Seguridad nuclear: ¿se puede entender?

La energía nuclear trae el "pecado original" de haber nacido a la opinión pública con las bombas atómicas de Hiroshima y Nagasaki. Luego siguieron décadas de desarrollo de usos pacíficos perfectamente responsables, pero en paralelo algunos pocos accidentes (desde incidentes menores que sólo dañaron a la instalación, hasta la catástrofe de Chernobil) colaboraron a que la imagen pública siguiera siendo negativa. Está claro que el problema no es la difusión pública de los incidentes, sino que el riesgo de accidentes en instalaciones nucleares se perciba como excesivo aún sin elementos de análisis. La divulgación de incidentes no ha sido acompañada en general con una explicación y presentación de información detallada acerca de los riesgos objetivos de la actividad y del enfoque técnico que se usa para reducirlo. En este contexto se entiende que haya dudas en el público respecto a si las instalaciones nucleares son seguras o no, y cabe preguntarse si es posible explicar de una manera clara y accesible en qué consiste el enfoque de ingeniería denominado "seguridad nuclear". Creemos que sí, que el método para prevenir accidentes (y si se dieran mitigar sus consecuencias) no es nada misterioso, que no es una cosa complicadísima sólo para iniciados, y este artículo es un intento de presentar esa explicación.

Néstor Masriera
Ing. Nuclear.
Egresado del Inst. Balseiro.
Profesional del INVAP y anteriormente de ENACE

SEGURIDAD NUCLEAR FORMAL

La seguridad nuclear consiste en asegurar que no se producirá daño por radiación ni a personas (trabajadores o público en general) ni al medio ambiente aún en caso de que haya cosas (componentes, equipos o estructuras) que fallen o se rompan. Yendo a funciones concretas, la manera de lograr este objetivo es primero diseñando con "holgura" para evitar fallas, y luego es asegurando que haya equipos que cumplan la función de mantener el material radioactivo confinado previendo en el diseño que cualquier cosa de los equipos puede fallar o romperse, que los operadores pueden equivocarse, y que hay eventos externos que pueden impactar en la Planta.

En la "jerga" técnica se habla de los "objetivos de seguridad" que se logran mediante sistemas que ejecutan ciertas "funciones de seguridad" de manera garantizada por diseño. Las funciones de seguridad nuclear en reactores (de investigación o de producción de electricidad) están bien definidas: aún en caso de accidente (o en caso de duda) hay que 1-apagar el reactor, 2-refrigerarlo, y 3-confinar todo material radioactivo.

La pregunta que surge es: ¿Se puede analizar un diseño de instalación nuclear para poder confiar que cumple con esto, antes de construirla? La respuesta positiva es el método de verificación de diseño denominado "Análisis de Seguridad", muy consolidado a nivel de prácticas reconocidas a nivel internacional, que es más o menos así:

El primer paso es hacer una lista muy completa de todas las cosas que podrían fallar o romperse (válvulas, bombas, caños, instrumentos, fuentes eléctricas, computadoras, mecanismos, soportes, etc.), incluyendo los eventos externos a la planta que pueden afectarla, y las maniobras erróneas que pueda realizar el personal de operación. Se las llama Eventos Iniciantes Postulados, y se dice "postulados" porque se hace la lista postulando que fallen, no importa si hay una buena razón para que fallen o no.

El segundo paso es evaluar lo que pasa después de cada uno de los Eventos Iniciantes, cómo evolucionan las cosas en lo que se denomina la "Secuencia Accidental". Por ejemplo, si se rompe un caño hay que ver cuál es el componente que se queda sin agua, y si

es de refrigeración de algún componente hay que ver qué le pasa.

El tercer paso es agrupar esas secuencias accidentales en casos que "envuelvan" muchos otros de los analizados, pasando de muchas secuencias de severidad variada, a unos pocos casos extremos denominados "Casos de Seguridad".

El cuarto paso es probablemente el más trabajoso, y consiste en analizar los casos de seguridad en suficiente detalle como para garantizar que uno sabe cómo resulta, en términos de si se conseguirá mantener el núcleo intacto y las envueltas de confinamiento activas. En general para esto se utilizan modelos de computadora que simulan la planta describiendo el comportamiento de cada componente que participan de la secuencia. O sea que se modela cada cañería, válvula, bomba, intercambiador de calor, tanque, etc, No es que sea un modelo de TODA la planta: hay sistemas que no aportan a esa respuesta dinámica: e.g. agua sanitaria, calefacción, iluminación, etc.

En el quinto paso se estudia la respuesta a los casos de seguridad en cuanto hay situaciones en que la planta "no se las arregla sola" y hay que poner sistemas de instrumentación y control que monitorean la planta (algunos caudales, temperaturas o presiones, etc.) y automáticamente actúan alguna válvula, alguna bomba, etc. O sea que en este paso hay que identificar qué "mirar" (cuáles son las "variables de seguridad") para identificar si la Planta está teniendo una secuencia accidental de los Casos de Seguridad. Por ejemplo, si el caudal de refrigeración del reactor se reduce un poco, ya se actúa como en el peor caso de pérdida de caudal aunque todavía no haya nada en riesgo.

En el sexto paso se definen y estudian las acciones de protección y los sistemas / componentes que las tiene que llevar a cabo las Funciones de Seguridad. Por ejemplo si hay que abrir una válvula para inyectar agua en un lugar que se está quedando corto de refrigeración. Este estudio también requiere los modelos de simulación computacional para reproducir la secuencia accidental de los casos de seguridad.

Para completar este análisis por pasos, además hay que prever que si hay una acción automática sobre equipos, cualquier cosa puede fallar a demanda. O sea que si hay un controlador automático que enciende una bomba para circular agua, ese arranque puede fallar, o si se actúa una válvula, puede trabarse. Si la instalación está bien diseñada, para las funciones de seguridad no basta poner un equipo que las lleve a cabo, sino que hay que prever un segundo equipo, o tal vez tres en paralelo, de manera que aunque uno falle las funciones de seguridad se lleven a cabo de todos modos.

En el "cierre" de este análisis está el "criterio de aceptación", que implica haber demostrado que evaluando la respuesta a una lista completa de Eventos Iniciantes Postulados, el diseño consigue responder "bien" aún considerando que cualquier cosa puede fallar a demanda.

Hay un séptimo paso del análisis de seguridad: ver qué pasa si las cosas que fallan son más que las previstas, o si el evento iniciante es de esas cosas rarísimas de tipo efecto dominó (como en películas) o errores sucesivos de operadores, o lo que sea que termine provocando que algo del combustible se dañe y haya material radioactivo "dando vueltas" por los sistemas de la planta. Para escenarios así, en que se postula que los sistemas previstos y analizados en los pasos previos no alcanzaron, se colocan provisiones de diseño para mitigar las consecuencias de esos hipotéticos accidentes severos. Hay conceptos asociados a ese tipo de análisis, por ejemplo "defensa en profundidad", "barreras múltiples", "falla segura", "mapas de fallas", diversidad, redundancia, etc.

Puesto todo lo anterior en resumen, un análisis de seguridad implica:

1. Construir una lista de Eventos Iniciantes Postulados (exhaustiva, clasificada)
2. Evaluar las Secuencias Accidentales en sus consecuencias
3. Agrupar las secuencias por tipos en pocos Casos de Seguridad (envolventes)
4. Análisis detallado de transitorios de Casos de Seguridad (modelo de simulación)
5. Detección de la secuencia accidental para los Casos de Seguridad
6. Desarrollo de acciones de protección para garantizar funciones de seguridad
7. Escenarios DBA - funciones de seguridad, BDBA - mitigación

Ahora bien, si el lector se mantuvo despierto y llegó hasta acá puede que todo lo anterior le haya parecido un montón de buenas intenciones difíciles de llevar a casos prácticos. Para mostrar un ejemplo práctico podríamos tomar una instalación nuclear, pero eso nos llevaría una cantidad de hojas que sí garantizaría que se duerman los lectores que quedan...

Así que se pondrá un ejemplo alternativo: evaluar el diseño de una aerosilla, que es algo más conocido y manejado por el público.

EVALUACIÓN DEL DISEÑO DE UNA AEROSILLA CON METODOLOGÍA DE SEGURIDAD NUCLEAR

Como ya se mencionó, para que un diseño cumpla con pautas de seguridad nuclear, debe tener en cuenta que las cosas pueden fallar (materiales, equipos, operadores, componentes, etc.).

Una aerosilla es un sistema compuesto de sillas colgadas de un cable de acero mediante "perchas". El cable se sostiene desde torres por sistemas de poleas, y en las estaciones terminales del recorrido hay ruedas para mantener el cable tensionado y con una rueda motriz es traccionado para que circule. Cuando se diseña una aerosilla (su "base de diseño") se considera el peso de las sillas con pasajeros, montacargas y cable; tensiones en el cable por peso y tracción; vibración por movimiento, sismo, viento y tensiones térmicas, etc.

Vayamos ahora a los pasos del Análisis de Seguridad:

En el primer paso, la identificación sistemática de las posibles fallas que lleven a secuencias accidentales (Eventos Iniciantes). Podemos postular fallas en las sillas, en las barandas, en las perchas de enganche, en las poleas, en las ruedas tensoras y de tracción. También tenemos que postular el descarrilamiento y fallas humanas.

En el segundo paso deberíamos analizar las Secuencias Accidentales que siguen a cada uno de los eventos. Por ejemplo: ante la falla de una polea, el cable se afloja de golpe y cae un poco hasta tensarse en las otras poleas, ahí puede rebotar y descarrilarse de otras poleas, aumentando el efecto que podría terminar en que se desploman el cable y todas las sillas. De manera similar puede estudiarse qué pasa después de cada evento de falla postulado, pero por espacio le quedará como tarea al lector.

En el tercer paso se tienen que agrupar las secuencias en envolventes de consecuencias extremas, que podrían ser los siguientes dos Casos de Seguridad:

- "caída de un pasajero / silla" es envolvente de fallas en la estructura de la silla, gancho, baranda, algunos errores humanos, etc.
- "caída del cable" es envolvente de falla de poleas, del cable, de ruedas

tensoras y motrices, de la estructura de una torre, descarrilamiento, etc.

En los pasos 4 a 6 deberíamos poder reproducir los casos de seguridad con cierto rigor, para asegurar que las provisiones de diseño adoptadas alcanzan para alcanzar el objetivo de que no se caigan los pasajeros (ni uno). En este contexto no se planteará reproducir los transitorios de los Casos de Seguridad usando modelos de simulación por computadora. Tal vez sería más adecuado hacerlo por ensayos. En todo caso el foco es cómo prevenir que el evento iniciante progrese hacia un accidente, y el desarrollo de acciones de protección.

Yendo a ejemplos: tomando el evento iniciante de falla del cable, se ve que como no se puede evitar que un cable individual falle, la salida es usando redundancia con varios cables (que sea multifilar). La protección para que el evento no progrese a accidente es la inspección para detectar hilos cortados, o aún una deformación (paso previo al corte) como la de la *foto*. La acción de protección sería el cambio del cable completo.

Tomando ahora el evento iniciante de falla de una polea. Para tolerar esta falla nuevamente se apela a la redundancia, que es colocar siempre más de una polea en serie (ver *foto*).

El descarrilamiento es el resultado de que el cable se desplace fuera del cauce de la polea, por algún otro evento que podría ser el viento, la falla de una polea, la pérdida de tensión repentina en el cable. La provisión de diseño para prevenir esto es la colocación de guías orientando el cable sobre las poleas (ver *foto*).

Para ambas situaciones (falla de polea o descarrilamiento) la protección para que el evento no progrese a accidente es el monitoreo permanente del personal que opera, y la acción de protección sería la detención inmediata usando botones de emergencia (esos típicos botones rojos con forma de hongo).

Yendo ahora a los eventos iniciantes producidos por el Factor Humano, puede decirse que este factor es la causa de incidentes más frecuente en aerosillas. De hecho una búsqueda rápida por Internet lleva a una variedad de anécdotas e imágenes de errores de pasajeros que terminan golpeados o colgados de la ropa. Para éstos casos se ve que la provisión de diseño para que un error del pasajero no termine en caída es la baranda de seguridad, pero es el mismo pasajero el que la sube o baja. Aquí aparece un punto débil del diseño de aerosillas en uso actualmente: ante un error humano se pierde la provisión de diseño que protege al pasajero. Puede parecer inverosímil que un pasajero quiera levantar la baranda con la silla en altura, pero el análisis de seguridad nuclear es muy taxativo en eso: los eventos iniciantes se postulan, y si son físicamente posibles no se los descarta por "verosimilitud" o porque requieran de un equívoco grueso.

Como conclusión de este ejercicio (que no pretende ser riguroso), vemos que un análisis sistemático siguiendo los lineamientos de IAEA para Análisis de Seguridad Nuclear permite evaluar objetivamente un diseño y decir si es aceptable o no.

Cabe aclarar que no se cuestiona cómo la industria de aerosillas analiza sus diseños, que de hecho usa conceptos de redundancia, monitoreo para la detección de eventos y actuaciones de protección que son análogos a los de seguridad nuclear. En todo caso se busca enfatizar que la metodología "nuclear" provee un enfoque sistemático para evaluar, y resulta muy útil para identificar puntos que pueden mejorarse.

Queda por describir la aplicación del séptimo paso para una aerosilla, que sería ver qué pasa cuando las provisiones de diseño no alcanzaron a cumplir su objetivo, y se produce la caída de un pasajero, una silla o todo el cable. O sea "situaciones más allá de la base de diseño". En un diseño "nuclear" deben preverse provisiones de mitigación, como por ejemplo un freno de emergencia (pasivo) para las poleas, que sería un mecanismo técnicamente viable para amortiguar la caía del cable en caso que se corte o descarrile.

Para reducir el impacto de caída las provisiones podrían ir desde sacar rocas bajo el trazado, optimizar la ruta para evitar grandes alturas, hasta acolchar toda la superficie bajo las sillas con goma-espuma. Claramente esto último es un disparate, lo que lleva a preguntarse ¿Cuál es el alcance razonable para las provisiones de diseño de mitigación? ¿Cuál es el criterio de aceptación en este aspecto? La respuesta es un análisis ulterior de tipo probabilístico, y se refiere a que hay un "umbral" de probabilidad de cosas que vale la pena tener en cuenta. Por ejemplo no puede diseñarse para prever la caída de un meteorito que tenga una probabilidad de ocurrir de una vez en 100 millones de años, pero hay que tener en cuenta terremotos o inundaciones de probabilidad de ocurrencia de uno en mil años. El umbral de probabilidad aceptable es más bajo para accidentes de mayores consecuencias.

CONCLUSIONES GLOBALES

Esperamos haber mostrado algo de por qué se está en condiciones de afirmar que es posible analizar el diseño de una instalación nuclear y decir si ese diseño es adecuado para evitar eficazmente todo daño relevante a las personas y el medio ambiente.

Lo que se afirma en estos párrafos es que se dispone de herramientas de análisis adecuadas, y que en sus trazos gruesos es posible hacer este análisis accesible y entendible a quien le interese conocerlo. Aunque en esto se debe ser muy claro: no siempre en todo lugar del mundo las personas responsables de velar por la seguridad de instalaciones nucleares hicieron su trabajo a conciencia. ■