoja: estos sistemas especializados, específicamente diseñados para hacer que la planta sea segura, son también sus peores puntos débiles.

1.4. Los sistemas son cada vez más opacos

Una de las consecuencias de los mencionados avances tecnológicos es que estos sistemas complejos y exhaustivamente defendidos pierden su transparencia ante las personas que los dirigen, mantienen y operan. Esta opacidad tiene dos aspectos: no saber lo que está pasando, y no entender cómo puede reaccionar el sistema.

Como hemos visto, la automatización ha suscitado un cambio fundamental en el papel que las personas desempeñan en el ámbito de ciertas tecnologías de alto riesgo. En lugar de contactar directamente con el proceso, las personas han sido «promocionadas» «... **a tareas de supervisión de alto nivel y a tareas de planificación y mantenimiento a largo plazo**» (RASMUSSEN, 1987). En cualquier caso, estos individuos quedan apartados del proceso: la interfaz informática filtra la información que reciben. Como ha quedado demostrado en numerosos accidentes, con frecuencia los operadores no pueden encontrar lo que necesitan saber, y a la vez se ven inundados de información —posiblemente innecesaria— que no saben interpretar. En sistemas menos sofisticados, siempre cabía un recurso: el operador o el responsable salían y comprobaban la situación por sí mismos, examinaban la calidad del producto, revisaban la válvula que goteaba o recurrían a alguien con verdadera experiencia en el asunto. Sin embargo, estas soluciones ya no son factibles en las modernas plantas químicas o nucleares, donde se desarrolla un proceso al que uno no puede acercarse y que apenas se comprende parcialmente, dentro de un abstruso laberinto de tuberías, recintos de contención reforzados y bunkers de cemento.

Existe otro factor que contribuye decisivamente a la opacidad del sistema: sus propias defensas. RASMUSSEN (1988) ha denominado este fenómeno «la falacia de la defensa exhaustiva».

«Otro aspecto importante inherente a la filosofía de 'defensa exhaustiva' es que —con frecuencia— el sistema no responde activamente ante fallos aislados. Como consecuencia, muchos de los errores y fallos cometidos por el personal y por los técnicos de mantenimiento no se revelan directamente mediante una respuesta funcional del sistema. La fiabilidad de la actuación humana puede ser muy elevada —incluso en entornos muy dinámicos— si las eventuales equivocaciones y los posibles fallos conllevan efectos inmediatamente evidentes y pueden ser corregidos. La supervivencia al conducir por las calles de París en horas punta depende de este hecho».

«Compárese lo expuesto con el funcionamiento de un sistema cuyo diseño se atiene al principio de 'defensa exhaustiva'. En este caso, deben coincidir diversos sucesos independientes para que el sistema responda con cambios apreciables en su conducta. Al violarse algunas condiciones iniciales de seguridad del sistema durante la explotación del mismo no se producirá —probablemente— una respuesta funcional inmediata, y los

efectos latentes de los errores humanos pueden, por tanto, permanecer ocultos en el sistema. Cuando se permite la permanencia de tales errores durante un prolongado lapso temporal, aumenta drásticamente la probabilidad de que acaezca la multiplicidad de fallos necesarios para provocar un accidente. El análisis de los grandes accidentes muestra que la seguridad básica del sistema tiende a erosionarse debido a los errores latentes. Por tanto, cabría inferir que la seguridad de un sistema se mejora más al reducir la duración o permanencia de los errores latentes, que al reducir su frecuencia básica» (RASMUSSEN, 1988, págs. 3-4).

2. LAS IRONIAS DE LA AUTOMATIZACION

La Dra. LISANNE BAINBRIDGE (1987) del University College London ha resumido muchas de las dificultades que subyacen a la relación hombre-máquina en una instalación tecnológicamente avanzada. Se trata de lo que ella denomina «las ironías de la automatización».

Con cierta frecuencia, los ingenieros de diseño de un sistema tienden a conceder poca fiabilidad o eficiencia al operador, y procuran suplantarlo mediante dispositivos automatizados. Esta actitud entraña dos ironías: por un lado, los errores de los diseñadores, tal como se discute posteriormente en este artículo, contribuyen significativamente al acontecer de incidencias y accidentes; por otro lado, el mismo diseñador que desea eliminar la intervención humana, necesita sin embargo recurrir a la figura del operador **«... para que realice las tareas que el diseñador es incapaz de automatizar»** (BAINBRIDGE, 1987, pág. 272).

En una planta automatizada se necesitan operadores para supervisar el correcto funcionamiento del sistema. Pero es de sobra conocido que los operadores —incluso estando altamente motivados— no pueden ejercer una vigilancia efectiva durante prolongados intervalos de tiempo, por lo que resultan tremendamente inadecuados para llevar a cabo las tareas complementarias de supervisión de incidencias y anomalías. Para ayudarles, los diseñadores deben prever la generación automática de señales de alarma, pero ¿quién toma las decisiones cuando dichas alarmas fallan o han sido desconectadas?

Otra de las tareas de un operador consiste en asumir el control manual cuando falle el sistema automático de control. El control manual exige plena capacitación, y todo operador debería ejercitar continuamente su pericia para mantenerla en óptimas condiciones. Sin embargo, un sistema automático —que rara vez falla— niega a los operadores la oportunidad de practicar sus habilidades básicas de control. Una de las consecuencias de la automatización, por tanto, es que los operadores pierden su capacidad de acometer las complementarias tareas de supervisión (que son precisamente las que justifican la existencia de dichos operadores). Además, el control se suele asumir ante situaciones anómalas, que son las que exigen en el operador la máxima habilidad. DUNCAN (1987) sostiene esta misma opinión: **«Cuanto más fiable es una planta, menos oportunidades tiene el operador para practicar una intervención directa, y más difíciles serán las restantes tareas que realmente requieren su intervención».**

Estas ironías salpican también al tema de la formación de los operadores. Conscientes de la tensión nerviosa y de las dificultades a las que se enfrenta un operador ante una emergencia, los diseñadores y directivos no han escatimado esfuerzos en intentar encontrar procedimientos predefinidos para cualquier actuación del operador. Dichos procedimientos suelen basarse en intrincadas estructuras arborescentes o en sofisticados algoritmos que teóricamente permiten discernir una situación entre un conjunto de posibles fallos. Con ello se revela otra ironía más de la automatización: se enseña a los operadores a cumplir a rajatable unas ins-

trucciones escritas que han aprendido de memoria, y luego se les «coloca» en un sistema para que aporten su inteligencia interactiva y capacidad de improvisación. **«Quizás la ironía final es que los sistemas altamente automatizados, que raramente necesitan de intervención manual, son los que pueden precisar la mayor inversión en formación de los operadores»** (BAINBRIDGE, 1987).

3. EL «CIRCULO VICIOSO» DEL CONTROL DE SUPERVISION HUMANO

Como ya se ha indicado, la razón básica para incluir operadores en los sistemas controlados principalmente por ordenadores inteligentes es la capacidad humana para resolver emergencias «no previstas en el diseño». En resumen, los operadores están ahí porque los diseñadores no pueden prever todas las posibles situaciones de fallo y, por tanto, no son capaces de incluir dispositivos automáticos de seguridad para cada contingencia.

Además de un cierto efecto estético, los humanos aportan a los sistemas de alto riesgo su exclusiva habilidad para solucionar «interactivamente» los problemas que se plantean en situaciones nuevas. Irónicamente, y sin menospreciar a los astronautas del Apolo 13 ni a otros «solucionadores» natos, esta exclusiva habilidad es más bien teórica (al menos, en las condiciones que prevalecen normalmente en las situaciones de emergencia). Efectivamente, el ser humano —bajo situaciones de tensión— tiende a utilizar patrones prefijados de conducta, olvidando sopesar y razonar cuidadosamente las cosas. En definitiva, el operador tiende a recurrir a soluciones «enlatadas» que —si bien cristalizan las experiencias pasadas— no resuelven las verdaderas necesidades de la situación presente.

Se nos revela así la primera parte del círculo vicioso: ¿por qué ponemos operadores en los sistemas complejos?, para solucionar las emergencias; ¿cómo actuarán realmente a la hora de resolver los problemas?, según patrones rutinarios basados en interacciones previas con un entorno específico; ¿cuál es la experiencia que adquieren en una sala de control?, supervisar y realizar pequeñas prácticas ocasionales en la planta mientras ésta funciona dentro de sus límites de seguridad. Por lo tanto ¿se puede pretender que operen adecuadamente cuando deban reasumir la verdadera actividad de control? La evidencia muestra que esta actividad se llega a hacer tan extraña —y el sistema tan complejo— que, en un significativo número de ocasiones, los operadores actúan incorrectamente.

La evidencia muestra que la actividad de control llega a ser tan extraña —y el sistema tan complejo— que, en un significativo número de ocasiones, los operadores actúan incorrectamente.

Una posible solución consistiría en que el operador dedicara gran parte de su turno a formarse —con supuestos prácticos de emergencias pasadas— en el diagnóstico y recuperación del sistema. Y esto nos lleva a la segunda parte del círculo vicioso: la naturaleza de los sistemas modernos, con su gran complejidad y escasa transparencia, tiende a reservarnos inopinadas y desagradables sorpresas. Como demuestra claramente la multitud de casos estudiados, los accidentes suelen comenzar de una manera convencional, pero raramente evolucionan según patrones previsibles; cada incidente es un evento radicalmente nuevo y —salvo en un sentido muy genérico— la experiencia pasada sirve de muy poco. En estas condiciones, los errores son prácticamente inevitables. Mientras que aprender de los propios errores resulta altamente beneficioso en las indulgentes condiciones de la vida cotidiana, en la sala de control de una planta nuclear o quí-

mica tales experiencias educativas pueden tener consecuencias fatales.

La cuestión es que el control de supervisión humano no es algo concebido pensando en los humanos, sino uno de los subproductos de la revolución de los microchips. De hecho, si un grupo de etólogos se reuniera con la perversa intención de diseñar una actividad completamente inadecuada a las características de la cognición humana, es casi seguro que se aproximarían bastante a la actividad que se supone deben realizar los operadores de plantas químicas y nucleares.

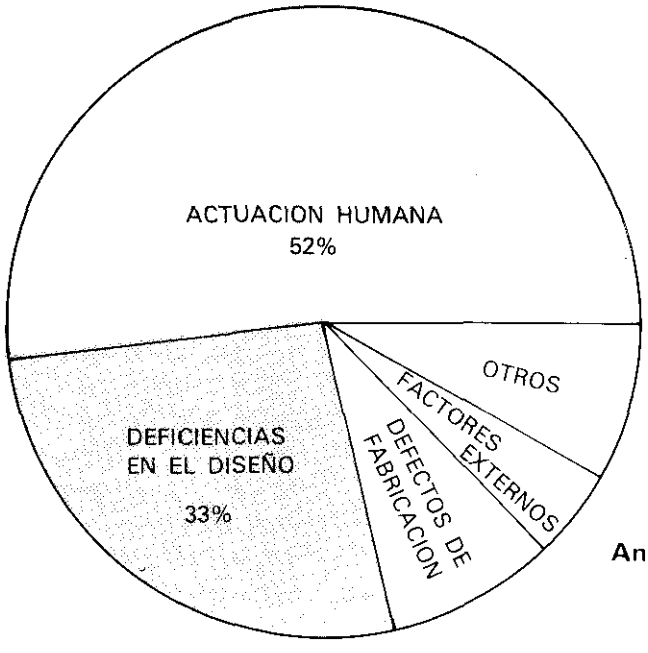
4. ALGUNOS DATOS CUANTITATIVOS SOBRE LOS FALLOS LATENTES

El Institute of Nuclear Power Operations, con sede en Atlanta (EE. UU.), llevó a cabo recientemente un detallado análisis de causalidad en 180 informes sobre eventos significativos (INPO, 1984). El análisis reveló 387 causas, que fueron clasificadas según su origen; los resultados se resumen en el siguiente gráfico.

A su vez, la actuación humana se clasificó en nuevas categorías: deficiencias en la documentación o en los procedimientos, 43%; falta de conocimientos o de formación, 18%; incorrecta ejecución de los procedimientos, 16%; deficiencias en la planificación o en la programación, 10%; inadecuada comunicación, 6%; defectos de supervisión, 3%; problemas en las políticas de la organización, 2%; otros, 2%.

De los anteriores datos cabe extraer dos importantes conclusiones:

1. Al menos del 92% de las causas determinantes se pueden atribuir a factores humanos.
2. Sólo un mínimo porcentaje se puede achacar directamente al personal de primera línea (por incorrecta ejecución de los procedimientos). La mayoría tienen sus orígenes en actividades relacionadas con el mantenimiento, o en decisiones incorrectas tomadas dentro de las esferas organizativas y directivas (fallos latentes).



Análisis de las causas determinantes (EE. UU., 1983/84).

5. ANALISIS DE CASOS DE ERRORES LATENTES

Esta sección pretende ilustrar la naturaleza y variedad de los errores latentes. Se analizan a tal efecto seis importantes accidentes: Three Mile Island, Bhopal, Challenger, Chernobyl, Zeebrugge y King's Cross. Estos sucesos no han sido elegidos por lo ostensible de los fallos latentes que concurrían; otros desastres como el de Flixborough, Seveso, Aberfan, Summerland, Tenerife, el estadio Heysel, o los incendios de Bradford y Piper Alfa, habrían también corroborado la importancia de estos fallos latentes.

Los criterios aplicados en la selección fueron los siguientes:

a) todos los sucesos son relativamente recientes, por lo que su naturaleza general resultará familiar al lector no especializado;

b) todos ellos están bien documentados y, de hecho, muchos de estos casos han sido sometidos a investigaciones gubernamentales de alto nivel; y

c) abarcan un amplio espectro de sistemas complejos de alto riesgo.

Debe destacarse que no se atribuirá especial importancia a las cantidades relativas de errores latentes y activos, ya que, habida cuenta de su relativa proximidad temporal, aquéllos serán siempre más numerosos que los últimos. Mi intención consiste más bien en ilustrar las insidiosas y —con frecuencia— imprevisibles formas en que tales fallos se combinan para romper las defensas del sistema en un momento crítico.

5.1. Three Mile Island

A las 04:00 del 28 de marzo de 1979, una de las turbinas se detuvo automáticamente (se bloqueó) en la unidad n.º 2 de los dos reactores de agua a presión (PWR) que la compañía Metropolitan Edison operaba en Three Mile Island, en el río Susquehanna, unos 16 km al sur de Harrisburg. El bloqueo se debió a la actuación de un equipo de mantenimiento que intentaba renovar la resina que se emplea para tratar el agua de la planta. Por una junta defectuosa en el sistema de clarificación del vapor condensado, se produjo una fuga de agua —el equivalente a una taza— que entró en el circuito de aire de los instrumentos neumáticos de la planta. La humedad interrumpió la presión de aire aplicada a las válvulas de las bombas de abastecimiento de agua; éstas «creyeron» que algo fallaba (lo que no era realmente cierto en este subsistema concreto), y se pararon automáticamente; con ello se interrumpió la entrada de agua al generador de vapor, y se bloqueó la turbina. Sin embargo, este dispositivo automático no fue suficiente para preservar la seguridad de la planta; sin las bombas, el calor del sistema primario de refrigeración (de alta radiactividad, por estar situado alrededor del núcleo) no se podía transferir al agua fría del sistema secundario (no radiactivo).

En ese momento se activaron automáticamente las bombas de emergencia, cuya función consiste en extraer el agua de un tanque especial y circularla por el sistema secundario, compensando así el agua que se evapora por el calor producido. Sin embargo, las conducciones para estas bombas de emergencia estaban bloqueadas: dos días antes, durante una actividad rutinaria de mantenimiento, algún operario se había dejado cerradas las correspondientes válvulas.

Al no extraerse el calor del sistema primario, la temperatura y la presión en el núcleo aumentaron rápidamente. Con ello se activó otro dispositivo automático de seguridad: la liberación de las barras de control. Estas barras, de grafito con un 80% de plata, se dejan caer en el núcleo del reactor para absorber los neutrones y detener así la reacción de fisión nuclear. Sin embargo, incluso tras extinguirse la reacción en cadena, los materiales del núcleo —todavía radiactivos— producen calor; éste

aumentó aún más la temperatura y la presión en el núcleo. En el diseño se había previsto que esta presión fuese liberada automáticamente por una válvula pilotada (PORV) que —una vez abierta— deja escapar el agua del núcleo hacia un enorme tanque presurizador, y de ahí a un sumidero situado bajo el recinto. Se supone que la PORV se abriría, bajaría la presión, y a continuación se cerraría automáticamente; pero en esta ocasión, cuando apenas habían transcurrido 13 segundos desde el inicio de la emergencia, la PORV se negó a cerrarse. Esta válvula abierta equivale a un agujero por el que el agua radiactiva del sistema primarios, sometida a gran presión, se estaba vertiendo al recinto, y de ahí hacia los sótanos de la planta.

En la emergencia, que duró algo más de 16 horas, se fugaron a la atmósfera pequeñas cantidades de material radiactivo. Aún no habiéndose asociado directamente a la pérdida de vidas humanas, el coste para las compañías explotadoras y las aseguradoras se situó en torno a los mil millones de dólares. Además, fue un auténtico jarro de agua fría para la energía nuclear en Estados Unidos, y sus repercusiones en la preocupación pública por la seguridad de las plantas nucleares todavía se dejan sentir en la actualidad.

En las investigaciones post-accidente se descubrió una amplia diversidad de torpezas gerenciales y un amplio número de dudosos procedimientos operativos. La inspección de la TMI-1 (la otra unidad del centro) reveló la pertinaz falta de mantenimiento. Por ejemplo, «**... de las válvulas colgaban estalactitas de boro de más de 30 cm, y en el suelo (del recinto de contención de la TMI-1) se habían formado estalagmitas**» (KEMENY, 1979). Otros descubrimientos de similares características fueron:

a) Los filtros de iodo se utilizaban continuamente (en vez de reservarse para filtrar el aire en el caso de contaminación radiactiva). Por ello, el día del accidente, presentaba una considerable reducción en su capacidad de filtrado.

b) Areas relativamente críticas de la planta estaban abiertas al público. El día anterior al accidente 750 personas habían accedido al edificio auxiliar.

c) Cuando se cambiaban los turnos, no se aplicaba ningún mecanismo para realizar una comprobación sistemática del estado de la planta. Además, se asignaban trabajos al personal de mantenimiento al principio de sus turnos respectivos, pero no se efectuaba una comprobación posterior de sus progresos en el trabajo.

d) Una revisión retrospectiva de los informes de eventos reveló la existencia de omisiones reiteradas, inadecuaciones en el análisis de fallos y falta de acciones correctoras.

e) Las tuberías y válvulas carecían de procedimientos adecuados de identificación (así, ocho horas después del inicio del accidente, los operarios emplearon más de diez minutos tratando infructuosamente de localizar —en una zona de alta radiación— tres válvulas de disminución de temperatura).

¿Era inusual este estado del TMI-2? ¿Se trataba simplemente de la «**manzana podrida del barril nuclear**? (PERROW, 1984). La evidencia sugiere lo contrario. Algunos años antes, MORRIS y ENGELKEN (1973) habían examinado ocho accidentes con fuga de refrigerante (LOCA). Dichos accidentes habían sucedido, en seis diferentes reactores de agua hirviendo, a lo largo de un período de dos años (cuando sólo existían 29 plantas en explotación). Centraron su atención en la búsqueda de coincidencias de fallos múltiples. En cada accidente concurrían entre dos y cuatros tipos diferentes de fallos; en la mitad de ellos se habían producido violaciones de los procedimientos operativos, pero siempre junto con otros dos a cinco fallos. Además, los fallos no se circunscribían al personal de la planta: en 20 plantas se encontraron válvulas deficientes suministradas por diez fabricantes diferentes. Como indi-

caba PERROW (1984), los accidentes como el del TMI-2 nacen de la concatenación de estos sucesos relativamente triviales en sistemas nada triviales. La generación de electricidad a partir de energía nuclear es una actividad de gran contenido técnico, pero resultaría ingenuo suponer que tal actividad está dirigida y operada por una raza especial de superhombres: no son peores que los que emplean las demás industrias, pero tampoco son mucho mejores.

5.2. Bhopal

En la noche del 2 al 3 de diciembre de 1984, una fuga de gas proveniente de una pequeña planta de fabricación de pesticidas, propiedad de una subsidiaria de Union Carbide Corporation, devastó la ciudad de Bhopal en la India central. Fue el peor desastre industrial de todos los tiempos: murieron al menos 2.500 personas, y hubo más de 200.000 heridos. El accidente de Bhopal, quizá más que cualquier otro de similar naturaleza, evidenció los riesgos que entraña la fabricación de productos químicos altamente tóxicos (en este caso, metil isocianato-MIC); estos riesgos, hasta entonces, no se habían tenido en cuenta.

El escape se produjo cuando una cierta cantidad de agua penetró en un tanque de almacenamiento del MIC. Para saber cómo llegó el agua hasta el tanque sería preciso desentrañar una intrincada historia de desidias en el mantenimiento, errores de los operarios, laberínticos diseños de las conducciones de bypass, fallo de los sistemas de seguridad, incompetencia gerencial, sequía, economía agrícola, nefastas decisiones gubernamentales y una cierta dosis de la mendacidad más absoluta.

5.3. Challenger

Reducida a términos meramente físicos, la causa del desastre de la lanzadera espacial Challenger en la mañana del 28 de enero de 1986 resulta brutalmente simple: poco después del despegue se partió una pieza de goma (el tristemente famoso «O-ring», junta en anillo) de uno de los impulsores del cohete; por la fisura salió proyectado el combustible inflamado, que causó la explosión de la lanzadera —y la muerte de sus siete tripulantes—. Después de nueve años de proyecto, la pieza en cuestión tenía una larga tradición de fallos e imperfecciones: mantenerla en el diseño del Challenger fue un claro ejemplo de incompetencia, «ceguera» selectiva, contraposición de objetivos y «pensar con los pies». Los principales protagonistas fueron el contratista de cohetes de combustible sólido (Morton Thiokol) y todos los escalafones directivos de la NASA.

5.4. Chernobyl

A las 01:24 del sábado 26 de abril de 1986 estalló la cúpula de cemento (más de 1.000 toneladas) que sellaba el reactor Chernobyl-4. En las dos explosiones que se produjeron, los fragmentos fundidos del núcleo del reactor se dispersaron por los alrededores, proyectándose a la atmósfera los productos de la fisión nuclear: era el peor accidente de la andadura comercial de la energía nuclear. Hasta ahora se ha cobrado más de 30 vidas, 1.000 km^2 en las inmediaciones de la planta ucraniana han quedado contaminados, y ha aumentado considerablemente el riesgo de muertes por cáncer en una extensa sona de Escandinavia y Europa Occidental. Fue un desastre causado enteramente por el hombre. Incluso al tiempo de escribir estas líneas (diciembre de 1988), todavía se restringe la venta de ovejas de los contaminados pastos del noroeste de Inglaterra.

La industria nuclear occidental se apresuró a afirmar enérgicamente que «eso aquí no habría pasado». Los analistas soviéticos señalaron como principal causa las infracciones y errores humanos, mientras que sus colegas occidentales —y especialmente Lord MARSHALL, jefe del CEGB— prefirieron culpar al pobre diseño del reactor RBMK y a la escasa «cultura soviética en materia de seguridad» —todavía resonaban los ecos de esta última afirmación cuando acontecieron los desastres de Zeebrugge y King's Cross.

5.5. Zeebrugge

A las 18:05 del 6 de marzo de 1987, el transbordador «Herald of Free Enterprise» de la Townsend Thoresen zarpaba del puerto interior de Zeebrugge con destino a Dover; sus compuertas de proa estaban abiertas. Al pasar frente al malecón exterior aumentó su velocidad, y el agua penetró por la proa inundando la cubierta inferior de coches (cubierta G). Hacia las 18:27, el Herald volcó con inusitada rapidez (en menos de dos minutos) y acabó tumbado y encallado, con su banda de estribor sobre las aguas. En este accidente perdieron la vida más de 150 pasajeros y 38 miembros de la tripulación; otras muchas personas resultaron heridas. El estudio del caso número 5 recoge la secuencia de acontecimientos y una breve relación de los fallos latentes.

En la tendencia general de los investigadores de accidentes —que suelen concentrar sus estudios en los errores activos—, la investigación de este desastre llevada a cabo por Mr. JUSTICE SHEEN (1987) ha supuesto una interesante excepción. Merece citarse con cierta extensión lo que escribió acerca de la responsabilidad gerencial en esta catástrofe:

«A primera vista, los errores que desencadenaron el desastre fueron los antes mencionados: errores de omisión por parte de miembros de la tripulación, y la inutilidad del Capitán KIRK a la hora de dar órdenes claras y hacerlas cumplir. Pero una investigación amplia de las circunstancias del desastre conduce inexorablemente a la conclusión de que los fallos subyacentes o cardinales recaen en las más altas esferas de la Compañía. Los directivos se habían desentendido de su responsabilidad en la seguridad de explotación de sus barcos. Ignorando sus auténticas obligaciones, no se plantearon la cuestión fundamental: ¿qué órdenes deberían dictarse para la seguridad de nuestros barcos? Da la impresión de que existen serias lagunas en la disposición del Herald para la travesia Dover/Zeebrugge. La cúpula directiva completa, desde el Consejo de Administración hasta los jefes de departamento, son culpables de lo que puede considerarse una responsabilidad compartida ante el fallo de la gestión. Desde lo más alto hasta los niveles inferiores, los miembros de la organización adolecían de una acusada desidia ... El fallo por parte de la Dirección en Tierra, que no emitió instrucciones claras y precisas, contribuyó asimismo al desastre» (Report of the Formal Investigation, 1987, pág. 14).

5.6. King's Cross

A las 19:25 del 18 de noviembre de 1987, el cigarrillo de algún descuidado fumador prendió fuego a la altamente inflamable borra que se había dejado acumular en las correderas de una escalera mecánica. Veinte minutos más tarde, las llamas inundaban el vestíbulo de taquillas donde se acumulaban las personas evacuadas por las escaleras de las líneas Victoria y Picadilly. A pesar de que los empleados de la estación y los pertinentes servicios de emergencia cometieron algunos errores activos, la principal causa de este desastre se encontraba presente en el sistema mucho antes de que el fuego se iniciase.

En la investigación posterior (FENNELL, 1988), el Inspector culpó tajantemente a la dirección de la London Regional Transport y a su compañía operativa, la London Underground. Tres citas bastarán para perfilar su valoración:

«El Presidente de la London Regional Transport, Sir KEITH BRIGHT, me comentó que los aspectos financieros eran supervisados meticulosamente, pero no así los temas de seguridad ... En mi opinión, equivocaba su verdadera reponsabilidad» (FENNELL, 1988, pág. 17).

«Resulta evidente, por lo que he podido escuchar, que la London Underground estaba intentando denodadamente reorientar su desafortunada política tradicional, y que se en-

contraba inmersa en lo que su Presidente y Director General, el Dr. RIDLEY, describió como 'un cambio de cultura y estilo'. Sin embargo, y a pesar de este cambio, la dirección seguía considerando que un incendio sería siempre algo inevitable en el metro más antiguo y extenso del mundo. En mi opinión, tal enfoque estaba profundamente descaminado» (op. cit. pág. 17).

«He dedicado un capítulo a la gestión de la seguridad porque la principal lección que hemos de aprender de esta tragedia es la política correcta que se debe adoptar en aras de la seguridad» (op. cit. pág. 18).

6. ERRORES Y TERGIVERSACIONES: LAS LECCIONES DE CHERNOBYL Y ZEEBRUGGE

Una conclusión importante que debe extraerse de los desastres de Chernobyl y Zeebrugge es que el término «error» no abarca la diversidad completa de factores humanos en los accidentes catastróficos. Al conformar un marco de trabajo adecuado para el análisis de conductas aberrantes (lit. «desviadas del camino»), es necesario distinguir entre errores e infracciones.

Con frecuencia, unos y otras pueden presentarse —y de hecho se presentan— en la misma secuencia de acciones, pero también pueden darse de manera independiente: una persona puede cometer un error sin por ello infringir nada, y una infracción no implica la comisión de un error.

Los errores pueden entrañar dos tipos de «desviación»: la divergencia involuntaria entre la actuación y la intención (lapsus y deslices), y el desvío de las acciones planificadas con respecto a trayectorias satisfactorias hacia los objetivos planteados (equivocaciones). Sin embargo, esta clasificación de los errores, al restringirse al proceso de información que desarrolla el individuo, apenas ofrece una visión parcial de las posibles conductas aberrantes. En efecto, se requeriría un nivel superior de análisis que partiera de la base de que, en la mayoría de los casos, los individuos no planifican y ejecutan sus acciones de manera aislada, sino dentro de un contexto social regulado. Así, si bien los errores pueden ser definidos en relación con el proceso cognitivo del propio individuo, las infracciones deberían ser concebidas dentro de un entorno social en el que la conducta se regula mediante procedimientos operativos, códigos, reglamentos, etc. A efectos de nuestro estudio, definimos «infringir» como «apartarse deliberadamente de aquellas prácticas que los diseñadores, gestores y entidades reguladoras estimen necesarias para mantener la seguridad en la explotación de un sistema potencialmente peligroso».

7. CLASIFICACION PRELIMINAR DE LAS INFRACCIONES

7.1. Categorías delimitadoras

Las infracciones pueden obedecer a múltiples motivos. Para identificar los extremos de esta gama de posibilidades podríamos considerar la intencionalidad de cada infracción. Como primer paso, nos preguntamos si existía intención previa; si la respuesta es negativa, la podemos incluir dentro de la categoría de «infracciones erróneas o no intencionadas»; si —por el contrario— ha sido deliberada, necesitaremos saber si existía o no intención de dañar el sistema, e incluso elevaríamos las infracciones dolosas a la categoría de sabotaje. Puesto que la primera categoría se sitúa dentro de la —ahora bien definida— zona de error, mientras que la última se sale del ámbito de la mayoría de las situaciones de accidente, las infracciones de mayor interés serán aquellas situadas entre ambas categorías, es decir, las que presentan un cierto grado de intencionalidad sin evidenciar un claro propósito de dañar el sistema.

Dentro de esta amplia nebulosa de infraccio-

nes deliberadas pero no dolosas, todavía podríamos distinguir dos amplias subcategorías: las rutinarias y las excepcionales. Las primeras se relacionan con los hábitos del individuo, y forman parte de su repertorio de conductas adquiridas; las últimas son infracciones excepcionales que se fraguan ante un conjunto de circunstancias particulares. La circulación rodada en las grandes urbes nos proporciona abundantes ejemplos claros de infracciones rutinarias; la conducta de los operarios y operadores de Chernobyl en los 20 minutos que precedieron a las explosiones son el perfecto ejemplo de infracciones extraordinarias.

7.2. Infracciones rutinarias

A la hora de conformar las infracciones habituales cabe destacar dos factores:

a) La tendencia natural en el hombre a seguir el método del mínimo esfuerzo.

b) La relativa indiferencia del entorno (que rara vez penaliza las infracciones, y pocas veces recompensa la observancia de las normas).

La experiencia demuestra que si la manera más rápida y cómoda de realizar una tarea implica transgredir un procedimiento de seguridad aparentemente trivial y rara vez sancionado, dicho procedimiento acabará por ser infringido rutinariamente por los operarios del sistema.

7.3. Infracciones excepcionales

Las infracciones excepcionales no están tan claramente especificadas, ya que son el producto de una amplia gama de condiciones de contorno. Sin embargo, tanto el desastre de Chernobyl como el de Zeebrugge sugieren la importancia de lo que podría denominarse «el doble ciego sistémico» o «las imposiciones contradictorias del sistema»: tareas particulares o circunstancias operativas que conducen inexorablemente a la infracción de las reglas, por loable que sea la intención de los operarios.

8. LOS «AGENTES PATOGENOS Y LA CAUSALIDAD DE LOS ACCIDENTES

El estudio de los casos aquí esbozados demuestra que los grandes desastres no suelen estar causados por un solo factor —ya sea éste mecánico o humano—, sino por la concatenación imprevista, y normalmente imprevisible, de diversos eventos diferentes, todos ellos necesarios pero no suficientes por sí mismos.

Todos los sistemas construidos por el hombre contienen agentes potencialmente dañinos, equiparables a los agentes patógenos en el cuerpo humano. En todo momento, cada sistema complejo entraña un cierto número de fallos latentes cuyos efectos no se manifiestan inmediatamente. Sin embargo, tales fallos latentes pueden propiciar actuaciones de los operarios en contra de la seguridad del sistema y —eventualmente— debilitar los mecanismos de defensa del mismo. En su mayoría, estos fallos latentes son tolerados, detectados y corregidos, o bien son controlados por medidas de protección. A veces, sin embargo, un conjunto de circunstancias externas (que aquí denominaremos **disparadores locales**) se coaliga con estos agentes patógenos para amenazar —de forma sutil y aparentemente imposible— las defensas del sistema, concitando su catastrófica destrucción.

Estos agentes patógenos incluyen las consecuencias de las decisiones incorrectamente tomadas por los gerentes, diseñadores, directivos, supervisores; también se incluyen aquí los errores latentes de mantenimiento y las infracciones rutinarias. Dentro de los disparadores locales se incluyen los fallos de componentes, estados atípicos del sistema, condiciones ambientales, errores activos del operador e infracciones excepcionales.

8.1. Algunos principios generales

Esta formulación de la causalidad de los accidentes en términos de agentes patógenos y dis-

paradores locales nos permite sentar una serie de principios generales.

8.1.1. La probabilidad de un accidente catastrófico es función del número de agentes patógenos presentes en ese momento en el sistema. Cuanto mayor es el número de agentes patógenos dentro de un sistema, mayor probabilidad habrá de que encuentren un conjunto de circunstancias —disparadores— suficientes para desencadenar un accidente.

8.1.2. En igualdad de condiciones, cuanto más complejo, interactivo, imbricado y opaco sea un sistema, mayor será el número de agentes patógenos. Sin embargo, a pesar de que los sistemas más simples suelen ser menos interactivos, menos centralizados y más transparentes, también tienden a ser considerablemente menos evolucionados en términos de seguridad o defensas internas. Por ello, un número relativamente reducido de agentes patógenos puede llegar a causar mayores daños en los sistemas más simples, que en los más avanzados.

8.1.3. El número de agentes patógenos generados por un cierto individuo será función directa de su nivel en la jerarquía de la toma de decisiones. Cuanto más alto es el nivel de una persona dentro del organigrama de una organización, mayor es su oportunidad para engendrar agentes patógenos. La excepción obvia a esta regla la constituyen los operarios de mantenimiento, cuyo trabajo entraña el acceso a una amplia gama de componentes del sistema, y cuyos errores e infracciones son susceptibles de trastornar la operatividad de subsistemas de vital importancia, y particularmente el funcionamiento de los dispositivos de seguridad.

8.1.4. A pesar de que algunos disparadores locales pueden y deberían ser anticipados y previstos por los diseñadores, directivos y operadores de un sistema determinado, es virtualmente imposible predecirlos en su totalidad. Como consecuencia, las medidas preventivas deberían centrarse en evaluar y reducir los agentes patógenos; éstos, al menos, son potencialmente detectables por aquéllos que conocen el sistema en su conjunto y que tienen adecuado acceso al mismo. Lo anterior plantea importantes cuestiones: ¿qué agentes patógenos estamos buscando? ¿Son algunos indicadores más significativos que otros a la hora de determinar el estado del sistema? ¿Cúal es la mejor manera de analizar prospectivamente la «salud» de un sistema? Estas cuestiones exigen —claramente— su propia y urgente investigación exhaustiva.

8.2. Implicaciones prácticas

Nuestro análisis sobre la causalidad de los accidentes implica todavía dos consecuencias adicionales. En primer lugar, si los métodos actuales de evaluación de riesgos (basados en árboles de fallos y eventos) no son capaces de proporcionar estimadores válidos de los errores activos de los operarios, tampoco serán capaces de descubrir los fallos latentes que pudieran llegar a combinarse con los disparadores locales para desencadenar un accidente.

En segundo lugar, si se acepta que las actuaciones socavadoras de la seguridad de un sistema tienen su verdadero origen en las decisiones erróneas de la dirección, entonces resulta evidente que los problemas residuales de seguridad inherentes a las tecnologías de alto riesgo no son atribuibles a puros «cambios de ingeniería». La investigación básica necesaria para mejorar la protección frente a accidentes desencadenados por una combinación de eventos, requiere por tanto una colaboración más estrecha entre los tecnócratas y las ciencias humanísticas.

9. DECISIONES INCORRECTAS Y ACTUACIONES PELIGROSAS

El estudio de los casos aquí descritos permite hacer una identificación preliminar de otros fac-

tores de interés: los designios del sistema que rigen la transformación de los defectos de diseño y los errores gerenciales, en actos que atentan contra la seguridad (errores e infracciones). A continuación consideramos nueve de estos factores:

9.1. Defectos en los equipos

En los seis accidentes estudiados se aprecia el efecto de decisiones incorrectas en materia de ubicación, diseño e instalación de los sistemas. En el caso de Three Mile Island, el incorrecto diseño de la sala de control y la inadecuación de las interfaces del sistema propiciaron los errores activos de los operadores. El accidente de Bhopal —y por ende sus terribles consecuencias— se puede atribuir directamente a fallos en los equipos. El desastre del Challenger radica en las largamente arraigadas deficiencias de la junta en anillo (deficiencias que la NASA y la Morton Thiokol —con su desidia— no subsanaron). Las explosiones de Chernobyl fueron causadas por una compleja interacción entre fallos activos y defectos inherentes al diseño, en el que se había obviado la importancia de un coeficiente positivo en vacío durante la operación a baja energía del reactor RBMK. Un factor decisivo en la tragedia del Herald fue la filosofía de su diseño que —si bien permite el transporte de un gran número de vehículos y pasajeros— coadyuvó a que volcara tan rápidamente, coartando así una eventual evacuación de emergencia. En King's Cross, la empresa debería haber reemplazado las escaleras mecánicas; esta negligencia jugó un papel fundamental en la tragedia resultante.

9.2. Incompatibilidad entre los objetivos del sistema y la seguridad

El estudio de los casos revela que, en la consecución de algunos objetivos del sistema, puede llegar a comprometer seriamente su seguridad. En el caso de Union Carbide y Townsend Thoresen, se trataba de aquilatar los beneficios y de asegurar la supervivencia empresarial: la dirección prefirió ahorrar dinero en vez de vidas. Se desconocen las causas por las que la dirección de Chernobyl autorizó la realización de una prueba que había sido rechazada —por motivos de seguridad— en otras plantas RMBK; sin embargo, puede ser que alguien quisiese apuntarse algunas medallas, pues se sabe que este tipo de reactores planteaba un problema técnico desde hacía tiempo —irónicamente, un problema cuya solución habría mejorado la seguridad del sistema—. En cuanto al Challenger, si bien ciertos criterios económicos influyeron en las decisiones gerenciales de Thiokol, es posible que la conveniencia política de explotar y mantener el éxito de la lanzadera indujera a los directivos de la NASA a menospreciar —y finalmente ignorar— las reiteradas advertencias de la junta en anillo. La dirección de la London Underground estaba plenamente inmersa en una amplia reconversión financiera; esta reorganización se hizo a costa de la seguridad de los pasajeros, de la cual ningún departamento era responsable. En tal clima, era inevitable que los mandos intermedios contemplaran la reducción de costes como objetivo primordial, y que las imprescindibles mejoras en la seguridad de los pasajeros fueran percibidas como algo completamente secundario.

9.3. Defensas inadecuadas o inexistentes

Este tipo de deficiencias resultó especialmente evidente en los desastres de Zeebrugge y Bhopal. En el primero de ellos, no habría resultado excesivamente caro implantar algún medio de evitar que el barco zarpara con las compuertas abiertas. La dirección respondió con el siguiente argumento a las repetidas solicitudes de instalación de indicadores en el puente de mando: «**... de nosotros no depende. En resumen, si las compuertas no quedan correctamente cerradas, la persona responsable de hacerlo debería ser amonestada**» (memorándum de un directivo, citado en el Report of

the Formal Investigation). En la estación de King's Cross no había planes de evacuación, un extintor de incendios se hallaba encerrado detrás de unas mamparas, y prácticamente nadie sabía dónde estaban los equipos auxiliares contra incendios. Además, algunas vías de escape estaban cortadas u obstaculizadas con puertas trancadas y barreras metálicas.

9.4. Procedimientos operativos inadecuados

En los seis accidentes cabe destacar la trágica influencia de las deficiencias en los procedimientos: desde el inadecuado procedimiento de relevo en los cambios de turno en el TMI-2, hasta el tristemente famoso «informe negativo» en la cubierta del Herald.

9.5. Desidia en el mantenimiento

La inadecuada gestión de las actividades de mantenimiento desempeñó un papel especialmente significativo en los accidentes de Bhopal, TMI-2 y King's Cross.

9.6. Formación inadecuada

Las serias deficiencias en los conocimientos y metodologías de los operadores contribuyeron significativamente a los accidentes de TMI-2, Bhopal y Chernobil. La ausencia de formación adecuada —para casos de incendio y emergencias— del personal de la estación de King's Cross se cobró vidas adicionales.

9.7. Condiciones propiciadoras de errores e infracciones

Estas condiciones quedaron especialmente patentes en Chernobyl y en el Herald. En el primer caso, se pidió a los operarios que realizaran una labor para la que no estaban cualificados y para la que, además, tenían que infringir las normas de seguridad. En Zeebrugge, la dirección había presionado para que se aumentara el número de servicios diarios; bajo este clima de presión, en más de una ocasión los barcos de la Townsend Thoresen habían abandonado el puerto con las compuertas de proa a popa abiertas.

9.8. Fallos organizativos

Estos fallos estuvieron presentes en los seis accidentes, pero constituyeron un factor probablemente decisivo en el caso de King's Cross. Tres divisiones de la London Underground disponían de personal especializado en materias de seguridad, pero ninguna persona o departamento asumía la responsabilidad general. La larga tradición de seguridad en los ferrocarriles parecía descartar la siniestralidad en el metro. En palabras del Inspector, la dirección de la London Underground adolecía de una **«autosuficiencia obtusa y peligrosa»** (op. cit. pág. 31).

9.9. Fallos de comunicación

A pesar de que los seis accidentes evidenciaban este tipo de deficiencias, los fallos de comunicación fueron especialmente relevantes en Chernobyl y en King's Cross. En este último caso, las vías de comunicación entre los distintos especialistas no estaban nada claras y, además, apenas se utilizaron. Las salas de control del metro de Londres carecían de sistemas adecuados de telefonía y señalización; esto ocasionó imperdonables retrasos en la comunicación de las instrucciones de la policía para evitar que otros trenes pararan en la estación. Además, los coches carecían de megafonía, y el circuito cerrado de televisión de la estación no se utilizó para dirigir la evacuación de los pasajeros. Por último, si bien la London Underground había ido recopilando y distribuyendo los informes de incendios anteriores en el metro, tales datos nunca llegaron a las altas esferas de la organización, y ni siquiera la Inspección de Ferrocarriles solicitó dicha información.

10. EPILOGO: LO QUE NOS ENSEÑAN LOS ACCIDENTES PASADOS

No resulta fácil aprender las lecciones que nos enseñan los accidentes catastróficos, especialmente si tales lecciones son consideradas como minadoras de la —ya de por sí— escasa confianza de la opinión pública en la seguridad de las tecnologías operadas por poderosos grupos de influencia. Las reacciones institucionales, tanto ante sus propios desastres como ante los de los demás, ponen de manifiesto dos defectos universales de la condición humana: **el error de la atribución fundamental, y el error de la sorpresa fundamental.**

El error de la atribución fundamental ha sido extensamente estudiado por la psicología social (cfr. FISKE y TAYLOR, 1984), y se refiere a la generalizada tendencia de atribuir los resultados negativos a las carencias personales de los individuos (factores disposicionales), en vez de achacarlos a factores situacionales que están más allá del control del individuo. Tal tendencia se evidencia en las respuestas al accidente de Chernobyl, tanto en la de los rusos como en la de los ingleses. Así, el informe ruso sobre Chernobyl (USSR State Committee on the Utilization of Atomic Energy, 1986) concluyó que: **«La causa principal del accidente residía en una combinación extremadamente improbable de infracciones de las instrucciones y procedimientos operativos».** Lord MARSHALL, Presidente del Central Electricity Generating Board (CEGB) del Reino Unido, prolongó el informe que la Atomic Energy Authority (1987) preparó sobre Chernobyl; sus palabras inculpan sin ambages: **«Para nosotros los occidentales, la secuencia de errores de los operadores del reactor resulta incomprensible. Quizá obedeciera a una suprema arrogancia, quizá a una completa ignorancia. Más plausiblemente, podemos especular que los operadores, como resultado del hábito, habían transgredido tranquilamente tantas reglas durante tanto tiempo, que las normas de seguridad perdieron completamente su relevancia».**

¿Podría ésto pasar en el Reino Unido? La revisión de Lord MARSHALL es la siguiente: **«... la enorme importancia de preservar la seguridad está tan profundamente enraizada en la cultura de la industria nuclear, que esto no podrá pasar en el Reino Unido».**

El término «sorpresa fundamental» fue acuñado por el israelita ZVRI LANIR (LANIR, 1987) en relación con la guerra del Yom Kippur; sin embargo, resulta particularmente apto tanto para el accidente del TMI-2 como para el de Chernobyl. Una sorpresa fundamental es la que revela una profunda discrepancia entre la realidad y la propia percepción del mundo; tales situaciones exigen una reorientación completa del enfoque adoptado. Las sorpresas situacionales, por otra parte, son sucesos localizados en los que basta con solucionar problemas específicos.

LANIR equipara la diferencia entre ambas sorpresas a la que existe entre «sorpresa» y «estupor», e ilustra su comparación con una anécdota de WEBSTER, el lexicólogo. Un día, al regresar a casa, WEBSTER descubrió a su mujer en brazos del mayordomo. «Me has sorprendido» dijo ella, «me has dejado estupefacto», respondió el. La señora WEBSTER experimentó una sorpresa situacional, pero la del señor WEBSTER fue una fundamental.

El individuo tiende a comportarse ante las sorpresas fundamentalmente como lo haría ante simples sorpresas situacionales. Por ello, el error de la sorpresa fundamental **«... supone desestimar toda significación fundamental, limitándose a aprender lecciones situacionales a partir de aspecto superficiales»** (LANIR, 1987). Y éste es precisamente el error que el estamento nuclear británico ha cometido con respecto a los accidentes de Chernobyl y Three Mile Island.

En la investigación pública del Sizewell B (LAYFIELD, 1986), los miembros del CEGB procuraron aislar a la futura estación de los proble-

mas que el reactor PWR presentó en Three Mile Island el 28 de marzo de 1979. Identificaron los aspectos más destacados del accidente del TMI-2 (la planta de vapor, atascos en las válvulas de escape, deficiencias en el diseño de la sala de control, inadecuada formación de los operarios, etc.) y afirmaron que estos y otros aspectos serían radicalmente mejorados en el reactor PWR de Sizewell B. En su informe, Sir FRANK LAYFIELD apunta una visión más amplia: **«algunos aspectos del accidente del TMI nos advierten de factores que son de general importancia»**, pero acaba concluyendo que no resultan aplicables en el Reino Unido debido a las diferencias organizativas.

Esta natural preocupación por distanciar las instalaciones británicas de las catástrofes de los países extranjeros se puso aún más de manifiesto en el análisis de la UKAEA sobre el desastre de Chernobyl (GITTUS, 1987): **«En conclusión, el accidente de Chernobyl se debe exclusivamente al diseño del reactor RBMK y, por tanto, hay poco que el Reino Unido pueda aprender de él. Su principal consecuencia ha sido la de reforzar y reiterar la importancia y validez de los estándares británicos actuales».**

Por lo tanto, ¿cuáles son las lecciones que hemos de aprender de los desastres de TMI y Chernobyl? En el caso de Three Mile Island, estas lecciones han sido destacadas —creo que muy acertadamente— por DAVID WOODS, en la actualidad en la Ohio University, aunque anteriormente trabajara en la Corporación Westinghouse (WOODS, 1987). Sus conclusiones generales pueden igualmente aplicarse a los accidentes de Chernobyl, Bhopal, Challenger, Zeebrugge y King's Cross.

«El accidente de TMI fue algo más que una inesperada cadena de fallos, algo más que una situación prevista pero resulta inadecuadamente, y algo más que una situación cuya previsión devino inadecuada. El accidente de TMI fue una sorpresa fundamental que reveló una incompatibilidad básica entre la realidad y la opinión que la industria nuclear se había formado sobre ella misma. Antes del accidente de TMI la industria podía considerar, y consideraba, que la energía nuclear era un sistema puramente técnico en el que todos los problemas se enmarcaban dentro de algún área técnica y en el que las soluciones a tales problemas dimanaban de las diversas disciplinas de la ingeniería. El accidente de TMI evidenció claramente lo falaz de ese punto de vista, ya que los fallos residían en el sistema socio-tecnológico, y no en factores técnicos ni humanos».

En cualquier tecnología, y para cualquier país que la aproveche, el mensaje de este artículo es muy claro: nadie posee el monopolio de defectos en el diseño, decisiones gerenciales inadecuadas y desidias en el mantenimiento. Y son estos fallos humanos latentes los que entrañan el principal riesgo residual para los modernos sistemas complejos.

REFERENCIAS

1. BAINBRIDGE, L.: "The ironies of automation". En: J. Rasmussen, K.
2. Duncan & J. Keplat (eds.): "New Technology and Human Error". Wiley, Londes, 1987.
3. BATSTONE, R.: "Workshop to develop a multisectoral/multidisciplinary research program to determine critical management and organizational failures that may lead to catastrophic system failure". The World Bank, Washington DC, 1987.
4. DUNCAN, K.: "Fault diagnosis for advanced continuos installations". En J. Rasmussen, K.