

COLECCIÓN DE NORMAS DE SEGURIDAD DEL OIEA

Evaluación y verificación
de la seguridad
de las centrales
nucleares

GUÍA DE SEGURIDAD

No. NS-G-1.2



IAEA

Organismo Internacional de Energía Atómica

PUBLICACIONES DEL OIEA RELACIONADAS CON LA SEGURIDAD

NORMAS DE SEGURIDAD DEL OIEA

Con arreglo a lo dispuesto en el artículo III de su Estatuto, el OIEA está autorizado a establecer o adoptar normas de seguridad para proteger la salud y reducir al mínimo el peligro para la vida y la propiedad, y a proveer a la aplicación de esas normas.

Las publicaciones mediante las cuales el OIEA establece las normas aparecen en la **Colección de Normas de Seguridad del OIEA**. Esta serie de publicaciones abarca la seguridad nuclear, radiológica, del transporte y de los desechos, así como la seguridad general (es decir, todas esas esferas de la seguridad). Las categorías comprendidas en esta serie son las siguientes: **Nociones fundamentales de seguridad, Requisitos de seguridad y Guías de seguridad**.

Las normas de seguridad llevan un código que corresponde a su ámbito de aplicación: seguridad nuclear (NS), seguridad radiológica (RS), seguridad del transporte (TS), seguridad de los desechos (WS) y seguridad general (GS).

Para obtener información sobre el programa de normas de seguridad del OIEA puede consultarse el sitio del OIEA en Internet:

<http://www-ns.iaea.org/standards/>

En este sitio se encuentran los textos en inglés de las normas de seguridad publicadas y de los proyectos de normas. También figuran los textos de las normas de seguridad publicados en árabe, chino, español, francés y ruso, el glosario de seguridad del OIEA y un informe de situación relativo a las normas de seguridad que están en proceso de elaboración. Para más información se ruega ponerse en contacto con el OIEA, PO Box 100, 1400 Viena (Austria).

Se invita a los usuarios de las normas de seguridad del OIEA a informar al Organismo sobre su experiencia en la aplicación de las normas (por ejemplo, como base de los reglamentos nacionales, para exámenes de la seguridad y para cursos de capacitación), con el fin de garantizar que sigan satisfaciendo las necesidades de los usuarios. La información puede proporcionarse a través del sitio del OIEA en Internet o por correo postal, a la dirección anteriormente señalada, o por correo electrónico, a la dirección Official.Mail@iaea.org.

OTRAS PUBLICACIONES RELACIONADAS CON LA SEGURIDAD

Con arreglo a lo dispuesto en el artículo III y el párrafo C del artículo VIII de su Estatuto, el OIEA facilita y fomenta la aplicación de las normas y el intercambio de información relacionada con las actividades nucleares pacíficas, y sirve de intermediario para ello entre sus Estados Miembros.

Los informes sobre seguridad y protección en las actividades nucleares se publican como **informes de seguridad**, que ofrecen ejemplos prácticos y métodos detallados que se pueden utilizar en apoyo de las normas de seguridad.

Otras publicaciones del OIEA relacionadas con la seguridad se publican como **informes sobre evaluación radiológica, informes del INSAG** (Grupo Internacional Asesor en Seguridad Nuclear), **Informes Técnicos**, y documentos **TECDOC**. El OIEA publica asimismo informes sobre accidentes radiológicos, manuales de capacitación y manuales prácticos, así como otras obras especiales relacionadas con la seguridad. Las publicaciones relacionadas con la seguridad física aparecen en la **Colección de Seguridad Física Nuclear del OIEA**.

**EVALUACIÓN Y VERIFICACIÓN
DE LA SEGURIDAD
DE LAS CENTRALES NUCLEARES**

Los siguientes Estados son Miembros del Organismo Internacional de Energía Atómica:

| | | |
|-------------------------------------|-----------------------------------|---|
| AFGANISTÁN, REPÚBLICA ISLÁMICA DEL | FEDERACIÓN DE RUSIA | NICARAGUA |
| ALBANIA | FILIPINAS | NÍGER |
| ALEMANIA | FINLANDIA | NIGERIA |
| ANGOLA | FRANCIA | NORUEGA |
| ARABIA SAUDITA | GABÓN | NUEVA ZELANDIA |
| ARGELIA | GEORGIA | OMÁN |
| ARGENTINA | GHANA | PAÍSES BAJOS |
| ARMENIA | GRECIA | PAKISTÁN |
| AUSTRALIA | GUATEMALA | PALAU |
| AUSTRIA | HAITÍ | PANAMÁ |
| AZERBAIYÁN | HONDURAS | PARAGUAY |
| BAHREIN | HUNGRÍA | PERÚ |
| BANGLADESH | INDIA | POLONIA |
| BELARÚS | INDONESIA | PORTUGAL |
| BÉLGICA | IRÁN, REPÚBLICA ISLÁMICA DEL | QATAR |
| BELICE | IRAQ | REINO UNIDO DE GRAN BRETAÑA E IRLANDA DEL NORTE |
| BENIN | IRLANDA | REPÚBLICA ÁRABE SIRIA |
| BOLIVIA | ISLANDIA | REPÚBLICA |
| BOSNIA Y HERZEGOVINA | ISLAS MARSHALL | CENTROAFRICANA |
| BOTSWANA | ISRAEL | REPÚBLICA CHECA |
| BRASIL | ITALIA | REPÚBLICA DE MOLDOVA |
| BULGARIA | JAMAHIRIYA ÁRABE LIBIA | REPÚBLICA DEMOCRÁTICA DEL CONGO |
| BURKINA FASO | JAMAICA | REPÚBLICA DOMINICANA |
| BURUNDI | JAPÓN | REPÚBLICA UNIDA DE TANZANÍA |
| CAMERÚN | JORDANIA | RUMANIA |
| CANADÁ | KAZAJSTÁN | SANTA SEDE |
| CHAD | KENYA | SENEGAL |
| CHILE | KIRGUISTÁN | SERBIA |
| CHINA | KUWAIT | SEYCHELLES |
| CHIPRE | LESOTHO | SIERRA LEONA |
| COLOMBIA | LETONIA | SINGAPUR |
| CONGO | LÍBANO | SRI LANKA |
| COREA, REPÚBLICA DE | LIBERIA | SUDÁFRICA |
| COSTA RICA | LIECHTENSTEIN | SUDÁN |
| CÔTE D'IVOIRE | LITUANIA | SUECIA |
| CROACIA | LUXEMBURGO | SUIZA |
| CUBA | MADAGASCAR | TAILANDIA |
| DINAMARCA | MALASIA | TAYIKISTÁN |
| ECUADOR | MALAWI | TÚNEZ |
| EGIPTO | MALÍ | TURQUÍA |
| EL SALVADOR | MALTA | UCRANIA |
| EMIRATOS ÁRABES UNIDOS | MARRUECOS | UGANDA |
| ERITREA | MAURICIO | URUGUAY |
| ESLOVAQUIA | MAURITANIA, REPÚBLICA ISLÁMICA DE | UZBEKISTÁN |
| ESLOVENIA | MÉXICO | VENEZUELA, REPÚBLICA BOLIVARIANA DE |
| ESPAÑA | MÓNACO | VIET NAM |
| ESTADOS UNIDOS DE AMÉRICA | MONGOLIA | YEMEN |
| ESTONIA | MONTENEGRO | ZAMBIA |
| ETIOPÍA | MOZAMBIQUE | ZIMBABWE |
| EX REPÚBLICA YUGOSLAVA DE MACEDONIA | MYANMAR | |
| | NAMIBIA | |
| | NEPAL | |

El Estatuto del Organismo fue aprobado el 23 de octubre de 1956 en la Conferencia sobre el Estatuto del OIEA celebrada en la Sede de las Naciones Unidas (Nueva York); entró en vigor el 29 de julio de 1957. El Organismo tiene la Sede en Viena. Su principal objetivo es “acelerar y aumentar la contribución de la energía atómica a la paz, la salud y la prosperidad en el mundo entero”.

COLECCIÓN DE
NORMAS DE SEGURIDAD DEL OIEA No. NS-G-1.2

EVALUACIÓN Y VERIFICACIÓN DE LA SEGURIDAD DE LAS CENTRALES NUCLEARES

GUÍA DE SEGURIDAD

ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA
VIENA, 2009

DERECHOS DE AUTOR

Todas las publicaciones científicas y técnicas del OIEA están protegidas en virtud de la Convención Universal sobre Derecho de Autor aprobada en 1952 (Berna) y revisada en 1972 (París). Desde entonces, la Organización Mundial de la Propiedad Intelectual (Ginebra) ha ampliado la cobertura de los derechos de autor que ahora incluyen la propiedad intelectual de obras electrónicas y virtuales. Para la utilización de textos completos, o parte de ellos, que figuren en publicaciones del OIEA, impresas o en formato electrónico, deberá obtenerse la correspondiente autorización, y por lo general dicha utilización estará sujeta a un acuerdo de pago de regalías. Se aceptan propuestas relativas a reproducción y traducción sin fines comerciales, que se examinarán individualmente. Las solicitudes de información deben dirigirse a la Sección Editorial del OIEA:

Dependencia de Promoción y Venta de Publicaciones
Sección Editorial
Organismo Internacional de Energía Atómica
Vienna International Centre
PO Box 100
1400 Viena (Austria)
fax: +43 1 2600 29302
tel.: +43 1 2600 22417
correo-e: sales.publications@iaea.org
<http://www.iaea.org/books>

© OIEA, 2009

Impreso por el OIEA en Austria
Noviembre de 2009

**EVALUACIÓN Y VERIFICACIÓN DE LA SEGURIDAD
DE LAS CENTRALES NUCLEARES**

OIEA, VIENA, 2009

STI/PUB/1112

ISBN 978-92-0-313509-2

ISSN 1020-5837

PRÓLOGO

Mohamed ElBaradei
Director General

Una de las funciones estatutarias del OIEA es establecer o adoptar normas de seguridad para proteger, en el desarrollo y la aplicación de la energía nuclear con fines pacíficos, la salud, la vida y los bienes, y proveer lo necesario para la aplicación de esas normas a sus propias operaciones, así como a las realizadas con su asistencia y, a petición de las Partes, a las operaciones que se efectúen en virtud de cualquier arreglo bilateral o multilateral, o bien, a petición de un Estado, a cualquiera de las actividades de ese Estado en el campo de la energía nuclear.

Los siguientes órganos supervisan la elaboración de las normas de seguridad: la Comisión sobre normas de seguridad (CSS); el Comité sobre normas de seguridad nuclear (NUSSC); el Comité sobre normas de seguridad radiológica (RASSC); el Comité sobre normas de seguridad en el transporte (TRANSSC); y el Comité sobre normas de seguridad de los desechos (WASSC). Los Estados Miembros están ampliamente representados en estos comités.

Con el fin de asegurar el más amplio consenso internacional posible, las normas de seguridad se presentan además a todos los Estados Miembros para que formulen observaciones al respecto antes de aprobarlas la Junta de Gobernadores del OIEA (en el caso de las Nociones fundamentales de seguridad y los Requisitos de seguridad) o el Comité de Publicaciones, en nombre del Director General, (en el caso de las Guías de seguridad).

Aunque las normas de seguridad del OIEA no son jurídicamente vinculantes para los Estados Miembros, éstos pueden adoptarlas, a su discreción, para utilizarlas en sus reglamentos nacionales respecto de sus propias actividades. Las normas son de obligado cumplimiento para el OIEA en relación con sus propias operaciones, así como para los Estados en relación con las operaciones para las que éste preste asistencia. A todo Estado que desee concertar con el OIEA un acuerdo para recibir su asistencia en lo concerniente al emplazamiento, diseño, construcción, puesta en servicio, explotación o clausura de una instalación nuclear, o a cualquier otra actividad, se le pedirá que cumpla las partes de las normas de seguridad correspondientes a las actividades objeto del acuerdo. Ahora bien, conviene recordar que, en cualquier trámite de concesión de licencia, la decisión definitiva y la responsabilidad jurídica incumbe a los Estados.

Si bien las mencionadas normas establecen las bases esenciales para la seguridad, puede ser también necesario incorporar requisitos más detallados, acordes con la práctica nacional. Además, existirán por lo general aspectos

especiales que será necesario aquilatar en función de las circunstancias particulares de cada caso.

Se menciona cuando procede, pero sin tratarla en detalle, la protección física de los materiales fisibles y radiactivos y de las centrales nucleares en general; las obligaciones de los Estados a este respecto deben enfocarse partiendo de la base de los instrumentos y publicaciones aplicables elaborados bajo los auspicios del OIEA. Tampoco se consideran explícitamente los aspectos no radiológicos de la seguridad industrial y la protección del medio ambiente; se reconoce que, en relación con ellos, los Estados deben cumplir sus compromisos y obligaciones internacionales.

Es posible que algunas instalaciones construidas conforme a directrices anteriores no satisfagan plenamente los requisitos y recomendaciones prescritos por las normas de seguridad del OIEA. Corresponderá a cada Estado decidir la forma de aplicar tales normas a esas instalaciones.

Se señala a la atención de los Estados el hecho de que las normas de seguridad del OIEA, si bien no jurídicamente vinculantes, se establecen con miras a conseguir que las aplicaciones pacíficas de la energía nuclear y los materiales radiactivos se realicen de manera que los Estados puedan cumplir sus obligaciones derivadas de los principios generalmente aceptados del derecho internacional y de reglas como las relativas a la protección del medio ambiente. Con arreglo a uno de esos principios generales, el territorio de un Estado ha de utilizarse de forma que no se causen daños en otro Estado. Los Estados tienen así una obligación de diligencia y un criterio de precaución.

Las actividades nucleares civiles desarrolladas bajo la jurisdicción de los Estados están sujetas, como cualesquier otras actividades, a las obligaciones que los Estados suscriben en virtud de convenciones internacionales, además de a los principios del derecho internacional generalmente aceptados. Se cuenta con que los Estados adopten en sus ordenamientos jurídicos nacionales la legislación (incluidas las reglamentaciones) así como otras normas y medidas que sean necesarias para cumplir efectivamente todas sus obligaciones internacionales.

NOTA EDITORIAL

Todo apéndice de las normas se considera parte integrante de ellas y tiene la misma autoridad que el texto principal. Los anexos, notas de pie de página y bibliografía sirven para proporcionar información suplementaria o ejemplos prácticos que pudieran ser de utilidad al lector.

En las normas de seguridad se usa la expresión “deberá(n)” (en inglés “shall”) al formular indicaciones sobre requisitos, deberes y obligaciones. El uso de la expresión “debería(n)” (en inglés “should”) significa la recomendación de una opción conveniente.

El texto en inglés es la versión autorizada.

ÍNDICE

| | | |
|----|--|----|
| 1. | INTRODUCCIÓN | 1 |
| | Antecedentes (1.1–1.2) | 1 |
| | Objetivo (1.3–1.5) | 1 |
| | Alcance (1.6–1.8) | 2 |
| | Estructura (1.9) | 3 |
| 2. | EVALUACIÓN Y ANÁLISIS DE LA SEGURIDAD Y VERIFICACIÓN INDEPENDIENTE | 3 |
| | Evaluación y análisis de la seguridad (2.1–2.7) | 3 |
| | Verificación independiente (2.8–2.12) | 4 |
| | Relación entre el diseño, la evaluación de la seguridad y la verificación independiente (2.13–2.19) | 5 |
| 3. | ASPECTOS DE INGENIERÍA IMPORTANTES PARA LA SEGURIDAD | 8 |
| | Generalidades (3.1) | 8 |
| | Prácticas de ingeniería y experiencia operacional probadas (3.2–3.6) | 8 |
| | Dispositivos innovadores en el diseño (3.7–3.9) | 9 |
| | Realización de la defensa en profundidad (3.10–3.16) | 10 |
| | Protección radiológica (3.17–3.25) | 12 |
| | Clasificación de las estructuras, sistemas y componentes atendiendo a la seguridad (3.26–3.31) | 14 |
| | Protección contra sucesos externos (3.32–3.49) | 15 |
| | Protección contra peligros interiores (3.50–3.56) | 19 |
| | Conformidad con los códigos, normas y guías aplicables (3.57–3.58) | 21 |
| | Cargas y combinación de cargas (3.59–3.62) | 22 |
| | Selección de materiales (3.63–3.72) | 23 |
| | Evaluación del fallo único y redundancia/independencia (3.73–3.80) | 24 |
| | Diversidad (3.81–3.85) | 27 |
| | Pruebas, mantenimiento, reparación, inspecciones y monitorización en servicio de los elementos importantes para la seguridad (3.86–3.90) | 28 |

| | |
|--|-----------|
| Cualificación de equipos (3.91–3.96) | 29 |
| Mecanismos de envejecimiento y de desgaste (3.97–3.101) | 30 |
| Interfaz hombre-máquina y aplicación de la ingeniería de factores humanos (3.102–3.116) | 32 |
| Interacciones entre sistemas (3.117–3.121) | 35 |
| Uso de ayudas computacionales en el proceso de diseño (3.122–3.123) | 36 |
| 4. ANÁLISIS DE SEGURIDAD | 37 |
| Orientación general (4.1–4.32) | 37 |
| Sucesos iniciadores postulados (SIP) (4.33–4.49) | 43 |
| Análisis determinista de seguridad (4.50–4.122) | 47 |
| Análisis probabilista de seguridad(4.123–4.231) | 65 |
| Estudios de sensibilidad y análisis de Incertidumbres (4.232–4.235) | 89 |
| Evaluación de los códigos de cálculo empleados (4.236–4.244) | 90 |
| 5. VERIFICACIÓN INDEPENDIENTE (5.1–5.10) | 92 |
| REFERENCIAS | 95 |
| COLABORADORES EN LA REDACCIÓN Y REVISIÓN | 97 |
| ÓRGANOS ENCARGADOS DE APROBAR LAS NORMAS DE SEGURIDAD | 99 |

1. INTRODUCCIÓN

ANTECEDENTES

1.1. Esta publicación sirve de complemento a la de Requisitos de Seguridad titulada “Seguridad de las centrales nucleares: Diseño” [1].

1.2. La presente Guía se ha preparado tras un examen sistemático de todas las publicaciones relevantes, en particular las referentes a Nociones Fundamentales de Seguridad [2], Seguridad de las centrales nucleares: Diseño [1], las revisiones actuales o en curso de otras guías de seguridad, informes INSAG [3, 4] y otras publicaciones que tratan de la seguridad tecnológica de las centrales nucleares. Esta Guía proporciona también orientación a las Partes Contratantes en la Convención sobre Seguridad Nuclear para el cumplimiento de sus obligaciones a tenor del artículo 14, Evaluación y verificación de la seguridad.

OBJETIVO

1.3. La publicación de Requisitos de Seguridad titulada “Seguridad de las centrales nucleares: Diseño” [1] establece que deberá realizarse una evaluación exhaustiva de la seguridad y una verificación independiente de esta evaluación antes de que el diseño sea presentado al órgano regulador (véanse los párrs. 3.10 a 3.13). Esta publicación proporciona orientaciones sobre cómo debería darse cumplimiento a este requisito.

1.4. La presente Guía de Seguridad formula recomendaciones a los responsables del diseño sobre cómo realizar una evaluación de la seguridad tecnológica durante la fase inicial del diseño y las modificaciones del mismo, así como a la entidad explotadora sobre cómo realizar una verificación independiente de la evaluación de la seguridad de nuevas centrales nucleares, tanto si se trata de diseños innovadores como de diseños ya existentes. Las recomendaciones para realizar una evaluación de la seguridad tecnológica proporcionan también orientación útil para examinar dicha seguridad en el caso de una central existente. El objetivo de examinar centrales ya existentes con referencia a normas y prácticas actuales es determinar si existe alguna desviación que pudiera repercutir en la seguridad de la central. Los métodos y las recomendaciones de esta Guía de Seguridad pueden ser empleados también por los órganos reguladores para la realización de exámenes y evaluaciones

reglamentarios. Aunque la mayoría de las recomendaciones de la guía son generales y de aplicación a todo tipo de reactor nuclear, hay algunas de ellas y algunos ejemplos específicos que son aplicables, principalmente, a los reactores refrigerados por agua.

1.5. Ciertos términos tales como evaluación de la seguridad, análisis de seguridad y verificación independiente se emplean con significado distinto en diferentes países. El significado de los términos empleados en la presente guía se explica en la Sección 2. El término “diseño”, tal como se usa aquí, incluye las especificaciones para el funcionamiento y la gestión seguros de la central.

ALCANCE

1.6. En esta Guía de Seguridad se formulan las recomendaciones esenciales para efectuar la evaluación de la seguridad y la verificación independiente. Se ofrece orientación detallada que complementa la Ref. [1], en particular en materia de análisis de seguridad. No obstante, no se incluyen todos los detalles técnicos disponibles y se remite a otras publicaciones del OIEA sobre cuestiones específicas de diseño y métodos concretos de análisis de la seguridad.

1.7. Los objetivos específicos de la seguridad tecnológica, ya obedezcan a planteamientos deterministas o probabilistas, o bien los límites radiológicos concretos, pueden variar de unos países a otros y su responsabilidad incumbe a los órganos reguladores. En esta Guía se hacen algunas referencias a objetivos y límites establecidos por organizaciones internacionales. Los explotadores, y en algunos casos los encargados del diseño, pueden fijar también sus propios objetivos de seguridad, que pueden ser incluso más estrictos que los fijados por las instancias reguladoras, o referirse a aspectos diferentes de la seguridad. En algunos países se cuenta con que los explotadores así lo hagan como muestra de su ‘responsabilización’ en todo lo referente a seguridad.

1.8. La presente Guía no incluye recomendaciones específicas acerca de la evaluación de la seguridad de aquellos sistemas de la central para los que existen guías de seguridad particularizadas.

ESTRUCTURA

1.9. En la Sección 2 se definen los términos evaluación de la seguridad, análisis de seguridad y verificación independiente, y se expone brevemente la relación existente entre ellos. En la Sección 3 se formulan las recomendaciones esenciales para la evaluación de la seguridad con respecto a los requisitos principales y los requisitos de diseño de la central. En la Sección 4 se formulan las recomendaciones esenciales para el análisis de seguridad. Se dan indicaciones para determinar los sucesos iniciadores postulados (SIP) que se emplean a lo largo de todo el proceso de evaluación, incluidos el análisis de seguridad, el análisis determinista de transitorios, el análisis de accidentes graves, y el análisis probabilista de seguridad. En la Sección 5 se formulan las recomendaciones esenciales para la verificación independiente de la seguridad de la central.

2. EVALUACIÓN Y ANÁLISIS DE LA SEGURIDAD Y VERIFICACIÓN INDEPENDIENTE

EVALUACIÓN Y ANÁLISIS DE LA SEGURIDAD

2.1. En este contexto, la evaluación de la seguridad tecnológica es el proceso sistemático que se lleva a cabo a lo largo de la elaboración del diseño para cerciorarse de que el diseño de la central propuesto (o real) satisface todos los requisitos importantes de seguridad. Entre ellos figuran también normalmente los requisitos fijados por la entidad explotadora y los órganos reguladores. La evaluación de la seguridad incluye, sin limitarse a ello, el análisis metódico de ese tema (véase la Sección 4). El diseño y la evaluación de la seguridad forman parte del mismo proceso iterativo que lleva a cabo el responsable del diseño de la central, tarea que continúa hasta que se llega a una solución de diseño que satisface todos los requisitos de seguridad, los cuales pueden incluir también los establecidos durante el proceso de diseño.

2.2. El objeto de la evaluación de la seguridad es comprobar que el diseño satisface los requisitos de gestión en materia de seguridad, los requisitos técnicos principales y los requisitos de diseño de la central y sus sistemas que se enuncian en las Secciones 3 a 6 de la publicación sobre “Seguridad de las

centrales nucleares: Diseño” [1], así como que se ha realizado un análisis exhaustivo de la seguridad tecnológica.

2.3. Los requisitos para la gestión de la seguridad (Sección 3 de la Ref. [1]) tratan cuestiones relacionadas con prácticas probadas de ingeniería, experiencia operacional e investigación sobre seguridad tecnológica.

2.4. Los requisitos técnicos principales (Sección 4 de la Ref. [1]) comprenden los que sirven para garantizar que se cuente con una defensa en profundidad suficiente y que se preste la máxima atención a la prevención de accidentes y la protección radiológica.

2.5. Los requisitos para el diseño de las centrales (Sección 5 de la Ref. [1]) tratan cuestiones tales como la cualificación del equipo, el envejecimiento y el logro de fiabilidad en los sistemas de seguridad adoptando medidas de redundancia, diversificación y separación física.

2.6. Los requisitos para el diseño de los sistemas de centrales (Sección 6 de la Ref. [1]) tratan cuestiones relacionadas con el diseño del núcleo del reactor, del sistema de refrigeración del reactor y de los sistemas de seguridad como los de contención y refrigeración de emergencia del núcleo.

2.7. En relación con el análisis de seguridad tecnológica, el párrafo 5.69 de la Ref. [1] establece que “Deberá llevarse a cabo un análisis de seguridad del diseño de la central en el que se aplicarán métodos de análisis deterministas y probabilistas. Sobre la base de dicho análisis se establecerá y se confirmará la base de diseño de los elementos de importancia para la seguridad. También deberá demostrarse que la central, tal como está diseñada, puede cumplir los límites prescritos para casos de liberación de materiales radiactivos y los límites aceptables para las dosis potenciales de radiación correspondientes a cada categoría de estados de la central (véase el párrafo 5.7), y que se ha hecho efectiva la defensa en profundidad”. El alcance y los objetivos de los análisis probabilista y determinista de seguridad tecnológica se reseñan más adelante en los párrafos 4.17 a 4.22.

VERIFICACIÓN INDEPENDIENTE

2.8. El párrafo 3.13 de la Ref. [1] establece que “Antes de presentar el diseño al órgano regulador, la entidad explotadora deberá asegurarse de que personas

o grupos distintos de los que realizaron el diseño llevan a cabo una verificación independiente de la evaluación de la seguridad”.

2.9. La verificación independiente debería ser efectuada bajo la responsabilidad de la entidad explotadora por un equipo de expertos que sean, en la medida de lo posible, independientes de los autores del diseño y de quienes realicen la evaluación de la seguridad. Se considera que esos expertos son independientes cuando no han intervenido en ninguna de las partes del diseño ni de la evaluación de la seguridad. Esta verificación independiente se lleva a cabo además de los exámenes de garantía de calidad (GC) que se efectúen en el marco de la entidad encargada del diseño.

2.10. Mientras que la evaluación de la seguridad es un estudio exhaustivo que llevan a cabo los diseñadores a lo largo del proceso de diseño para satisfacer todos los requisitos pertinentes de seguridad, la verificación independiente suele ser realizada por la entidad explotadora o en su nombre, y puede referirse solamente al diseño que se presenta al órgano regulador para su aprobación.

2.11. En vista de la complejidad de las cuestiones de diseño y de evaluación de la seguridad que tienen que abordarse en la verificación independiente, es habitual realizar parcialmente esta verificación en paralelo con el proceso de diseño, en vez de dejarla para el final.

2.12. Las instancias reguladoras suelen llevar a cabo un examen independiente por separado para comprobar que el diseño cumple los requisitos por ellas estipuladas.

RELACIÓN ENTRE EL DISEÑO, LA EVALUACIÓN DE LA SEGURIDAD Y LA VERIFICACIÓN INDEPENDIENTE

2.13. La figura 1 presenta la relación existente entre la evaluación de la seguridad, la verificación independiente, el análisis de seguridad y otras actividades llevadas a cabo durante el diseño de una central nuclear. Esta figura muestra también cómo la presente Guía de Seguridad se relaciona con otras publicaciones relativas al proceso de diseño.

2.14. A medida que el diseño evoluciona desde su concepción inicial hasta su completa elaboración, el diseñador ha de tener en cuenta todos los requisitos de seguridad, y cualesquiera otros definidos tanto por el explotador de la

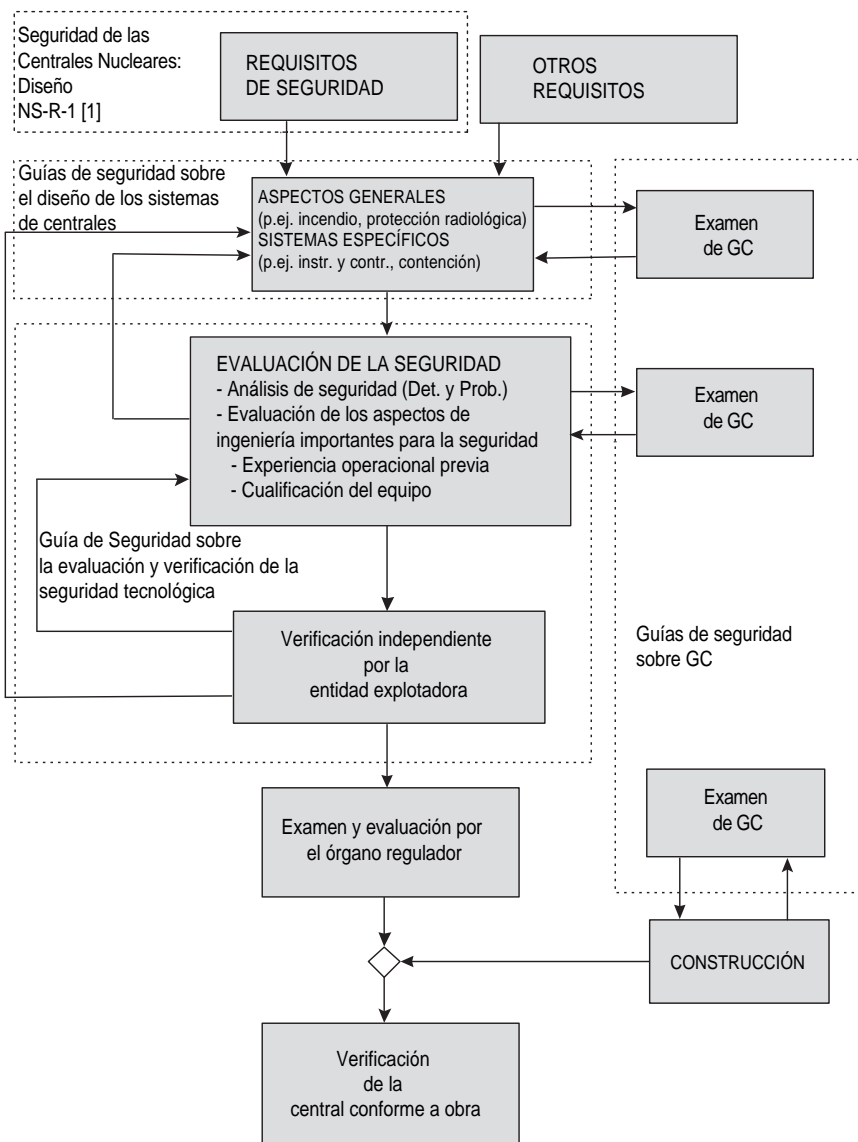


FIG. 1. Temas tratados por las normas de seguridad del OIEA relativas al diseño de centrales nucleares [1] (Det.: determinista; Prob.: probabilista).

central como por el regulador. Cuando se trate de programas nucleares en desarrollo o de la implantación de nuevos diseños, los requisitos de diseño pueden ser revisados o aclarados durante el proceso de diseño. En el caso de los diseños novedosos, los requisitos pueden establecerse en detalle mientras avanza el diseño.

2.15. A lo largo del proceso de diseño, la evaluación de la seguridad y la verificación independiente corren a cargo de grupos o entidades diferentes. Ahora bien, por ser partes integrantes en el proceso iterativo de diseño, ambas comparten el objetivo principal de garantizar que la central cumpla los requisitos de seguridad tecnológica. Por esta razón, los dos temas se tratan en la misma guía de seguridad. En algunos casos, el órgano regulador participa también en la fase de diseño.

2.16. En diferentes etapas del proceso de diseño (por ejemplo, antes de iniciar la construcción o el funcionamiento a potencia) se dejará en suspenso ese proceso y se realizará un estudio analítico de seguridad, en el que se expone la labor de diseño y de evaluación de la seguridad que se haya llevado a cabo hasta ese punto. Ello proporciona información al órgano regulador para su tarea de examen y evaluación.

2.17. La verificación independiente es más efectiva si se efectúa en paralelo con el diseño y la evaluación de la seguridad, ya que el pronto examen y aclaración de las cuestiones de seguridad acelera y facilita su resolución. Toda recomendación que se formule para mejorar el diseño o la evaluación de la seguridad tecnológica se puede atender con la máxima facilidad mientras el trabajo de diseño esté en curso. Por otro lado, una relación demasiado estrecha hará que se cuestione la independencia de la verificación, y debería encontrarse un punto de equilibrio entre la efectividad y la independencia.

2.18. Las decisiones importantes que se hayan de tomar en el curso del diseño pueden requerir exámenes independientes especiales del mismo por parte de la entidad explotadora, limitados al alcance de la decisión que se tenga que tomar y en los que posiblemente se considere el cumplimiento de los requisitos de seguridad aplicables al tema que se vaya a decidir.

2.19. El trabajo de diseño debería realizarse conforme a un programa de GC, que incluya exámenes independientes de todos los documentos pertinentes. El proceso general de GC se trata en la Guía de Seguridad SG-Q-10-[5].

3. ASPECTOS DE INGENIERÍA IMPORTANTES PARA LA SEGURIDAD

GENERALIDADES

3.1. En esta sección figuran recomendaciones y consideraciones importantes para evaluar la conformidad del diseño con los requisitos de las Secciones 3 a 5 de la Ref. [1]. Estos requisitos se refieren a los aspectos generales de ingeniería importantes para la seguridad y se aplican a todos los sistemas de la central nuclear. Aunque es posible que la evaluación de la correcta aplicación de los requisitos en tales aspectos no se considere explícitamente en el análisis de seguridad, constituye un elemento importante para evaluar la seguridad. En algunos de estos aspectos no existen criterios de aceptación bien definidos y, por lo tanto, la evaluación del cumplimiento de los requisitos de seguridad se basa en gran parte en sólidas apreciaciones de ingeniería.

PRÁCTICAS DE INGENIERÍA Y EXPERIENCIA OPERACIONAL PROBADAS

3.2. En los reactores de tipo evolutivo, el diseño debería hacerse empleando en lo posible estructuras, sistemas y componentes (ESC) que hayan dado buen resultado ya en centrales en funcionamiento, o, por lo menos, debería tomarse buena nota de la experiencia operacional pertinente obtenida en otras centrales.

3.3. Al evaluar la seguridad debería tenerse en cuenta la experiencia operacional existente con objeto de cerciorarse de que han sido adecuadamente consideradas en el diseño todas las enseñanzas importantes en esa materia. La experiencia operacional debería ser una fuente fundamental de información para mejorar la defensa en profundidad de la central.

3.4. Al utilizar los aportes de la experiencia operacional para el diseño y la evaluación de la seguridad debería aprovecharse al máximo el gran cúmulo de información operacional que, en su mayor parte, está libremente accesible para las entidades y particulares interesados. Los datos sobre experiencia operacional deberían tomarse de: i) el banco de datos nacionales; ii) los sistemas de notificación de incidentes de la Asociación Mundial de Explotadores de Instalaciones Nucleares (WANO) así como OIEA-Agencia

para la Energía Nuclear de la OCDE (AEN de la OCDE); y iii) los informes de las misiones ASSET (Assessment of Safety Significant Events Team) del OIEA.

3.5. El análisis por extrapolación de una secuencia real de sucesos hasta lo que podría haber ocurrido finalmente en una central de haberse producido otros fallos adicionales (comparados con los que realmente tuvieron lugar) ha demostrado ser una herramienta útil de diseño.

3.6. Los resultados de los programas generales de investigación sobre seguridad tecnológica pueden también proporcionar un apoyo útil a los diseñadores y los examinadores en sus tareas de evaluación. Estos resultados de la investigación sobre seguridad están generalmente accesibles en reuniones de composición abierta, en la bibliografía y en bases de datos informatizadas. Las bases genéricas de datos de seguridad tecnológica del OIEA y los documentos técnicos del OIEA (documentos IAEA-TECDOC) son ejemplos de resultados internacionales en materia de investigación sobre la seguridad.

DISPOSITIVOS INNOVADORES EN EL DISEÑO

3.7. Tomando como base las enseñanzas de la experiencia operacional, los análisis y la investigación en el campo de la seguridad, se impone admitir el examen de la necesidad y utilidad de mejoras de diseño que se salgan de la práctica establecida. Cuando se adopte un diseño o un dispositivo innovador o no probado en el diseño, debería demostrarse mediante un programa comprobante apropiado que se cumplen los requisitos de seguridad; los dispositivos nuevos deberían someterse a las pruebas adecuadas antes de su puesta en servicio.

3.8. Por ejemplo, los sistemas de seguridad pasivos son independientes de sistemas auxiliares externos como los de energía eléctrica, y pueden resultar más simples y fiables que los sistemas activos. No obstante, el comportamiento y la fiabilidad reales de los sistemas pasivos deberían ser demostrados convincentemente mediante adecuados y rigurosos programas de desarrollo, pruebas y análisis.

3.9. Otro ejemplo de aplicación de la moderna tecnología es el uso de los sistemas informatizados de seguridad y control. Los sistemas informatizados tienen ventajas potenciales con respecto a los sistemas clásicos de cableado, entre ellas su mayor funcionalidad, mayor capacidad de prueba y mayor

fiabilidad del equipo físico. Estas ventajas, no obstante, pueden haberse conseguido en algunos casos a expensas de la simplicidad y la transparencia, y por ello deberían efectuarse evaluaciones y pruebas detalladas del comportamiento y de la fiabilidad general de esos sistemas computarizados, incluidos los programas informáticos, en condiciones lo más parecidas posible a las de funcionamiento real. Puede verse más orientación al respecto en la Ref. [6].

REALIZACIÓN DE LA DEFENSA EN PROFUNDIDAD

3.10. El objetivo de la estrategia de defensa en profundidad, según se indica en el párrafo 2.10 de la Ref. [1], es doble: primero, la prevención de accidentes; y segundo, si la prevención falla, detectar y limitar sus posibles consecuencias e impedir que cualquier evolución tienda a situaciones de mayor gravedad.

3.11. La defensa en profundidad se estructura generalmente en cinco niveles. Si fallara un nivel, debería ser compensado o corregido por el nivel siguiente. Los niveles de defensa actúan independientemente de la eficacia de los niveles superiores o inferiores. El objetivo de cada nivel de protección y los medios esenciales para conseguirlo se muestran en el cuadro 1. Las medidas relativas a los tres primeros niveles de defensa deberían considerarse en el marco de la base de diseño, con el fin de asegurar el mantenimiento de la integridad estructural del núcleo y limitar los riesgos potenciales de radiación a miembros de la población. En cambio, las medidas relativas al cuarto nivel de defensa se deberían considerar fuera del marco de la base de diseño con objeto de reducir la probabilidad de condiciones graves de la central y las emisiones radiactivas correspondientes al valor más bajo que pueda razonablemente alcanzarse (ALARA), teniendo en cuenta los factores económicos y sociales.

3.12. Debería darse la máxima prioridad a la prevención de: situaciones que impongan exigencias indebidas a la integridad de las barreras físicas; fallo o derivación de una barrera cuando esté sometida a importantes exigencias; fallo de una barrera como consecuencia del fallo de otra; emisiones considerables de materiales radiactivos.

3.13. El diseño debería ser evaluado de modo que se verifique que se adoptan medidas concretas para asegurar la eficacia de los niveles de defensa 1 a 4.

CUADRO 1. OBJETIVO DE CADA NIVEL DE PROTECCIÓN Y MEDIOS ESENCIALES PARA CONSEGUIRLO

| Nivel | Objetivo | Medios esenciales |
|---------|--|--|
| Nivel 1 | Prevención de funcionamiento anormal y de fallos | Diseño conservador y alta calidad en la construcción y modos de funcionamiento |
| Nivel 2 | Control de funcionamiento anormal y detección de fallos | Sistemas de control, limitación y protección; otros dispositivos de vigilancia |
| Nivel 3 | Control de accidentes en el marco de la base de diseño | Dispositivos protectores técnicos y procedimientos de emergencia |
| Nivel 4 | Control de situaciones graves en la central, incluida la prevención de la progresión de accidentes y la mitigación de las consecuencias de los accidentes graves | Medidas complementarias y gestión de accidentes |
| Nivel 5 | Mitigación de las consecuencias radiológicas de emisiones significativas de materiales radiactivos | Respuesta a emergencias fuera del emplazamiento |

3.14. La evaluación de la efectividad de la defensa en profundidad debería hacerse demostrando, de forma avalada por el análisis completo de seguridad, que se cumple un gran número de requisitos. Esta evaluación debería confirmar que en el correspondiente nivel de defensa en profundidad se responde adecuadamente a los posibles sucesos iniciadores, garantizando que las funciones fundamentales de seguridad se ejecuten y se controle la emisión de materiales radiactivos.

3.15. En el proceso de evaluación se debería prestar especial atención a los peligros internos y externos que pudieran tener el potencial de afectar adversamente y a la vez a más de una barrera, o causar fallos simultáneos en equipos redundantes de los sistemas de seguridad.

3.16. El diseño debería prever dispositivos para la detección del fallo o la derivación de cada nivel de defensa, en la medida aplicable. Se deberían especificar los niveles de defensa requeridos para cada uno de los modos

operacionales (por ejemplo, en ciertos modos de parada se puede permitir una contención abierta y, en tal modo, los niveles de defensa especificados deberían estar listos para actuar en todo momento).

PROTECCIÓN RADIOLÓGICA

3.17. Hay una guía de seguridad específica¹ del OIEA en la que se dan recomendaciones detalladas sobre aspectos del diseño relacionados con la protección radiológica. La entidad diseñadora debería tener presentes estas recomendaciones al diseñar la central. El objeto de la evaluación es demostrar que se cumple el objetivo de protección radiológica establecido en las Nociones fundamentales de seguridad. A continuación se examinan algunos aspectos importantes del diseño de la protección radiológica.

3.18. En lo que atañe a la operación normal y los incidentes operacionales previstos deberían tenerse en cuenta dos objetivos de diseño: (1) mantener las dosis de radiación por debajo de los niveles prescritos; (2) reducir las dosis de radiación al valor más bajo que pueda razonablemente alcanzarse. El cumplimiento del primer objetivo se debería demostrar por comparación de la dosis equivalente calculada con el límite prescrito en la legislación nacional. Los cálculos pertinentes de diseño deberían ser evaluados por la entidad responsable del mismo, para cerciorarse de la corrección de los datos de partida y la validez de la metodología empleada (véase la Sección 4).

3.19. El segundo objetivo de diseño (cumplimiento del principio ALARA) significa que todas las dosis deberían reducirse al valor más bajo que pueda razonablemente alcanzarse, habida cuenta de los factores económicos y sociales. El proceso de optimización de la protección radiológica debería contemplar algún grado de compensación entre inconvenientes (costes) y ventajas (mejoras de la seguridad). En este proceso de optimización, los valores orientativos de la exposición a la radiación y las medidas de diseño conexas se podrían deducir de centrales similares existentes con buen historial de funcionamiento. Al evaluar la seguridad se debería tener en cuenta la experiencia operacional y considerar la posibilidad de adoptar disposiciones o mejoras adicionales de diseño que reduzcan aún más la exposición a la radiación de los trabajadores y los miembros de la población. Tales medidas

¹ Colección Seguridad No. 50-SG-D9. Cuestiones de diseño relacionadas con la protección radiológica en centrales nucleares (1986).

podrían ser tanto directas (mejoras en blindaje) como indirectas (reducción del tiempo de mantenimiento de los equipos).

3.20. Las exposiciones a la radiación deberían mantenerse bajas mediante prácticas tales como la reducción al mínimo de los defectos de vainas, empleo de materiales resistentes a la corrosión, reducción de la formación de isótopos de período largo por corrosión o por activación, existencia de fugas muy bajas en el circuito primario de refrigeración, minimización del mantenimiento en áreas de elevada radiación, y empleo de robots y herramientas de manejo remoto.

3.21. Durante el diseño deberían evaluarse sistemáticamente medidas tales como la suficiencia de espacio para inspecciones y mantenimiento, la adecuación del blindaje para la protección radiológica, y la correcta instalación de los equipos de la central.

3.22. Los responsables del diseño de la central y de la evaluación de la seguridad deberían tener en cuenta también las dosis operacionales durante la clausura final. La selección de los materiales y la suficiencia de espacio de acceso para el desmantelamiento de equipos y utillaje son temas que merecen atención, así como el empleo de pantallas de sacrificio en las estructuras sometidas a altas dosis de radiación, como p. ej. los blindajes de hormigón alrededor de la vasija de presión, para minimizar la cantidad de desechos de alta actividad y facilitar su retirada.

3.23. Al diseñar espacios y equipos tales como las instalaciones de almacenamiento y manipulación de combustible gastado y almacenamiento de desechos radiactivos, se deberían prever disposiciones para minimizar las emisiones que podrían producirse en caso de que fallaran.

3.24. La entidad diseñadora debería demostrar que en el diseño se han tomado medidas suficientes para permitir la adecuada monitorización de la protección radiológica en conformidad con la Ref. [1].

3.25. Debería evaluarse la idoneidad de las disposiciones de diseño para la protección contra situaciones de accidente comparando las emisiones y las dosis calculadas en el análisis de seguridad con los límites especificados o aceptados por el órgano regulador. La mitigación de las consecuencias radiológicas de los accidentes que sobrepasen la base de diseño puede requerir actuaciones especiales en el emplazamiento y en los alrededores de la central (gestión de accidentes y planes de respuesta a emergencias). Al evaluar la seguridad, la entidad diseñadora debería cerciorarse de que en el diseño de la

central se han incorporado debidamente los parámetros relevantes para la gestión de accidentes y la planificación de emergencias.

CLASIFICACIÓN DE LAS ESTRUCTURAS, SISTEMAS Y COMPONENTES ATENDIENDO A LA SEGURIDAD

3.26. Se debería determinar la importancia para la seguridad de todas las estructuras, sistemas y componentes (ESC) y establecer, conforme a lo prescrito en la Ref. [1], un sistema de clasificación atendiendo a la seguridad en el que se precisen con respecto a cada clase:

- Los códigos y normas apropiados y, en consecuencia, las disposiciones que haya que adoptar en el diseño, fabricación, construcción e inspección de cada componente;
- Las características relacionadas con el sistema, como el grado de redundancia y la necesidad de alimentación eléctrica de emergencia y de cualificación para satisfacer las condiciones medioambientales;
- El estado de disponibilidad o de indisponibilidad de los sistemas con respecto a los sucesos iniciadores postulados que hayan de considerarse en el análisis determinista de seguridad;
- Las disposiciones relativas a GC.

3.27. En general, se deberían establecer las siguientes clasificaciones y verificar su adecuación y consistencia:

- Clasificación de los sistemas según la importancia de la función de seguridad afectada;
- Clasificación de los componentes sometidos a presión, según la gravedad de las consecuencias de su fallo, la complejidad mecánica y las presiones nominales;
- Clasificación relativa a la resistencia sísmica, según la necesidad de que la estructura o el componente considerado conserve su integridad y desempeñe su función durante y después de un terremoto, habida cuenta de las réplicas y los consecuentes incrementos del daño;
- Clasificación de los sistemas eléctricos, de instrumentación y control según sus funciones de seguridad tecnológica o de apoyo a la misma; esta clasificación puede ser diferente de la clasificación de otros sistemas de la central a causa de la existencia de sistemas de clasificación, ampliamente empleados, específicos en este campo;
- Clasificación de las disposiciones relativas a GC.

3.28. La adscripción de las ESC a clases de seguridad tecnológica debería hacerse siguiendo los planteamientos nacionales, y se debería dar la importancia adecuada tanto a las consideraciones deterministas y probabilistas como a los sólidos criterios de ingeniería.

3.29. A efectos del análisis determinista de seguridad tecnológica, las funciones de seguridad que se consideren para determinar la conformidad con los criterios de aceptación deberían ser realizadas usando exclusivamente ESC clasificados.

3.30. El análisis probabilista de seguridad (APS) puede utilizarse en la fase de diseño para confirmar que la clasificación de las estructuras, sistemas y componentes es adecuada.

3.31. El fallo de un sistema y/o componente de una clase de seguridad tecnológica no debería causar el fallo de otros sistemas y/o componentes de una clase de seguridad superior. Se debería evaluar la idoneidad del aislamiento y la separación de los sistemas pertenecientes a diferentes clases de seguridad tecnológica que puedan interactuar entre sí.

PROTECCIÓN CONTRA SUCESOS EXTERNOS

3.32. Los sucesos externos han sido ampliamente tratados en varias publicaciones específicas² de la Colección Seguridad del OIEA, que aportan también información sobre la evaluación de la seguridad. No obstante, a continuación se resumen algunas cuestiones fundamentales.

² Colección Seguridad Nos. 50-SG-D5, “Sucesos exteriores imputables al hombre en relación con el diseño de centrales nucleares” (1999); 50-SG-D15, “Seismic Design and Qualification for Nuclear Power Plants” (1992); 50-C-S (Rev.1), “Código sobre la seguridad de las centrales nucleares: Emplazamiento” (1989); 50-SG-S1 (Rev.1), “Terremotos y cuestiones conexas en relación con el emplazamiento de centrales nucleares (1994); 50-SG-S5, “Sucesos exteriores imputables al hombre en relación con el emplazamiento de centrales nucleares” (1982); 50-SG-S7, “Aspectos hidrogeológicos del emplazamiento de centrales nucleares” (1986); 50-SG-S10A, “Inundaciones tipo en el caso de centrales nucleares emplazadas junto a ríos” (1984); 50-SG-S10B, “Inundaciones tipo en el caso de centrales nucleares emplazadas en la costa” (1984); 50-SG-S11A, “Sucesos meteorológicos extremos en relación con el emplazamiento de centrales nucleares, excluidos los ciclones tropicales” (1982); 50-SG-S11B, “Ciclón tropical tipo para centrales nucleares” (1986).

3.33. El conjunto de sucesos que deberían estudiarse al evaluar la seguridad depende del emplazamiento elegido para la central, pero por regla general deberían incluirse:

Los sucesos naturales externos tales como:

- Condiciones meteorológicas extremas;
- Terremotos;
- Inundaciones externas;

Sucesos de origen humano tales como:

- Caída de aeronaves;
- Peligros derivados de las actividades de transporte y las actividades industriales (incendio, explosión, proyectiles, emanación de gases tóxicos).

3.34. La base de diseño debería ser la adecuada para el emplazamiento elegido y fundarse en datos históricos y físicos, así como expresarse por un conjunto de valores seleccionados según la distribución general de probabilidad de cada suceso, en conformidad con umbrales especificados³.

3.35. Cuando no es posible esa evaluación probabilista por falta de confianza en la calidad de los datos, se aplican métodos deterministas apoyados en criterios globales y en sólidos criterios de ingeniería.

3.36. Las estructuras, sistemas y componentes necesarios para desempeñar las funciones básicas de seguridad tecnológica deberían diseñarse de modo que resistan las cargas provocadas por los sucesos base de diseño y sean capaces de realizar sus funciones durante dichos sucesos y después de ellos. Esto debería conseguirse aplicando medidas adecuadas de diseño estructural, redundancia y separación.

³ En algunos Estados Miembros se da por supuesto que el diseño preverá protección contra los sucesos naturales de frecuencia mayor que 10^{-4} por año. Véase también la publicación de la Colección Seguridad No. 50-SG-S1 (Rev.1), “Terremotos y cuestiones conexas en relación con el emplazamiento de centrales nucleares” (1994).

3.37. El riesgo radiológico inherente a los sucesos externos no debería exceder la gama de riesgo radiológico correspondiente al accidente de origen interno. Debería verificarse que los sucesos externos ligeramente más graves que los incluidos en la base de diseño no conducen a un aumento desproporcionado de consecuencias.

3.38. Condiciones meteorológicas extremas: debería definirse un suceso base de diseño para cada una de esas condiciones. Entre ellas se incluirían normalmente las siguientes:

- Cargas por vientos extremos,
- Temperaturas atmosféricas extremas,
- Lluvias y nevadas extremas,
- Temperaturas extremas del agua de refrigeración y formación de hielo,
- Masas extremas de vegetación marina.

3.39. En la base de diseño se deberían tomar en consideración las combinaciones de condiciones meteorológicas extremas que quepa razonablemente suponer que pueden ocurrir al mismo tiempo.

3.40. Debería demostrarse mediante pruebas, experimentos análisis técnicos que las estructuras de la central nuclear resistirán las cargas impuestas por los sucesos externos sin provocar ningún fallo de los elementos necesarios para que la central retorne y se mantenga en un estado en el que todas las funciones básicas de seguridad tecnológica puedan garantizarse durante largo tiempo.

3.41. Debería demostrarse mediante pruebas, experimentos o análisis técnicos que los sistemas de seguridad pueden realizar sus funciones en la gama de condiciones especificadas en la base de diseño (p. ej. temperaturas atmosféricas, niveles y temperaturas del agua del mar).

3.42. Para deducir el nivel sísmico SL-2 aplicable al emplazamiento se debería hacer uso de los resultados de los reconocimientos geológicos de la zona circundante, de los datos históricos de los terremotos ocurridos en ella y de los datos paleosísmicos, según se indica en la publicación de la Colección

Seguridad del OIEA No. 50-SG-S1 (Rev.1)⁴. El terremoto SL-2 debería adoptarse para establecer el terremoto base de diseño de la central nuclear.

3.43. Las estructuras, sistemas y componentes que tengan la misión de parada de la central y su mantenimiento en estado seguro y estable durante un largo período de tiempo, deberían diseñarse de modo que resistan el terremoto base de diseño sin pérdida de funcionalidad.

3.44. La cualificación sísmica debería incluir análisis estructurales, pruebas en la mesa de sacudidas y comparación con la experiencia operacional, según proceda.

3.45. Inundaciones externas: la región en torno al emplazamiento debería ser evaluada para determinar las posibilidades de que ocurra una inundación exterior que pusiera en peligro la central nuclear. Ello debería incluir la posibilidad de inundaciones ocasionadas por precipitaciones intensas, grandes mareas, desbordamiento de ríos, rotura de presas y sus posibles combinaciones.

3.46. Debería preverse la protección necesaria para impedir que ocurra una inundación externa que cause el fallo de equipos de sistemas de seguridad⁵.

3.47. La probabilidad estimada de caída de aeronaves sobre la central debería obtenerse a partir de las estadísticas pertinentes de accidentes de ese tipo, teniendo en cuenta la distancia a aeropuertos, las rutas de vuelo y el número de movimientos de aeronaves de todo tipo en las proximidades del emplazamiento. Las estadísticas sobre caídas de aviones deberían mantenerse al día a lo largo de toda la vida de la central.

⁴ Colección Seguridad No. 50-SG-S1 (Rev.1), “Terremotos y cuestiones conexas en relación con el emplazamiento de centrales nucleares” (1994). Esta guía de seguridad define también un segundo nivel sísmico (SL-1), que corresponde a un terremoto llamado frecuentemente terremoto base operacional, que quepa prever razonablemente que ocurra en el emplazamiento de la central durante su vida operacional. Puede corresponder también al terremoto de nivel de inspección, después del cual la seguridad de la central es revaluada antes de continuar operando.

⁵ Para más información sobre inundaciones externas véanse las publicaciones de la Colección Seguridad Nos. 50-SG-S10A, “Inundaciones tipo en el caso de centrales nucleares emplazadas junto a ríos” (1984); y 50-SG-S10B, “Inundaciones tipo en el caso de centrales nucleares emplazadas en la costa” (1984).

3.48. Si la probabilidad estimada de caída de aviones es mayor que el valor aceptable, la protección debería incluir el refuerzo de las estructuras que alberguen los sistemas y componentes importantes para la seguridad, y la separación y segregación de los conjuntos redundantes de equipos, de tal modo que el impacto de una aeronave o el subsiguiente incendio de su combustible no los dañe a todos. La protección contra dichas caídas debería centrarse en los elementos necesarios para llevar de nuevo la central a una situación segura y mantenerla en un estado en el que se puedan garantizar todas las funciones de seguridad⁶.

3.49. En cuanto a los peligros provenientes del transporte y las actividades industriales, se deberían determinar y especificar los correspondientes sucesos base de diseño, los transportes de materiales peligrosos en las cercanías del emplazamiento⁷ y las actividades industriales que causen incendio, explosión, proyectiles o emanación de gases tóxicos, y afecten a la seguridad de la central nuclear.

PROTECCIÓN CONTRA PELIGROS INTERIORES

3.50. Los peligros internos son ampliamente tratados en determinadas publicaciones de la Colección Seguridad del OIEA⁸, que proporcionan también orientación sobre la evaluación de la seguridad. En esta sección se resumen algunos aspectos esenciales.

3.51. En el diseño se deberían tener en cuenta las cargas y las condiciones ambientales específicas (temperatura, presión, humedad, radiación) impuestas a las estructuras o los componentes por sucesos de origen interno, tales como:

⁶ Para más información sobre el examen de las caídas de aviones véase la publicación de la Colección Seguridad No. 50-SG-S5, “Sucesos exteriores imputables al hombre en relación con el emplazamiento de centrales nucleares” (1982), que será reemplazada por una guía sobre sucesos exteriores de origen humano en la evaluación del emplazamiento de las centrales nucleares, que se publicará más adelante.

⁷ Para más información sobre el examen de los peligros provenientes de las actividades industriales, véase la publicación de la Colección Seguridad No. 50-SG-S5 (que se reemplazará como indica la nota 6).

⁸ Colección de Normas de Seguridad No. NS-R-1, “Seguridad de las centrales nucleares: Diseño” (2004); Colección Seguridad No. 50-SG-D2, “Protección contra incendios en centrales nucleares” (1996); 50-SG-D4, “Protección contra proyectiles de procedencia interior y sus efectos secundarios en centrales nucleares” (1981).

- Efecto de látigo en las tuberías;
- Fuerzas de impacto de fluidos;
- Inundación interna y rociado a causa de fugas o roturas de tuberías, bombas o válvulas;
- proyectiles internos;
- Caída de objetos pesados;
- Explosión interna;
- Incendio.

3.52. Debería demostrarse que se han considerado suficientemente en el diseño los efectos de fallos de tuberías, tales como fuerzas de impacto de chorros, efecto de látigo, fuerzas de reacción, fuerzas de ondas de presión, aumentos de presión, humedad, temperatura y radiación sobre los componentes, las estructuras de edificios, los equipos eléctricos y de instrumentación y control. Concretamente, debería probarse que:

- Se han tenido en cuenta las fuerzas de reacción al diseñar los equipos clasificados como de seguridad tecnológica, los soportes de estos equipos y las estructuras de edificios conexas;
- Los componentes importantes para la seguridad y sus mecanismos internos se han diseñado tomando en consideración las fuerzas verosímiles de ondas de presión y las causadas por la circulación de fluidos;
- En los edificios importantes para la seguridad, como el de contención, se ha tenido en cuenta el aumento de la presión;
- Los equipos eléctricos y de instrumentación y control importantes para la seguridad se han diseñado para soportar niveles extremos de temperatura, humedad y radiación en el caso de las fugas y roturas postuladas.

3.53. En cuanto a las inundaciones internas, debería analizarse la inundación de los principales edificios de la central y considerarse las siguientes causas potenciales iniciadoras de inundación: fugas y roturas de componentes que mantengan la presión, inundación por agua procedente de edificios próximos, actuación espuria del sistema contra incendios, rebosamiento de depósitos y fallos de dispositivos de aislamiento.

3.54. Las estructuras, sistemas y componentes importantes para la seguridad deberían situarse a una altura superior al nivel esperado de inundación o estar suficientemente protegidos.

3.55. Pueden generarse proyectiles internos por avería de componentes rotativos, como las turbinas, o por fallo de componentes sometidos a presión. Deberían considerarse las trayectorias preferentes de vuelo de los posibles proyectiles de las turbinas y tenerlas en cuenta para la orientación de la turbina con respecto a los edificios clasificados como relevantes para la seguridad, a menos que se pueda demostrar que no es probable que los eventuales proyectiles causen deterioro significativo a las ESC importantes para dicha seguridad. Del mismo modo, en la medida de lo posible, debería restringirse la ubicación de componentes muy energéticos en los edificios clasificados como relevantes para la seguridad.

3.56. En el diseño debería considerarse la avería de mecanismos elevadores cuando la caída de las correspondientes cargas pueda dar lugar a exposición a la radiación dentro o fuera de la central, o cuando pueda causar daño en un sistema importante para la seguridad.

CONFORMIDAD CON LOS CÓDIGOS, NORMAS Y GUÍAS APLICABLES

3.57. Para garantizar la seguridad de la central nuclear, al diseñar las ESC se debería tener presente su importancia al respecto. El diseño de las ESC que sean importantes para la seguridad debería llevarse a cabo con arreglo a los requisitos correspondientes a la importancia de las funciones de seguridad tecnológica que vayan a cumplir. La clase asignada a las ESC sirve de base para determinar los códigos y las normas que se aplicarán a su diseño.

3.58. En general, la entidad explotadora especifica una lista de códigos y normas de diseño como requisitos que impone la compañía eléctrica, o directamente el órgano regulador. No obstante, estos códigos y normas deberían ser examinados y analizados con objeto de evaluar su aplicabilidad, adecuación y suficiencia a fin de diseñar las ESC importantes para la seguridad conforme al estado actual de la tecnología y los conocimientos. Si algunos de los códigos y normas resultan insuficientes para garantizar la calidad de las ESC que corresponda a la importancia de la función de seguridad que éstas tengan que cumplir, tales códigos y normas deberían complementarse o modificarse en la medida necesaria para asegurar la calidad apropiada de las ESC.

CARGAS Y COMBINACIÓN DE CARGAS

3.59. Las estructuras y componentes clasificados como relevantes para la seguridad tecnológica deberían diseñarse de modo que resistan todas las cargas importantes que surjan en los estados operacionales y en los accidentes base de diseño, incluidos los resultantes de peligros de origen interno y externo.

3.60. Por tanto, una parte significativa de la evaluación de la seguridad consiste en:

- Determinar, para cada estructura o componente clasificado como importante para la seguridad, las cargas y sus combinaciones;
- Determinar, para cada carga y combinación de cargas, la frecuencia con que se prevé que ocurran;
- Evaluar las tensiones y deformaciones en las estructuras y componentes clasificados por su importancia en materia de seguridad, para las cargas y sus combinaciones que se hayan determinado;
- Evaluar el deterioro en cada caso particular y el deterioro acumulado en la estructura o componente, tomando en consideración todos los deterioros relevantes (p. ej. fluencia, fatiga, envejecimiento) y sus interacciones potenciales.

3.61. El conjunto de cargas y sus combinaciones debería ser completo y coherente con los supuestos del análisis de seguridad. Su frecuencia probable, junto con el número total de transitorios previstos en la vida de la central, deberían ser evaluados a la luz de los registros históricos, la experiencia operacional, los requisitos impuestos por la compañía eléctrica y las características del emplazamiento, según proceda.

3.62. Además de todas las magnitudes físicas pertinentes, al evaluar las tensiones y deformaciones se deberían tener en cuenta las condiciones ambientales resultantes de cada carga, cada combinación de cargas, y las condiciones apropiadas de contorno. Los criterios de aceptación deberían reflejar adecuadamente la prevención de fallos consecutivos de las estructuras o componentes necesarios para mitigar las consecuencias de los riesgos relacionados con las cargas supuestas.

SELECCIÓN DE MATERIALES

3.63. Los materiales deberían cumplir las normas y requisitos aplicables a su diseño y fabricación. La vida de diseño de los materiales debería determinarse considerando los efectos de las condiciones operacionales (p. ej. el ambiente radiológico y químico, o las cargas ocasionales y las periódicas). Además, deberían considerarse los efectos de los accidentes base de diseño sobre sus características y comportamiento.

3.64. Cuando se trate de materiales cuya idoneidad se demuestre mediante pruebas, todos los resultados de las pruebas deberían quedar documentados.

3.65. Los materiales en contacto con efluentes radiactivos deberían tener propiedades anticorrosivas contra los mecanismos de corrosión que interesen y ser resistentes a las reacciones químicas en las condiciones operacionales. Debería evitarse, en la medida de lo posible, el contacto del acero al carbono con productos radiactivos. Los materiales poliméricos deberían ser resistentes a la radiación si son empleados en sistemas que contengan efluentes radiactivos.

3.66. El acero inoxidable o las aleaciones de níquel, los materiales de los tubos del generador de vapor, las tuberías principales y los plaqueados en contacto con el refrigerante del reactor deberían tener propiedades anticorrosivas adecuadas. Los elementos de bajo punto de fusión como el plomo, antimonio, cadmio, indio, mercurio, cinc, bismuto, estaño, y sus aleaciones, no deberían entrar en contacto con los componentes del circuito primario de refrigeración del reactor, ni con los del circuito secundario fabricados con acero inoxidable o con aleaciones de níquel. Debería evitarse las aleaciones de cojinetes que contengan elementos de bajo punto de fusión que contaminen el sistema de agua de alimentación. Con el fin de reducir las dosis operacionales debería minimizarse, en la medida de lo posible, el contenido de cobalto de los materiales que estén en contacto con el refrigerante del reactor, y deberían justificarse los casos excepcionales de empleo de aleaciones de cobalto. Debería evaluarse el escape al refrigerante del reactor de níquel de los materiales que estén en contacto con él.

3.67. El diseño debería garantizar el control de los halógenos presentes en los materiales que estén en contacto con componentes de acero inoxidable (p. ej. en los aislamientos de tuberías), con el fin de evitar grietas por corrosión intergranular bajo tensión.

3.68. Respecto de los materiales ferríticos de la barrera de presión del refrigerante del reactor, debería probarse la resistencia, en condiciones de alta presión y temperatura, a la propagación rápida de fracturas, así como la resistencia a la fatiga. Todas las soldaduras en acero inoxidable deberían ser resistentes a la corrosión intergranular, y debería controlarse el contenido de ferrita delta con el fin de minimizar la formación de microgrietas durante el proceso de soldadura de aceros inoxidables austeníticos.

3.69. Debería prestarse especial atención a la compatibilidad de los materiales que se utilicen en lo que respecta a la química del agua, con el fin de evitar los fenómenos de corrosión. En todos los equipos expuestos a vapor húmedo, o a fluidos que puedan causar erosión grave, se deberían emplear materiales resistentes a la corrosión y la erosión. Se puede emplear una aleación de acero baja en cromo ($\text{Cr} > 0,5\%$).

3.70. Los materiales de aislamiento se deberían seleccionar de modo que se minimicen sus efectos perjudiciales (p. ej. dosis al personal durante las paradas, obstrucción de los sumideros en los accidentes). Debería comprobarse, para los materiales de aislamiento seleccionados, el comportamiento obstructivo de los fragmentos que generen por el impacto de chorros en el curso de accidentes.

3.71. Al seleccionar los materiales empleados en ambientes de radiación se debería considerar el efecto de ésta sobre las propiedades de los materiales. Por ejemplo, las fibras ópticas pueden resultar dañadas cuando se exponen a campos neutrónicos. Ello tendría efectos perjudiciales sobre las funciones de seguridad para las que sirvan esos cables (generalmente, los sistemas informatizados de protección y control).

3.72. A causa de la activación por la radiación, la selección de los materiales empleados en un ambiente de radiactividad podría tener un efecto significativo durante la clausura. Estos aspectos deberían ser evaluados en la fase de diseño.

EVALUACIÓN DEL FALLO ÚNICO Y REDUNDANCIA/ INDEPENDENCIA

3.73. La aplicación del criterio de fallo único, según se expone en la Ref. [1] y se explica más a fondo en la publicación de la Colección Seguridad No. 50-P-1 del OIEA “Application of the Single Failure Criterion” [7], sirve como garantía de que no se excedan las funciones de seguridad tecnológica requeridas a raíz de

un suceso iniciador postulado (SIP)⁹ considerado en el marco de la base de diseño ni excedan los límites especificados en la base de diseño para este suceso, en el supuesto de un fallo único en cualquier componente del grupo de seguridad tecnológica¹⁰.

3.74. Al aplicar el criterio de fallo único, debería determinarse cualquier fallo que pueda ocurrir como consecuencia del SIP e incluirse en la base de partida del análisis según el criterio del fallo único.

3.75. Por cada uno de los SIP definidos para la central debería especificarse el grupo de seguridad tecnológica que cumple el conjunto de funciones de seguridad requeridas. En el análisis del fallo único se deberían precisar todos los modos de fallo de los componentes del grupo de seguridad, incluso los de todos los sistemas de apoyo necesarios. Además, se deberían especificar todos los fallos que puedan ocurrir como consecuencia del fallo único, e incluirse en el análisis junto al fallo único. Ello debería incluir los fallos que puedan ocurrir en un componente a causa del fallo de un sistema de apoyo como el de suministro eléctrico o el de agua de refrigeración. No obstante, en ningún caso debería suponerse en el análisis del fallo único que ocurra más de un solo fallo aleatorio.

3.76. El criterio de fallo único debería aplicarse cuando el grupo de seguridad tecnológica se encuentre en la configuración más desfavorable. En particular, si el funcionamiento de la central permite poner fuera de servicio, por un tiempo considerable, equipos con fines de mantenimiento, prueba, inspección o reparación, en momentos en que podría haber necesidad de disponer del grupo de seguridad, debería suponerse que el fallo único tiene lugar en una ocasión en que sean máximos los equipos fuera de servicio permitidos por las reglas de operación o las especificaciones técnicas de la central. A pesar de ello, según se establece en la Ref. [1], párrafo 5.38, el incumplimiento del criterio de fallo único puede estar justificado en el caso de paradas de duración limitada especificadas. En todos estos casos debería presentarse una justificación,

⁹ En el apéndice I de la publicación de la Colección de Normas de Seguridad del OIEA, No. NS-R-1, “Seguridad de las Centrales Nucleares: Diseño”, figura la definición y una explicación más detallada de los SIP.

¹⁰ Grupo de seguridad tecnológica se define como: “Conjunto de componentes de equipo destinados a realizar todas las funciones requeridas si se produce un suceso iniciador postulado determinado para asegurar que no se rebasen los límites especificados en la base de diseño correspondientes a los incidentes operacionales previstos y a los accidentes base de diseño.”

acompañada de la forma de deducir los tiempos de interrupción permitidos (véase el párrafo 5.42 de la Ref. [1]).

3.77. Los fallos que deberían considerarse en el análisis del fallo único incluyen por lo general los de componentes activos (tales como el fallo de las válvulas en su apertura o cierre, según se necesite, y el fallo de las bombas en su arranque y funcionamiento) y los de componentes pasivos (tales como el fallo de tuberías de un sistema de seguridad) que tengan una amplia serie de probabilidades de ocurrir. En el análisis del fallo único puede no considerarse el supuesto de fallo de un componente pasivo proyectado, fabricado, inspeccionado y mantenido en servicio con un nivel de calidad extremadamente alto, siempre que no sea afectado por el SIP. No obstante, debe presentarse una justificación relativa a cada modo de fallo de un componente que sea omitido en el análisis del fallo único. En el caso de un componente pasivo, se debería tener en cuenta a este respecto el período total de tiempo durante el que se prevé que el componente funcionará después de ocurrir el SIP. En la práctica, los fallos únicos de los componentes pasivos se suelen considerar sólo en el largo plazo (p. ej. 24 horas) después de ocurrir un SIP, a causa de las normas de calidad aplicadas.

3.78. El análisis del fallo único puede no requerir la consideración de los SIP que ocurran con muy baja frecuencia o no requerir el estudio de las consecuencias de un SIP que sea muy improbable.

3.79. La publicación de Requisitos de seguridad titulada “Seguridad de las centrales nucleares: Diseño” [1] especifica que las siguientes funciones de seguridad deberían ser realizadas por los sistemas propios de la central en el supuesto de un fallo único:

- Parada rápida del reactor,
- Eliminación del calor residual del núcleo,
- Refrigeración de emergencia del núcleo,
- Aislamiento de la contención,
- Eliminación de calor de la contención,
- Control y limpieza de la atmósfera de la contención.

3.80. En la práctica, se pueden prever niveles de redundancia mayores que los que se deriven del criterio de fallo único, para conseguir una fiabilidad suficientemente alta o por razones operacionales, por ejemplo (i) poder retirar del servicio equipos con fines de mantenimiento o de reparación en una oportunidad en la cual se necesite que el grupo de seguridad esté disponible; (ii) poder realizar pruebas de vigilancia; o (iii) reducir problemas de

disposición en la central. Esto significa que un SIP, en sí mismo, no es un accidente. Es sólo el suceso que inicia una secuencia que da lugar a un incidente operacional, un accidente base de diseño, o un accidente grave, según los fallos adicionales que se produzcan. Son ejemplos típicos: los fallos de equipos (incluida la rotura de tuberías), los errores humanos, los sucesos de origen humano y los sucesos naturales. Las conexiones entre conjuntos de equipo deben diseñarse de tal forma que un fallo único no pueda afectar a más de un conjunto. Los conjuntos redundantes deberían separarse por medio de barreras o distanciándolos entre sí, con el fin de asegurarse de que un peligro interno no puede originar la pérdida de más de uno de ellos.

DIVERSIDAD

3.81. La fiabilidad de un sistema de seguridad tecnológica en el que se incorpora redundancia empleando componentes similares estará limitada por un fallo de causa común, que puede conducir al fallo simultáneo de varios de los componentes redundantes. Para evitar esta limitación, se puede aumentar la fiabilidad recurriendo a la incorporación de diversidad (véase el apéndice II de la Ref. [1]).

3.82. El grado de diversidad incorporado puede ser diferente según la solución de diseño que se adopte. Es alto si los sistemas diversos llevan a cabo la misma función de seguridad de maneras físicamente diferentes y emplean tipos de equipo diferentes. Por ejemplo, la parada de un reactor en la que los sistemas diversos actúan dejando caer un absorbente neutrónico sólido en el núcleo e inyectando una solución de absorbente neutrónico en el refrigerante del circuito primario. Ahora bien, el grado es menor si los sistemas diversos llevan a cabo la función de seguridad tecnológica de la misma manera, utilizando componentes de diferente tipo. Por ejemplo, un sistema de agua de alimentación de emergencia en el que las bombas y las válvulas de las distintas partes del sistema son de un tipo diferente o son suministradas por fabricantes diferentes.

3.83. Cuando se requiera una fiabilidad muy alta, deberían incorporarse medios diversificados para llevar a cabo la función de seguridad. El grado de diversidad debería ser proporcionado a la fiabilidad que se exija a esos medios para cumplir dicha función.

3.84. Cuando se prevea la diversidad en los sistemas de seguridad, debería demostrarse que se satisface la fiabilidad requerida de esos sistemas. A este

respecto, debería considerarse adecuadamente la existencia potencial de vulnerabilidades comunes, como los fallos de causa común. Por ejemplo, puede tratarse de una deficiencia de diseño, una deficiencia de fabricación, un error operacional o de mantenimiento, un fenómeno natural, un suceso de origen humano, o un efecto en cascada fortuito resultante de cualquier otra operación o fallo en la central.

3.85. Debería reconocerse que la introducción de diversidad aumenta la complejidad y los costes de la central y que origina dificultades y costes de funcionamiento y mantenimiento. Ello se debería tener en cuenta en el proceso de diseño y se debería alcanzar un punto de equilibrio entre los aumentos de fiabilidad de los sistemas de seguridad y la complejidad adicional introducida.

PRUEBAS, MANTENIMIENTO, REPARACIÓN, INSPECCIONES Y MONITORIZACIÓN EN SERVICIO DE LOS ELEMENTOS IMPORTANTES PARA LA SEGURIDAD

3.86. Las ESC importantes para la seguridad tecnológica, con las excepciones que luego se indicarán, deberían diseñarse para ser probadas, mantenidas, reparadas e inspeccionadas o monitorizadas periódicamente con objeto de evaluar su integridad y capacidad funcional durante la vida de la central nuclear. La periodicidad puede variar de días a años, según la naturaleza del componente. Obviamente, cuanto mayor sea la frecuencia del mantenimiento con la central en marcha menor será la necesidad de efectuarlo con la central parada. El diseño debería contemplar la realización de estas actividades siguiendo estándares acordes con la importancia de las funciones de seguridad que se hayan de cumplir, sin exposición indebida del personal del emplazamiento a la radiación.

3.87. Si no es factible diseñar las ESC importantes para la seguridad de modo que se puedan probar, inspeccionar o monitorizar en el grado deseable, deberían adoptarse precauciones adecuadas de seguridad para compensar posibles fallos no detectados.

3.88. Los diseñadores deberían preparar guías específicas de diseño destinadas a garantizar la accesibilidad para la inspección y pruebas. Los temas esenciales que deberían evaluarse a este respecto son, entre otros: disponibilidad de suficiente espacio alrededor de los componentes; reducción de los campos de radiación alrededor de los componentes mediante disminución del depósito de material radiactivo en el interior de la barrera primaria de presión o del

blindaje; reducción de fugas de agua del primario; previsión de pasarelas de acceso, fijas o desmontables, y de puntos de amarre en las estructuras para el movimiento de componentes; finalmente, instalación de los componentes en posición conveniente para facilitar la inspección y pruebas.

3.89. Cuando la accesibilidad resulte impracticable, el diseño puede prever carriles permanentes y espacio suficiente para posicionar y manejar adecuadamente, mediante dispositivos de control remoto, los equipos de inspección. Al evaluar la seguridad se debería comprobar que tales posibilidades han sido consideradas.

3.90. Aunque la adopción de disposiciones como las que acaban de ser esbozadas tiende a resolver, en la mayoría de los casos, el conflicto entre la necesidad de mantener bajas las dosis operacionales y la de realizar pruebas e inspecciones periódicas, en algunas situaciones complejas se debería hacer un estudio detallado de la solución correcta de transacción entre estas dos necesidades, haciendo uso del análisis de seguridad en la etapa de diseño.

CUALIFICACIÓN DE EQUIPOS

3.91. La cualificación de equipos se aplica principalmente a los sistemas de seguridad que deben realizar sus funciones en situaciones de accidente.

3.92. Las condiciones en las que se prevé que los equipos realicen una función de seguridad pueden diferir de aquellas a las que estén normalmente expuestos y su comportamiento puede ser afectado por el envejecimiento o por las condiciones de servicio conforme prosigue la central su funcionamiento. Las condiciones ambientales en las que se prevé que operen los equipos se deberían definir como parte del proceso de diseño. Entre ellas deberían figurar las condiciones supuestas en una amplia gama de accidentes, en particular los valores extremos de temperatura, presión, radiación, vibración y humedad, así como impacto de chorros de fluidos.

3.93. La capacidad de funcionamiento requerida debería mantenerse a lo largo de la vida de la central. En el diseño debería prestarse atención a los efectos del envejecimiento en relación con los fallos de causa común. El envejecimiento debería tenerse en cuenta en el diseño definiendo adecuadamente las condiciones ambientales, las condiciones de los procesos, los ciclos de trabajo, los programas de mantenimiento, la vida de servicio, los programas de pruebas tipo, las partes sustituibles y los intervalos de sustitución.

3.94. Debería confirmarse mediante un procedimiento de cualificación que los equipos son capaces de realizar a lo largo de su vida operacional sus funciones de seguridad en las condiciones ambientales existentes en el momento en que son necesarios (efectos dinámicos, temperatura, presión, impacto de chorros, radiación, humedad). Estas condiciones ambientales deberían incluir las variaciones prescritas en situaciones de funcionamiento normal, incidente operacional previsto y accidente. En los casos en que los equipos estén expuestos a sucesos naturales externos y se prevea que realicen una función de seguridad durante o a continuación de uno de ellos, el programa de cualificación debería reproducir las condiciones impuestas al equipo por los fenómenos naturales.

3.95. Además, se deberían incluir en el programa de cualificación todas las situaciones ambientales inusuales que quepa razonablemente prever y puedan presentarse en condiciones operacionales específicas, por ejemplo durante la comprobación periódica de la tasa de fugas de la contención. En la medida de lo posible, debería demostrarse con razonable confianza, mediante pruebas, experimentos o análisis técnicos, que los equipos que se prevé hayan de funcionar en el curso de accidentes graves son capaces de cumplir su objetivo de diseño en las condiciones propias de esos accidentes.

3.96. Es preferible que la cualificación se realice mediante pruebas en equipos prototipo (pruebas tipo). Ello no siempre es completamente factible para los ensayos vibratorios de grandes componentes o para el envejecimiento de equipos. En tales casos debería recurrirse a la extrapolación del comportamiento de equipos en situaciones similares, análisis, o pruebas acompañadas de análisis.

MECANISMOS DE ENVEJECIMIENTO Y DE DESGASTE

3.97. La evaluación de la seguridad tecnológica debería tener en cuenta el hecho de que los sistemas y componentes de la central están expuestos en diversa medida a los efectos del envejecimiento. Algunos de estos efectos son bien conocidos y pueden tomarse medidas para contrarrestarlos. Otros, según indica la experiencia, no son previsibles, y para descubrir las posibilidades de que ocurra deberían emplearse programas adecuados de prueba, inspección y vigilancia. En la fase de diseño debería prepararse un programa completo de actuaciones que abarque toda la vida de la central y establecerse los prerequisites técnicos para su aplicación. Un buen procedimiento para determinar si los mecanismos de envejecimiento y desgaste han sido

correctamente tenidos en cuenta, y para detectar otros problemas no previstos, es el de las revisiones periódicas de seguridad.

3.98. La vasija debería diseñarse teniendo en cuenta la fragilización debida a la acción del flujo de neutrones rápidos procedente del núcleo durante toda la vida de la central. La protección estriba en un buen diseño para prevenir la fragilización excesiva, en facilitar la detección de la fragilización y en posibles medidas reparadoras. Este problema afecta más a los reactores de agua a presión que a los de agua en ebullición, a causa de los efectos dimensionales y/o neutrónicos. Las partes soldadas son afectadas más fácilmente por la fragilización, ya que las impurezas introducidas en el proceso de soldadura pueden hacer que la zona soldada sea particularmente sensible a la irradiación neutrónica. La zona afectada por el calor alrededor de una soldadura es frecuentemente el lugar donde se acumulan microgrietas y tensiones residuales, lo que sensibiliza aún más esta región a los efectos de fragilización.

3.99. Debería evitarse, en todo lo posible, la presencia de soldaduras a la altura de la región activa del combustible.

3.100. Debería prestarse la adecuada atención a limitar y monitorizar la fragilización de la vasija. Con esta finalidad, la fluencia neutrónica (el flujo neutrónico integrado a lo largo de la vida de la central) debería mantenerse por debajo de un nivel que asegure la conservación de las propiedades mecánicas, aun teniendo en cuenta las incertidumbres. Debería asegurarse la existencia de programas de vigilancia adecuados mediante el empleo de probetas de soldadura de la vasija y de medidores de fluencia neutrónica sometidos al flujo neutrónico en condiciones representativas. Otro proceso importante de envejecimiento es el que afecta a los tubos de los generadores de vapor de los reactores de agua a presión. La degradación de los tubos tiene lugar por muchas causas y debería ser vigilada con el fin de tomar medidas preventivas o reparadoras, tales como cambios en la química del agua y reparación o taponado de tubos antes de que tengan fugas o fallen. El diseño debería facilitar la vigilancia, reparación y sustitución del generador de vapor mediante un acceso adecuado, carriles y puntos de amarre.

3.101. A continuación figura una lista de otros posibles efectos de envejecimiento que la experiencia operacional aconseja tener en cuenta. El diseño de la central debería prever la forma de eliminar los problemas ya en la fase de diseño o incluir los medios para su oportuna detección en estado incipiente y la aplicación de las medidas correctoras apropiadas:

- Hidruración y fragilización de canales en reactores de canales a presión, lo cual puede dar lugar a la sustitución de canales;
- Corrosión de componentes internos de la vasija, vibraciones y roturas, cuya posibilidad de producirse debería ser detectable por medios adecuados de vigilancia;
- Agrietamiento de toberas de refrigeración del núcleo y de componentes internos del reactor;
- Transitorios de temperatura y presión en toberas y tuberías;
- Mezclado térmico en zonas de uniones de tubos;
- Estratificación térmica en tuberías y erosión de tuberías en componentes, que deberían ser detectables mediante inspecciones periódicas, facilitadas por disposiciones adecuadas en el diseño;
- Envejecimiento de los materiales orgánicos de aislamiento de cables o de sellado de la ventilación, que debería preverse en el diseño para permitir su detección y posible sustitución.

INTERFAZ HOMBRE-MÁQUINA Y APLICACIÓN DE LA INGENIERÍA DE FACTORES HUMANOS

3.102. En determinadas guías de seguridad del OIEA¹¹ se dan recomendaciones detalladas sobre la aplicación de los principios relativos a factores humanos en el diseño. En esta sección se resumen algunos de los aspectos fundamentales.

3.103. El diseño de la central debería facilitar el trabajo de los operadores y promover un comportamiento humano óptimo en los estados operacionales y en los accidentes. Ello debería realizarse poniendo cuidadosa atención en el diseño de la central, el establecimiento de los procedimientos de operación y la capacitación de todo el personal operador.

3.104. Los factores humanos y la interfaz hombre-máquina deberían recibir una atención sistemática en el diseño desde las primeras etapas de su elaboración y a lo largo de todo el proceso.

¹¹ Colección Seguridad No. 50-SG-D3, “Sistema de protección y dispositivos conexos en centrales nucleares” (1981); 50-SG-D8, “Sistemas e instrumentación y control de centrales nucleares relacionados con la seguridad” (1985); y Colección de Normas de Seguridad No. NS-G-2.2, “Límites y condiciones operacionales y procedimientos de operación en las centrales nucleares” (en preparación).

3.105. Se deberían precisar las medidas de seguridad encomendadas al personal operador. Ello suele incluir las medidas de seguridad llevadas a cabo por los operadores que sean responsables de monitorizar y controlar la central, hacer frente a fallos y realizar actividades de mantenimiento, pruebas y calibración.

3.106. Debería efectuarse un análisis de tareas referido a las medidas de seguridad tecnológica, con objeto de evaluar las exigencias que pesarán sobre los operadores en cuanto a la toma de decisiones y la ejecución de las medidas. Los resultados del análisis de tareas deberían ser determinantes para las especificaciones de diseño de la interfaz hombre-máquina, la información y los controles que se han de prever, la preparación de los procedimientos operacionales, y los programas de capacitación.

3.107. La información y los controles previstos deberían ser suficientes para que los operadores puedan:

- Ejecutar las operaciones normales tales como cambiar el nivel de potencia del reactor;
- Evaluar rápidamente el estado general de la central en funcionamiento normal, en caso de incidentes operacionales previstos y en condiciones de accidente;
- Monitorizar el estado del reactor y de todos los equipos de la central;
- Detectar los cambios de estado de la central que sean importantes para la seguridad tecnológica;
- Confirmar que se ejecutan las medidas automáticas de seguridad previstas en el diseño;
- Identificar todas las medidas prescritas y ejecutarlas.

3.108. El operador debería recibir suficiente información sobre los parámetros relacionados con cada uno de los sistemas y equipos de la central para confirmar que las medidas de seguridad requeridas han sido cumplidas e informar de que dichas medidas han producido los efectos deseados.

3.109. Las zonas y los ambientes de trabajo del personal del emplazamiento deberían diseñarse con arreglo a principios ergonómicos que faciliten la realización de las tareas de forma fiable y eficiente. Esto debería también aplicarse al diseño de la sala de control central, la sala de control de emergencias, y todo puesto de control local en la central y en cualquier zona donde se lleven a cabo tareas de mantenimiento y pruebas. Debería prestarse

especial atención a los sistemas de visualización, la configuración de paneles y los espacios de acceso para las actividades de mantenimiento y pruebas.

3.110. La interfaz hombre-máquina debería diseñarse de modo que proporcione a los operadores información completa pero fácilmente manejable para tomar decisiones y medidas correctas.

3.111. La necesidad de que un operador tenga que intervenir con premura debería reducirse al mínimo. Debería preverse la automatización de todas las acciones que se hayan de ejecutar en tiempos cortos. Los márgenes de tiempo se deberían evaluar sobre la base de la estimación óptima justificable.

3.112. Con respecto a todas las acciones del operador, el análisis de tareas debería demostrar que el operador tiene tiempo suficiente para decidir y actuar; que la información necesaria para la decisión se presenta de manera sencilla y sin ambigüedad; y que el ambiente físico después del suceso es aceptable en la sala de control o en el puesto de control suplementario, y en el acceso a ese puesto de control.

3.113. El diseño de una central debería ser tolerante con los errores humanos. En la medida de lo posible, cualquier acción humana incorrecta debería quedar invalidada. Con este fin, debería sopesarse cuidadosamente la atribución de prioridad a la acción del operador o la actuación de un sistema de seguridad. Por un lado, no debería permitirse al operador invalidar la actuación del sistema de protección del reactor mientras rijan los criterios de iniciación de la actuación. Por otro lado, hay situaciones en las que son necesarias las intervenciones del operador en el sistema de protección. Son ejemplo de ello las derivaciones manuales para realizar pruebas o la adopción de criterios de actuación con el fin de modificar el estado operacional. Además, el operador debería tener una última posibilidad de intervenir en el sistema de protección, bajo estricto control administrativo, para hacer frente a accidentes que sobrepasen la base de diseño, en caso de grandes fallos en el sistema de protección del reactor.

3.114. Debería disponerse de procedimientos escritos para todas las actividades llevadas a cabo por el personal operador, incluido el funcionamiento en condiciones normales de la central y la recuperación después de sucesos anómalos y accidentes, incluidos los accidentes graves. Los procedimientos de respuesta a los incidentes anormales y los accidentes deberían orientarse preferentemente hacia los síntomas. Los procedimientos

deberían ser validados mediante visitas de inspección y el empleo de maquetas y de simuladores, según proceda.

3.115. Deberían preverse sistemas de comunicación suficientes y fiables para permitir la transmisión de información e instrucciones entre los distintos lugares en apoyo de las acciones del operador, tanto en fase de funcionamiento normal como de recuperación después de accidentes. Ello incluiría las comunicaciones entre las salas de control principal o de emergencias y el personal de operación que pueda tener que realizar en lugares remotos acciones que afecten al estado de la central; así como la comunicación con entidades de fuera del emplazamiento en situaciones de accidente. Los sistemas de comunicación deberían estar disponibles en todas las situaciones de accidente que lo requieran y no deberían interferir con el sistema de protección de la central.

3.116. La disposición e identificación de los controles ubicados en lugares remotos debería diseñarse teniendo en cuenta los factores humanos, de modo que se reduzca la posibilidad de error del operador al seleccionar los controles situados en tales lugares.

INTERACCIONES ENTRE SISTEMAS

3.117. Se deberían evaluar cuidadosamente las posibles interacciones entre los sistemas de una misma central, entre una central e instalaciones externas, y entre diferentes centrales en un mismo emplazamiento. Las interacciones de los sistemas deberían ser consideradas en todos los estados operacionales de la central, incluidos los peligros provenientes del exterior y accidentes graves.

3.118. El análisis debería tomar en consideración no sólo las interconexiones físicas sino también el efecto del funcionamiento, mantenimiento, función defectuosa o fallo de los sistemas sobre el ambiente físico de los demás sistemas importantes para la seguridad. Los cambios ambientales podrían afectar a la fiabilidad de los sistemas para funcionar conforme a lo previsto. Son ejemplos de fallos que podrían influir perjudicialmente en el comportamiento de otros sistemas las averías en el acondicionamiento de aire sobre los equipos electrónicos o las averías en los sistemas de fluidos que causen inundaciones o elevada humedad en áreas donde haya equipos de los sistemas de seguridad.

3.119. Al evaluar la seguridad tecnológica del diseño debería prestarse atención a la influencia de las interacciones red-central sobre la fiabilidad

requerida del suministro eléctrico a los sistemas de la central importantes para la seguridad, cuestión tratada en detalle en una guía concreta de seguridad del OIEA¹².

3.120. Las estructuras, sistemas y componentes importantes para la seguridad no deberían compartirse entre dos o más reactores de potencia. No obstante, si se comparten, debería demostrarse mediante pruebas, experimentos o análisis de ingeniería que es posible satisfacer todos los requisitos de seguridad para todos los reactores en todos los estados. En el caso de que uno de los reactores se vea afectado por condiciones de accidente, debería ser posible proceder ordenadamente a la parada y a la eliminación del calor de decaimiento en los restantes reactores. Debería prestarse especial atención a los sucesos externos que puedan causar accidentes en más de un reactor. Los sistemas de apoyo comunes deberían ser capaces de atender las exigencias de todos los reactores afectados.

3.121. Otras interfaces entre diseño y operación que deberían ser comprobadas al evaluar la seguridad son las especificaciones técnicas y los procedimientos de operación.

USO DE AYUDAS COMPUTACIONALES EN EL PROCESO DE DISEÑO

3.122. En el diseño de obras de ingeniería se usa un gran número de herramientas informáticas, tales como diagramas, monogramas, fórmulas, algoritmos y códigos de computación (neutrónica, dinámica de fluidos, análisis estructural, etc.). Estas herramientas, así como los modelos numéricos empleados en ellas, deberían someterse a los pertinentes procedimientos de GC, incluyendo su verificación y validación según los principios expuestos en la Sección 4 para los códigos de computación (párrafos 4.236–4.244).

3.123. Todos los modelos numéricos deberían demostrar su fiabilidad mediante comparaciones, análisis independientes y procedimientos de cualificación, con el fin de cerciorarse de que su nivel intrínseco de incertidumbre se ajusta a la fiabilidad requerida para el diseño en su conjunto.

¹² Colección Seguridad No. 50-SG-D7, “Sistemas de emergencia de suministro de energía en centrales nucleares” (1993).

4. ANÁLISIS DE SEGURIDAD

ORIENTACIÓN GENERAL

4.1. El objetivo del análisis de seguridad debería ser establecer y confirmar, mediante la utilización de herramientas analíticas adecuadas, la base de diseño de los elementos importantes para la seguridad tecnológica, y garantizar que el diseño general de la central es capaz de satisfacer los límites prescritos y aceptables relativos a las dosis de radiación y las emisiones en cada categoría de condiciones de la central. El diseño, la fabricación, la construcción y la puesta en servicio deberían integrarse con el análisis de seguridad para garantizar que los objetivos de diseño queden plasmados en la central tal como se haya construido.

4.2. Como parte del proceso de diseño, el análisis de seguridad tecnológica debería ser llevado a cabo por las dos entidades que desempeñan un papel importante en la producción segura de energía nucleoelectrica, las cuales son:

- La entidad *diseñadora*, que utiliza el análisis de seguridad como parte importante e integral del proceso de diseño. Ello continúa a lo largo de la fabricación y la construcción de la central.
- La entidad *explotadora*, a la que el análisis de seguridad sirve como garantía de que el diseño, una vez plasmado en obra, se comportará en su funcionamiento conforme a lo previsto, y le sirve para demostrar que el diseño satisface los requisitos de seguridad en cualquier momento de la vida proyectada de la central.

4.3. El análisis de seguridad, como parte de la evaluación de la seguridad realizada para la concesión de la licencia a la central, debería desarrollarse en paralelo con el proceso de diseño, con iteración entre ambas actividades. El alcance y el nivel de detalle del análisis de seguridad deberían aumentar a medida que avanza el programa de diseño, de modo que el análisis final de seguridad refleje el diseño final de la central tal como ha sido construida.

4.4. Las recomendaciones sobre la ejecución de análisis de seguridad durante el proceso de diseño pueden servir también como guía para el análisis periódico de la seguridad de una central en funcionamiento o para la justificación de la seguridad de una propuesta de modificación del diseño. Las prescripciones relativas a las evaluaciones periódicas se estipulan en los

Requisitos de seguridad del OIEA sobre funcionamiento y en las guías de seguridad que los complementan.

4.5. Los modelos y datos de diseño de la central (que son bases fundamentales del análisis de seguridad) deberían mantenerse actualizados durante la fase de diseño y durante toda la vida de la central, incluida la clausura. Ello debería ser responsabilidad de la entidad diseñadora durante la fase de diseño y de la entidad explotadora durante la vida de la central

4.6. El proceso de actualización debería servir para incorporar la nueva información a medida que se disponga de ella, abordar los nuevos problemas a medida que se presenten, hacer uso de herramientas y métodos más perfeccionados conforme sean asequibles, y evaluar los resultados de las modificaciones del diseño y los procedimientos operativos que pudieran considerarse a lo largo de la vida de la central.

4.7. La evaluación de los aspectos de ingeniería importantes para la seguridad tratados en la Sección 3, y el análisis de seguridad a que se refiere esta sección deberían llevarse a cabo en paralelo.

Objetivos del análisis de seguridad

4.8. El análisis de seguridad debería evaluar el comportamiento de la central en una amplia gama de condiciones operacionales, sucesos iniciadores postulados y otras circunstancias (muchas de las cuales puede que no se den nunca en el funcionamiento real de la central), con el fin de llegar a una comprensión completa de la forma en que se prevé se comportará la central en esas situaciones. Dicho análisis debería demostrar también que la central puede mantenerse en el marco de los regímenes de funcionamiento seguro establecidos por la entidad diseñadora.

4.9. El análisis de seguridad debería evaluar de manera metódica el comportamiento de la central en diversas condiciones operacionales y de accidente, en contraste con los objetivos o criterios de seguridad y de emisiones radiológicas que hayan establecido la entidad explotadora, el órgano regulador, u otras autoridades nacionales o internacionales, en la medida en que sean de aplicación a la central.

4.10. El análisis de seguridad debería descubrir los posibles puntos débiles del diseño, evaluar las mejoras propuestas del mismo y proporcionar una demostración de que se cumplen los requisitos de seguridad, y de que el riesgo

proveniente de la central es aceptablemente bajo. Ello debería comprender una comparación con los criterios de riesgo, en el caso de que hayan sido definidos.

4.11. El análisis de seguridad debería respaldar el funcionamiento seguro de la central sirviendo como herramienta importante para determinar y confirmar los puntos de tarado y parámetros de regulación de los sistemas de protección y control de la central, Debería ser utilizado también para establecer y validar las especificaciones y límites de funcionamiento de la central, los procedimientos de operación en condiciones normales y anormales, los requisitos de mantenimiento e inspección, y los procedimientos normales y de emergencia.

4.12. El análisis de seguridad debería servir también de apoyo en los procesos de toma de decisiones de la dirección de la central y del órgano regulador conforme surjan nuevas cuestiones y problemas a lo largo de la vida de la central. El análisis inicial de seguridad de la central y la capacidad de rehacerlo, total o parcialmente, para resolver nuevas cuestiones técnicas, debería conservarse durante la vida de la central. Ello significa que la información real y actualizada del diseño y los datos del comportamiento operacional de la central se deberían incorporar al modelo de la misma, según sea necesario, para apoyar este proceso de análisis.

4.13. El análisis de seguridad debería ser una ayuda para poner de manifiesto cuestiones, estados de la central y sucesos iniciadores que no fueron considerados adecuadamente en las primeras etapas del diseño. Del mismo modo, el análisis de seguridad puede servir para determinar aspectos, por ejemplo SIP o criterios de aceptación establecidos, que no es necesario considerar (esto es, tras un examen más detenido concluye que no afectan ni contribuyen a la seguridad de la central, a causa de la frecuencia extremadamente baja con que se presentan, su probabilidad condicional insignificante o el impacto mínimo de sus potenciales consecuencias).

4.14. En el análisis de seguridad se debería evaluar si:

- La defensa en profundidad prevista es suficiente y se mantienen los niveles de defensa porque las secuencias potenciales de accidentes se interrumpen lo antes posible.
- La central es capaz de resistir las condiciones físicas y medioambientales a las que podría estar sometida. Ello incluiría niveles extremos de condiciones medioambientales y de otra naturaleza.

- Han sido adecuadamente consideradas las cuestiones de factores humanos y comportamiento humano.
- Los mecanismos de envejecimiento a largo plazo que pudieran mermar la fiabilidad de la central a lo largo de su vida, se detectan, vigilan y remedian (p.ej. mediante mejoras, renovaciones o sustituciones) de modo que la seguridad no se vea afectada y que el riesgo no aumente.

4.15. El análisis de seguridad debería demostrar mediante pruebas, evaluaciones, cálculos o análisis técnicos que los equipos incorporados para impedir que incidentes operacionales previstos o accidentes base de diseño progresen y degeneren en accidentes graves y para mitigar sus efectos, así como los procedimientos de operación de emergencia y las medidas de gestión de accidentes, son eficaces y reducen el riesgo a niveles aceptables.

4.16. El proceso de análisis de seguridad debería ser altamente fidedigno, con suficiente alcance, calidad, exhaustividad y precisión para generar la confianza de la entidad diseñadora, el órgano regulador, la entidad explotadora y el público en la seguridad del diseño de la central. Los resultados del análisis de seguridad servirán para garantizar, con alto nivel de confianza, que la central se comportará conforme a su diseño y cumplirá todos los criterios de aceptación previstos en el mismo al ser puesta en servicio y a lo largo de toda su vida.

Evaluaciones determinista y probabilista

4.17. La consecución de un alto nivel de seguridad tecnológica debería demostrarse principalmente por vía determinista. No obstante, el análisis de seguridad debería incluir tanto métodos deterministas como probabilistas. Se ha demostrado que estos métodos se complementan mutuamente y deberían emplearse ambos en el proceso de toma de decisiones con respecto a la seguridad, y la aptitud de la central para recibir la licencia. El método probabilista proporciona indicaciones claras sobre el comportamiento de la central, la defensa en profundidad y el riesgo, que no se obtienen con el enfoque determinista.

4.18. El objetivo del método determinista debería ser estudiar el comportamiento de la central en estados operacionales y condiciones de accidente concretos predeterminados, y aplicar un conjunto de reglas específicas para juzgar la adecuación del diseño.

4.19. En general, el análisis determinista con fines de diseño debería ser conservador. El análisis de los accidentes que sobrepasen la base de diseño es generalmente menos conservador que el análisis de los accidentes base de diseño.

4.20. El análisis probabilista de seguridad (APS) debería tener como objetivo determinar todos los factores que contribuyen de manera importante a los riesgos resultantes de la central y evaluar hasta qué punto el diseño de la configuración general de los sistemas está bien equilibrado, no existen riesgos atípicos y el diseño cumple los objetivos probabilistas básicos. En el APS se debería hacer uso preferente de un enfoque basado en estimaciones óptimas.

4.21. Las indicaciones precisas aportadas tanto por el análisis determinista como por el probabilista deberían ser utilizadas en el proceso de toma de decisiones. En general, se suele observar que tales indicaciones son coherentes. Concretamente, cuando se descubren puntos débiles en el diseño o el funcionamiento de la central, ello suele estar relacionado con un bajo grado de redundancia o de diversidad en los sistemas previstos para realizar una o más funciones de seguridad.

4.22. Hay situaciones en las que las indicaciones aportadas por el análisis determinista y el probabilista no son coherentes. Este problema debería ser estudiado caso por caso.

Información esencial

4.23. El proceso de análisis de seguridad debería basarse en información sobre el diseño de la central que sea completa y exacta. Esta información debería referirse a todas las ESC de la central, las interfaces externas y las características específicas del emplazamiento.

4.24. El diseño de la central debería documentarse y mantenerse al día incluidos el diseño aprobado de la central, el de la central ya construida y el de la central con sus modificaciones.

4.25. Cuando se trate de una central en funcionamiento, el análisis de seguridad (realizado, por ejemplo, para introducir modificaciones en el diseño) debería hacerse usando los datos específicos de funcionamiento de la central. Ello incluye información sobre las dosis radiológicas a los operadores durante el funcionamiento normal y las descargas habituales de material radiactivo desde el emplazamiento. En cuanto a los sistemas de la central, los datos acopiados deberían incluir las temperaturas, presiones, niveles de fluidos y

caudales normales de funcionamiento, así como las características y cronología de las respuestas transitorias a cualquier incidente operacional.

4.26. Los datos de funcionamiento deberían incluir también información sobre el comportamiento de componentes y sistemas, frecuencia de sucesos iniciadores, datos sobre la tasa de fallos de componentes, modos de fallo, indisponibilidad de los sistemas durante el mantenimiento o pruebas, y tiempos de reparación de componentes y sistemas.

4.27. Cuando se trate de una central en fase de diseño, los datos empleados deberían obtenerse a partir de datos genéricos de centrales en funcionamiento de diseño similar, o de resultados de investigación y pruebas. En el caso de una central que ya funcione, algunos aspectos de estas bases genéricas de datos pueden mejorarse con el tiempo a partir de los datos específicos del propio historial de funcionamiento y mantenimiento de la central, y de la experiencia y los resultados de las inspecciones.

4.28. En el análisis de seguridad se debería considerar todas las fuentes de material radiactivo de la central. Además del núcleo del reactor, esto incluye el combustible irradiado en tránsito, el combustible irradiado en almacenamiento y los desechos radiactivos almacenados.

Criterios de aceptación del análisis de seguridad

4.29. Deberían definirse los criterios de aceptación aplicables a la evaluación determinista y al APS. Esos criterios reflejan normalmente los adoptados por la entidad diseñadora o por la entidad explotadora y son congruentes con los requisitos estipulados por el órgano regulador.

4.30. Los criterios deberían ser suficientes para satisfacer el objetivo general de seguridad nuclear, el objetivo de protección radiológica y el objetivo de seguridad técnica que figuran en la publicación de Nociones fundamentales de seguridad del OIEA [2] y en la titulada “Seguridad de las centrales nucleares: Diseño” [1].

4.31. Además, se deberían establecer criterios detallados que contribuyan a garantizar el cumplimiento de esos objetivos de seguridad de más alto nivel (véanse los párrafos 4.98 y 4.103, infra). Ello simplificará habitualmente el análisis.

4.32. Los criterios probabilistas de seguridad deberían ser tenidos en cuenta cuando se hayan especificado por ley o como requisitos reglamentarios, o bien

deberían establecerse cuando proceda aplicarlos. Deberían guardar relación con la probabilidad de accidentes que tengan consecuencias radiológicas importantes, tales como deterioro del núcleo, grandes emisiones al exterior del emplazamiento, y dosis de radiación a trabajadores y a miembros de la población, según corresponda.

SUCESOS INICIADORES POSTULADOS (SIP)

Determinación de los sucesos iniciadores postulados

4.33. El punto de partida del análisis de seguridad es el conjunto de SIP que es preciso considerar. Un SIP se define en la Ref. [1] como “suceso indicado en el diseño que origina incidentes operacionales previstos o condiciones de accidente”. Los SIP incluyen sucesos tales como el fallo de equipos, los errores humanos y sucesos naturales o provocados por actividades humanas. Normalmente, el análisis determinista de seguridad y el APS deberían hacer uso del mismo conjunto de SIP.

4.34. El conjunto de SIP formulado para el análisis de seguridad debería ser exhaustivo y definirse de tal modo que los sucesos comprendan todos los fallos verosímiles de los sistemas y componentes de la central, y los errores humanos que puedan tener lugar en cualquier régimen de funcionamiento de la misma (por ejemplo arranque, parada y recarga). Ello debería incluir tanto los sucesos de origen interno como externo.

4.35. El conjunto de los SIP debería definirse de modo sistemático. Ello debería comprender la adopción de un método estructurado para determinarlos, que podría incluir lo siguiente:

- Empleo de métodos analíticos tales como el análisis de los riesgos y la operabilidad (*hazard and operability analysis*, HAZOP)¹³, el análisis de modos de fallo y sus efectos (*failure mode effect analysis*, FMEA)¹⁴, y diagramas lógicos maestros;

¹³ HAZOP es un proceso sistemático en el que se usa un conjunto de palabras clave para precisar los fallos que podrían ocurrir y conducir a SIP.

¹⁴ FMEA es un proceso sistemático que considera cada uno de los modos de fallo de los componentes sucesivamente para determinar si podrían conducir a un SIP (véase el apéndice V de la Ref. [10]).

- Comparación con la lista de los SIP establecidos para los análisis de seguridad de centrales similares (aunque este método no debería ser el único en utilizarse, ya que podría propagar errores anteriores);
- Análisis de los datos de experiencia operacional de centrales similares.

4.36. El conjunto de SIP considerado debería incluir también fallos parciales de los equipos, si pueden contribuir al riesgo significativamente.

4.37. El conjunto de SIP debería someterse a examen a medida que avancen el diseño y la evaluación de la seguridad, lo cual debería dar lugar a un proceso iterativo entre estas dos actividades.

4.38. El conjunto de SIP debería incluir también sucesos muy poco frecuentes o de consecuencias muy leves, por lo menos en la fase inicial del proceso. Tal vez sea posible eliminar algunos SIP. No obstante, la eliminación de cualquier SIP debería justificarse plenamente y documentarse muy bien las razones para ello. Muchos SIP permanecerán en el análisis hasta el final, y será sólo al concluir este proceso cuando se determinará si son insignificantes.

4.39. Todos los SIP deberían definirse cuantitativamente en términos de la frecuencia con que ocurran. Esta frecuencia debería definirse cuantitativamente en el caso de las aplicaciones del APS, pero en los análisis deterministas se utiliza siguiendo un planteamiento cualitativo.

SIP internos

4.40. Los SIP internos (los que se inician dentro de la central) se deberían establecer con miras a detectar posibles amenazas a la función fundamental de seguridad. El modo en que se ejecuten las funciones de seguridad depende de la concepción detallada del reactor. No obstante, las categorías de sucesos iniciadores que por lo general se definen son, entre otras, las siguientes:

- Aumento o disminución de la eliminación de calor del sistema de refrigeración del reactor,
- Aumento o disminución del caudal del sistema de refrigeración del reactor,
- Anomalías en la reactividad y la distribución de potencia,
- Aumento o disminución del inventario de refrigerante del reactor,
- Escape de material radiactivo de un subsistema o componente.

4.41. Al determinar el conjunto de SIP internos se deberían considerar también las diversas formas de fallo de los sistemas y componentes de seguridad, y los fallos de los sistemas y componentes que no sean de seguridad pero puedan tener impacto sobre una función o un sistema de seguridad fundamental. La mayoría de estos fallos pueden ser asignados a alguna de las categorías indicadas. No obstante, algunos de los SIP basados en estos fallos no encajan en las mencionadas categorías y se agrupan aparte. Como ejemplos de esos otros fallos determinados en APS realizados hasta la fecha cabe citar: (a) fallos en los sistemas de apoyo tales como pérdida de refrigeración de componentes o de agua de servicio; (b) inundación interna causada por avería en los sistemas de circulación de agua, agua de servicio o protección contra incendios, o en depósitos elevados de compensación; (c) señales espurias del aislamiento de la contención que den lugar a pérdida de refrigeración por la bomba del sistema primario; y (d) activación de las válvulas de alivios por inadvertencia.

4.42. En el proceso de determinación del conjunto de SIP internos se deberían también tener en cuenta los diversos modos de fallo de la barrera de presión del reactor. Ello debería incluir la rotura de tuberías en todos los lugares posibles, incluidas las que puedan ocurrir fuera de la contención.

4.43. Los SIP internos deberían incluir las modalidades de fallo que puedan darse en todos los modos de funcionamiento de la central (por ejemplo, transitorios de reactividad durante la criticidad inicial del núcleo y pérdida de inventario de refrigerante durante la recarga con la contención abierta), excluyendo los que sean de duración despreciable. Los modos de duración despreciable deberían ser excluidos sólo después de una cuidadosa consideración y un análisis conservador que demuestre que no tienen importancia al compararlos con la frecuencia de daño al núcleo calculada para otros SIP.

4.44. El conjunto de SIP debería incluir aquéllos que puedan ocurrir como consecuencia de errores humanos. Este grupo puede abarcar desde operaciones de mantenimiento incompletas o deficientes hasta el tarado incorrecto de los límites en los equipos de control, o acciones erróneas del operador. Estos SIP no tienen por qué ser similares a los causados por fallos de equipos, porque pueden ir acompañados de fallos de causa común que se sumen al suceso iniciador.

4.45. El conjunto de SIP internos debería incluir sucesos tales como incendio, explosiones, impactos de proyectiles de la turbina e inundaciones de origen interno que puedan afectar a la seguridad tecnológica del reactor y causar averías en alguno de los equipos del sistema de seguridad que proporcione protección frente a ese suceso iniciador. Estos SIP se han examinado ya en la Sección 3.

SIP externos

4.46. El conjunto de SIP establecido debería incluir todos los sucesos que pudieran originarse fuera de la central y comprometer la seguridad nuclear, incluidos los sucesos de origen natural y los provocados por actividades humanas. Estos sucesos iniciadores externos podrían dar lugar a un suceso iniciador interno y al fallo de alguno de los equipos del sistema de seguridad que se necesitarían para la protección contra el suceso. Por ejemplo, un terremoto podría producir averías en los equipos de la central además de la pérdida de alimentación eléctrica externa.

4.47. El conjunto de los SIP establecido para el análisis de seguridad determinado debería incluir los sucesos de origen natural que sean verosímiles para un emplazamiento. Ello debería comprender los sucesos tales como terremotos, incendios e inundaciones (incluso las causadas por rotura de presas, diques o terraplenes) que ocurran fuera del emplazamiento, las condiciones meteorológicas extremas (temperatura, lluvia, nevada, vendaval) y las erupciones volcánicas.

4.48. Se deberían incluir en el conjunto de los SIP definidos para el análisis de seguridad los sucesos externos provocados por actividades humanas que sean verosímiles en un emplazamiento dado. Ello debería comprender la caída de aeronaves, los efectos de instalaciones industriales próximas y las explosiones en sistemas de transporte.

4.49. Pueden verse recomendaciones detalladas sobre los sucesos externos en la publicación de Requisitos de seguridad del OIEA relativa a la selección de emplazamientos¹⁵ y en las Guías de seguridad complementarias.

¹⁵ Colección Seguridad No. 50-C-S (Rev.1), “Código sobre la seguridad de las centrales nucleares: Emplazamiento” (1989).

ANÁLISIS DETERMINISTA DE SEGURIDAD¹⁶

Funcionamiento normal

4.50. El objetivo del análisis de seguridad en el caso de funcionamiento normal debería ser cerciorarse de que:

- El funcionamiento normal de la central puede efectuarse de forma segura, confirmando por tanto que:
- Las dosis radiológicas a los trabajadores y los miembros de la población se ajustan a los límites aceptables,
- Las emisiones programadas de material radiactivo de la central se ajustan a los límites aceptables.

4.51. En el análisis de seguridad relativo a funcionamiento normal se deberían considerar todas las situaciones de la central en las que los sistemas y equipos funcionan conforme a lo previsto, sin problemas internos o externos. Ello incluye todas las fases de funcionamiento, tanto en estado de operación a potencia como en situación de parada o de mantenimiento, en el régimen normal para el que la central fue diseñada, a lo largo de toda su vida.

4.52. El funcionamiento normal de una central nuclear incluye generalmente los siguientes estados:

- Aproximación inicial a la criticidad del reactor;
- Arranque normal del reactor desde la situación de parada, pasando por el estado crítico hasta llegar a potencia;
- Funcionamiento a potencia, inclusive tanto a plena potencia como a potencia reducida;
- Cambios en el nivel de potencia del reactor, incluidos los modos de seguimiento de carga, si se emplean;
- Parada del reactor desde el funcionamiento a potencia;
- Parada en modo de parada caliente;
- Parada en modo de parada fría;

¹⁶ Figura más información al respecto en una publicación de la Colección de Informes de Seguridad del OIEA titulada “Accident Analysis for Nuclear Power Plants” (en preparación).

- Parada en modo de recarga o modo equivalente de mantenimiento, en el que se abran elementos importantes de cierre en la barrera de presión del refrigerante;
- Parada en otros modos o configuraciones de la central con temperatura, presión o condiciones de inventario de refrigerante excepcionales;
- Manipulación y almacenamiento de combustible irradiado y no irradiado.

4.53. En el análisis de seguridad se debería evaluar si es posible llevar a cabo el funcionamiento normal de la central en forma segura sin que los valores de sus parámetros excedan los límites operacionales.

4.54. El análisis de seguridad debería establecer los límites y condiciones para un funcionamiento seguro. Ello incluiría aspectos como:

- Los límites de seguridad de los sistemas de protección y control del reactor y de otros dispositivos técnicos,
- Los límites operacionales y tarados de referencia del sistema de control,
- Las restricciones de procedimiento en el control operacional de procesos,
- La determinación de las configuraciones operacionales aceptables.

En la Ref. [8] figura información más detallada.

4.55. Al evaluar la seguridad del diseño en régimen de funcionamiento normal se debería verificar que un disparo del reactor o una activación de los sistemas de seguridad tecnológica sólo podría ocurrir en caso necesario. Los disparos o las iniciaciones espurias de sistemas de seguridad son generalmente perjudiciales para la seguridad.

Dosis radiológicas a los trabajadores y a los miembros de la población en funcionamiento normal

4.56. El análisis de seguridad en funcionamiento normal debería incluir un examen del diseño y funcionamiento global de la central para: predecir las dosis de radiación que probablemente reciban los trabajadores y los miembros de la población; cerciorarse de que estas dosis se ajustan a los límites aceptables; y cuidar de que se satisfaga el principio de reducir las dosis al valor más bajo que sea razonablemente posible.

4.57. En lo que respecta a los trabajadores del emplazamiento, las predicciones de dosis deberían basarse en las tareas específicas requeridas para el funcionamiento y mantenimiento de la central. En esas predicciones se

deberían incluir las contribuciones de la radiación directa y de la incorporación de sustancias radiactivas. En el análisis se debería tener presente la duración y frecuencia de esas tareas y el número de personas que intervengan en cada una de ellas. Deberían hacerse estimaciones tanto de la dosis individual más alta como de la dosis anual media por grupos.

4.58. En cuanto a los miembros de la población, las predicciones de dosis deberían incluir las contribuciones de la radiación directa, la incorporación de sustancias radiactivas y las dosis recibidas a través de la cadena alimentaria como consecuencia de las descargas de material radiactivo de la central. Deberían estimarse las dosis al grupo crítico.

4.59. En caso de incertidumbres al formular las predicciones de dosis, se deberían adoptar supuestos conservadores.

4.60. Cuando las predicciones de dosis dependan de las tasas de dosis resultantes del nivel creciente de los inventarios de material radiactivo o del nivel de contaminación, la predicción debería basarse en los valores máximos que probablemente se alcancen a lo largo de la vida de la central.

4.61. Al predecir las dosis se deberían tener en cuenta todos los datos pertinentes aportados por la experiencia de funcionamiento. Estos datos podrían basarse en el funcionamiento de la propia central o de centrales similares.

4.62. Esas estimaciones de dosis deberían compararse con los criterios radiológicos establecidos para la central. Este cotejo debería incluir los límites de dosis estipulados por la ley o por el órgano regulador y debería tener en cuenta las recomendaciones vigentes de la Comisión Internacional de Protección Radiológica (CIPR).

4.63. Los resultados de estas estimaciones de dosis deberían evaluarse a fin de detectar cualquier punto débil del diseño o del sistema de funcionamiento de la central; deberían hacerse mejoras cuando sean razonablemente realizables.

Emisiones programadas de material radiactivo de la central

4.64. El análisis de seguridad en funcionamiento normal debería incluir una estimación de las emisiones programadas de material radiactivo de la central.

4.65. Estas estimaciones de emisiones programadas de material radiactivo se deberían comparar con los criterios radiológicos establecidos para la central, incluso los requisitos estipulados por la ley o por el órgano regulador, y examinar a la luz de los principios ALARA. Se deberían evaluar el diseño y el funcionamiento de la central e introducirse mejoras, cuando sean razonablemente factibles, para reducir las emisiones programadas.

Incidentes operacionales previstos y accidentes base de diseño

4.66. Las situaciones de la central consideradas en el análisis base de diseño incluyen los incidentes operacionales previstos y los accidentes base de diseño (ABD). La distinción entre ellos se funda en la frecuencia con la que ocurren.

4.67. Los incidentes operacionales previstos son sucesos más complejos que las maniobras que se realizan durante el funcionamiento normal y pueden, en potencia, comprometer la seguridad del reactor. Cabe esperar que estos sucesos ocurran por lo menos una vez durante la vida de la central. En general se presentan con una frecuencia superior a 10^{-2} por reactor-año.

4.68. Los accidentes base de diseño tienen una frecuencia menor que los incidentes operacionales previstos. Normalmente, no es de esperar que se presenten durante toda la vida de la central, pero conforme al principio de defensa en profundidad, se tienen en cuenta al diseñarla. Los ABD ocurren con una frecuencia comprendida en el intervalo de 10^{-2} a 10^{-5} por reactor-año, si bien hay algunos grupos de sucesos iniciadores postulados que tradicionalmente se incluyen en el análisis base de diseño y pueden tener frecuencias inferiores.

4.69. La finalidad del análisis base de diseño debería consistir en obtener una sólida demostración de la tolerancia del diseño técnico a los fallos y de la efectividad de los sistemas de seguridad. Ello se lleva a cabo mediante un análisis conservador en el que se deberían tener en cuenta las incertidumbres de las modelizaciones.

Sucesos iniciadores postulados que dan lugar a incidentes operacionales previstos

4.70. En el caso de muchos SIP los sistemas de control compensarán los efectos del suceso sin que se produzca el disparo del reactor ni se impongan otras exigencias a los sistemas de seguridad (nivel 2 de defensa en profundidad). No obstante, la categoría de incidentes operacionales previstos debería incluir

todos los SIP que quepa esperar tengan lugar durante la vida de la central y en los que se pueda reanudar el funcionamiento tras la rectificación del fallo.

4.71. Ejemplos típicos de SIP que dan lugar a incidentes operacionales previstos serían, entre otros, los que figuran a continuación. Esta lista tiene carácter general indicativo. La lista real dependerá del tipo de reactor y del diseño real de los sistemas de la central:

- *Aumento de la eliminación de calor del reactor*: apertura fortuita de las válvulas de alivio del vapor; mal funcionamiento del control de presión en el secundario que dé lugar a un aumento del caudal de vapor; mal funcionamiento del sistema de agua de alimentación que cause un aumento en la tasa de eliminación de calor.
- *Disminución de la eliminación de calor del reactor*: disparo de las bombas de agua de alimentación; reducción del caudal de vapor por diversas causas (mal funcionamiento de controles, cierre de la válvula principal del vapor, disparo de la turbina, pérdida de carga externa, pérdida de alimentación eléctrica, pérdida de vacío en el condensador).
- *Disminución del caudal del sistema de refrigeración del reactor*: disparo de una bomba principal de refrigeración; aislamiento fortuito de un circuito del sistema principal de refrigeración (en su caso).
- *Anomalías en la reactividad y la distribución de potencia*: extracción fortuita de barras de control; dilución del boro por mal funcionamiento del sistema de control volumétrico (si se trata de un reactor de agua a presión); posicionamiento erróneo de un conjunto combustible.
- *Aumento del inventario de refrigerante del reactor*: mal funcionamiento del sistema de control químico y volumétrico.
- *Disminución del inventario de refrigerante del reactor*: pérdida muy pequeña de refrigerante (LOCA) debida a fallo de una tubería de instrumentación.
- *Escape de material radiactivo de un subsistema o componente*: pequeña fuga de un sistema de desechos radiactivos.

Sucesos iniciadores postulados que dan lugar a accidentes base de diseño

4.72. Se debería determinar el subconjunto de SIP que se considere darán lugar a accidentes base de diseño. Todos los SIP reconocidos como iniciadores de incidentes operacionales previstos deberían ser considerados también iniciadores potenciales de accidentes base de diseño. Aunque no es habitual incluir en el análisis los SIP que se presentan con muy baja frecuencia, al fijar

un límite umbral se deberían tener en cuenta los objetivos de seguridad establecidos para el reactor en cuestión.

4.73. Ejemplos típicos de SIP conducentes a accidentes base de diseño podrían ser los dados a continuación. Esta lista tiene carácter general indicativo. La lista real dependerá del tipo de reactor y del diseño real:

- Aumento de la eliminación de calor del reactor: rotura en la tubería de vapor.
- Disminución de la eliminación de calor del reactor: rotura en la tubería de agua de alimentación.
- Disminución del caudal del sistema de refrigeración del reactor: disparo de todas las bombas primarias de refrigeración; agarrotamiento del rotor o rotura del eje de una bomba primaria de refrigeración.
- Anomalías en la reactividad y distribución de potencia: retirada incontrolada de una barra de control; expulsión de una barra de control; dilución del boro a causa de la puesta en marcha de un circuito inactivo (en un reactor de agua a presión).
- Aumento del inventario de refrigerante del reactor: entrada fortuita en funcionamiento de la refrigeración de emergencia del núcleo.
- Disminución del inventario de refrigerante del reactor: una serie de posibles LOCA; apertura fortuita de las válvulas de alivio del sistema primario; fugas de refrigerante primario al sistema secundario.
- Escape de material radiactivo de un subsistema o componente: sobrecalentamiento o deterioro de combustible usado en tránsito o almacenado; rotura en un sistema de tratamiento de desechos gaseosos o líquidos.

4.74. Debería señalarse que algunos de los sucesos iniciadores de accidente que han sido tradicionalmente considerados como ABD pueden tener una frecuencia inferior a 10^{-5} por año. Éste puede ser el caso de SIP tales como un LOCA causado por una rotura grande en centrales proyectadas y construidas según los estándares modernos. Es posible, no obstante, que las normas reglamentarias sigan exigiendo la consideración de estos SIP en la categoría de ABD.

Agrupamiento

4.75. Siguiendo las directrices precedentes se definirá un gran número de SIP. No es necesario analizarlos todos. La práctica habitual es agruparlos y elegir casos límite para el análisis de cada grupo.

4.76. Los casos límite deberían definir los accidentes que impongan las mayores exigencias a cada una de las principales funciones de seguridad especificadas. En algunos casos, un accidente puede ser el más grave atendiendo a un parámetro determinado de seguridad (por ejemplo, un pico de presión en el sistema de refrigeración del reactor), mientras que otro puede ser el más grave atendiendo a otro parámetro de seguridad (por ejemplo, un pico de temperatura en el combustible). En tales situaciones, todas estas secuencias de accidente se analizan en el proceso de diseño como casos límite.

4.77. El análisis de seguridad debería confirmar que el agrupamiento y la delimitación de los sucesos iniciadores son aceptables.

Objetivos del análisis de los incidentes operacionales previstos y los ABD

4.78. El análisis de seguridad de los incidentes operacionales previstos y los ABD debería demostrar que los sistemas de seguridad son capaces de cumplir los requisitos de seguridad porque están en condiciones de:

- Parar el reactor y mantenerlo en el estado de parada segura durante y después de situaciones de ABD.
- Eliminar el calor residual del núcleo después de parar el reactor en cualquier estado operacional y en cualquier situación de ABD.
- Reducir el potencial de emisión de material radiactivo y ofrecer garantías de que toda emisión se sitúe por debajo de los límites prescritos durante los estados operacionales y por debajo de los límites aceptables durante las situaciones de ABD.

4.79. El análisis de seguridad debería demostrar que no se sobrepasan los límites de la central ni los límites radiológicos. En particular, debería demostrar que algunas o todas las barreras contra la emisión de material radiactivo de la central conservarán su integridad en la medida requerida.

4.80. El análisis de seguridad debería definir las capacidades de diseño de la central y los puntos de tarado de los sistemas de protección que sean garantía de que las funciones fundamentales de seguridad se mantengan en todo momento. Los sucesos base de diseño son el fundamento para diseñar los sistemas de control de la reactividad, el sistema de refrigeración del reactor, los dispositivos protectores técnicos (p. ej. el sistema de refrigeración de emergencia del núcleo, el sistema de contención y los sistemas de protección de la contención), los sistemas de suministro eléctrico y los diversos sistemas auxiliares importantes para la seguridad.

4.81. Los períodos de tiempo evaluados para los sucesos deberían ser suficientemente largos para determinar todas las consecuencias de los sucesos base de diseño. Esto significa que los cálculos relativos a los transitorios de la central han de extenderse mas allá del momento en que ésta se ha parado y se han activado los sistemas de refrigeración de seguridad (es decir, hasta haber alcanzado un estado estable de larga duración).

4.82. En el caso de las centrales nuevas y las que estén siendo objeto de una evaluación periódica de la seguridad, se debería llevar a cabo una definición y evaluación completas de todos los sucesos base de diseño. Cuando se trate de modificaciones de centrales existentes, la evaluación debería centrarse en los sucesos base de diseño que queden afectados por la modificación.

4.83. En los casos de modificación o revaluación de una central existente, puede que sea necesario modificar la metodología y los supuestos adoptados en el diseño original, por varias razones:

- Es posible que la base de diseño o los criterios de aceptación originales no sean ya adecuados.
- Las herramientas empleadas en el análisis de seguridad pueden haber sido superadas por métodos más perfeccionados.
- Es posible que la base de diseño original ya no se cumpla.

4.84. El análisis de seguridad realizado en el caso de los incidentes operacionales previstos es esencialmente idéntico al que se lleva a cabo para los accidentes. No obstante, al analizar los primeros no es preciso proceder de manera tan conservadora como cuando se trata de los ABD. Por ejemplo, en el análisis de los incidentes operacionales previstos no se suele necesariamente suponer la indisponibilidad de todos los equipos y sistemas no clasificados como de seguridad.

4.85. Además, los incidentes operacionales previstos no deberían conducir a la imposición de ninguna exigencia innecesaria a los equipos de seguridad diseñados básicamente para la protección en caso de ABD.

Métodos y supuestos en el análisis de los incidentes operacionales previstos y los ABD

Métodos

4.86. En el análisis de seguridad de los incidentes operacionales previstos y de los ABD se deberían emplear códigos adecuados de computación en física neutrónica, termohidráulica, cálculo de estructuras y radiología para determinar la respuesta del reactor a los incidentes operacionales y a los accidentes considerados.

4.87. Los códigos de computación utilizados en el análisis de los incidentes operacionales previstos y de los ABD deberían estar adecuadamente verificados y validados. Ello incluye los códigos utilizados para predecir el comportamiento del núcleo del reactor, los códigos termohidráulicos y los códigos relativos a las emisiones radiológicas y sus consecuencias. Además, los analistas y los usuarios de los códigos deberían poseer cualificación, capacitación y experiencia suficientes.

4.88. Los códigos de computación usados para el análisis de seguridad de los ABD/incidentes operacionales previstos deberían estar basados en la experiencia de operación que pueda deducirse de centrales nucleares similares y de los datos experimentales pertinentes. Puesto que es de esperar que los incidentes operacionales previstos ocurran una o más veces a lo largo de la vida de una central, hay una cierta base acumulada de experiencia operacional y datos referentes a estos transitorios.

4.89. Los parámetros, las condiciones iniciales y los supuestos de disponibilidad de los equipos que se adoptan en los modelos de los códigos de computación son tradicionalmente muy conservadores, con valores límite prudentes para todos los parámetros del análisis. No obstante, en el pasado esto ha dado lugar a veces a secuencias engañosas de sucesos, predicción de escalas de tiempo no realistas, y la omisión de algunos fenómenos físicos. Teniendo en cuenta tales limitaciones y la madurez actual de los códigos para estimaciones óptimas, deberían utilizarse éstos en el análisis de seguridad, combinándolos con una selección razonablemente conservadora de los datos de entrada y una evaluación suficiente de la incertidumbre de los resultados.

4.90. También puede ser aceptable usar un código de computación para estimaciones óptimas combinado con supuestos realistas acerca de las condiciones iniciales y las condiciones límite. Este método debería basarse en

incertidumbres combinadas estadísticamente para las situaciones de la central y en modelos de computación para acreditar, con una probabilidad especificada alta, que los resultados calculados no exceden los criterios de aceptación.

4.91. El análisis de seguridad debería someterse a un programa de GC adecuado. En particular, todas las fuentes de datos deberían estar referenciadas y documentadas, y la totalidad del proceso debería quedar registrada y archivada, para permitir comprobaciones independientes.

Supuestos

4.92. Entre los supuestos conservadores adoptados para el análisis base de diseño deberían figurar en general los siguientes:

- El suceso iniciador ocurre en un momento desfavorable en cuanto a las condiciones iniciales del reactor, en particular nivel de potencia, nivel de calor residual, condiciones de reactividad, y temperatura, presión e inventario del sistema de refrigeración del reactor.
- Debería suponerse que cualquier sistema de control opera solamente si su funcionamiento se traduce en agravar los efectos del suceso iniciador. No debería reconocerse ningún valor a la actuación de los sistemas de control en la mitigación de los efectos del suceso iniciador.
- Debería suponerse que todos los sistemas y equipos de la central no clasificados ni mantenidos como corresponde a la categoría de seguridad (GC total, cualificación sísmica y cualificación de equipos) fallan de forma tal que se producen los efectos más graves del SIP que se analiza.
- Debería suponerse que ocurre el fallo único más desfavorable en el funcionamiento de los grupos de seguridad requeridos para el suceso iniciador. En el caso de sistemas redundantes se suele suponer que arranca y actúa el número mínimo de conjuntos de equipo.
- Debería suponerse que los sistemas de seguridad funcionan a su nivel mínimo de rendimiento. En cuanto al disparo del reactor y a los sistemas de activación del sistema de seguridad, se debería suponer que los hechos ocurren en el extremo más desfavorable de la gama de posibilidades.
- Debería suponerse la indisponibilidad de toda estructura, sistema o componente que no pueda considerarse completamente operable, o que alcance durante el accidente un límite para el cual el diseñador no haya probado su plena operabilidad.

- Las actuaciones del personal de la central para prevenir o mitigar el accidente deberían modelizarse solamente si puede demostrarse que hay tiempo suficiente para que el personal lleve a cabo las acciones requeridas, si se dispone de amplia información para el diagnóstico del suceso (considerando los efectos del suceso iniciador y el criterio de fallo único), si se dispone de procedimientos escritos adecuados, y si se ha impartido suficiente capacitación. Se supone por lo general que las actuaciones del personal tienen lugar, como más pronto, a los diez minutos de haberse iniciado el suceso.

4.93. Los supuestos conservadores adoptados deberían tener en cuenta las incertidumbres de las condiciones iniciales del reactor, incluidos los puntos de tarado para la actuación de los sistemas de seguridad.

4.94. El análisis base de diseño debería incluir todos los fallos que puedan ocurrir como consecuencia del suceso iniciador (y que son, por lo tanto, parte del SIP). Entre ellos figuran los siguientes:

- Si el suceso iniciador es un fallo de parte de una red de distribución eléctrica, el análisis del ABD debería suponer la indisponibilidad de todos los equipos alimentados por dicha parte de la red.
- Si el suceso iniciador es de naturaleza energética, tal como el fallo de un sistema a presión que dé lugar a un escape de agua caliente o a un efecto de látigo en las tuberías, la definición del ABD debería incluir el fallo del equipo que podría resultar afectado.
- En el caso de sucesos internos, como incendios o inundaciones, o externos como terremotos, la definición del suceso base de diseño debería incorporar el fallo de todos los equipos que no hayan sido concebidos para resistir los efectos del suceso, ni estén protegidos contra él.

4.95. Dada la naturaleza decididamente conservadora de estas hipótesis, el análisis de la base de diseño a menudo proporciona una sólida demostración de que se dispone de amplios márgenes antes de que lleguen a excederse los límites de seguridad. Sin embargo, hay que proceder con cautela al hacer uso del análisis, porque no siempre sucede así.

4.96. El análisis de seguridad de los incidentes operacionales previstos debería incluir también muchos de los supuestos conservadores de los análisis deterministas de los ABD, especialmente aquellos que guarden relación con los sistemas que permiten mantener las funciones críticas de seguridad durante estos transitorios. Sin embargo, no es necesario suponer que estén

indisponibles todos los sistemas y equipos que no sean de seguridad, y que no pueda reconocerse ningún valor a los sistemas de control para mitigar los efectos del suceso iniciador, a no ser que el SIP deje indisponibles dichos sistemas.

4.97. Los resultados de la evaluación deberían estructurarse y presentarse en formato adecuado para ofrecer una clara comprensión del transcurso del suceso y permitir una fácil comprobación de los criterios de aceptación particulares.

Criterios de aceptación

4.98. Deberían definirse criterios de aceptación para los sucesos y situaciones comprendidos en la base de diseño como se establece en la Ref. [1]. Estos criterios deberían garantizar el mantenimiento de un nivel adecuado de defensa en profundidad impidiendo el deterioro de las barreras previstas contra la emisión de material radiactivo y previniendo las emisiones radiológicas inaceptables.

4.99. Los criterios de aceptación deberían establecerse a dos niveles, como sigue:

- Criterios de nivel global/alto, relacionados con las dosis a la población o con la prevención de un fallo consecutivo de una barrera de presión en un accidente. Estos criterios suelen estar definidos por la ley o por el órgano regulador.
- Criterios detallados, definidos por el diseñador o analista. Estos criterios se seleccionan de modo que sean suficientes, pero no necesarios para cumplir los criterios globales de aceptación. Además, el analista puede establecer metas a nivel más detallado (criterios de aceptación más exigentes) para simplificar el análisis (por ejemplo, para no tener que hacer cálculos muy refinados). Deberían especificarse claramente el alcance y las condiciones de aplicabilidad de cada criterio específico.

4.100. Los criterios de aceptación deberían relacionarse con las circunstancias asociadas al accidente — por ejemplo, con la frecuencia de un suceso iniciador o el diseño del reactor y las condiciones de la central. Por lo general, es preciso aplicar criterios diferentes para juzgar la vulnerabilidad de cada barrera y para los diversos aspectos del accidente. Se suele aplicar criterios más restrictivos a los sucesos que ocurren con más frecuencia.

4.101. Los criterios de aceptación radiológicos aplicables a los incidentes operacionales previstos son habitualmente más restrictivos porque sus frecuencias son mayores. En general, no debería haber fallos en ninguna de las barreras físicas (pastilla de combustible, vaina del combustible, barrera de presión del refrigerante o contención) ni daño al combustible (o ningún daño adicional al combustible si ya existen fugas menores, dentro de los límites operacionales).

4.102. El criterio global de aceptación para los ABD debería ser o bien un impacto radiológico nulo fuera del emplazamiento, o bien sólo un impacto radiológico menor fuera de la zona de exclusión. La definición de impacto radiológico menor debería ser establecida por el órgano regulador, pero generalmente se corresponde con límites de dosis muy restrictivos, a fin de descartar la necesidad de actuaciones de emergencia fuera del emplazamiento.

4.103. Entre los criterios detallados de aceptación podrían figurar los siguientes:

- Un suceso no debería originar una situación subsiguiente más grave de la central sin que ocurra otro fallo independiente. Así pues, un incidente operacional previsto no debería originar por sí mismo un ABD, y un ABD por sí mismo no debería originar un accidente que sobrepase la base de diseño.
- No debería producirse ningún efecto consecutivo de pérdida de funcionalidad de los sistemas de seguridad necesarios para mitigar las consecuencias de un accidente.
- Los sistemas empleados en la mitigación de accidentes deberían diseñarse para soportar las cargas, tensiones y condiciones ambientales máximas propias de los accidentes analizados. Este punto debería evaluarse mediante análisis por separado relativos a las condiciones ambientales (esto es, temperatura, humedad o entorno químico) y a las cargas térmicas o mecánicas impuestas a las estructuras y los componentes de la central.
- La presión en los sistemas primario y secundario no debería exceder los límites correspondientes de diseño para las condiciones existentes en la central. Pueden ser necesarios análisis adicionales de sobrepresión para estudiar la influencia de fallos en las válvulas de seguridad y de alivio.
- Habría que determinar para cada tipo de SIP el número de fallos de vainas del combustible que podrían ocurrir sin que se incumplan los criterios radiológicos globales.

- En los casos de LOCA en que el combustible quede al descubierto y se sobrecaliente debería mantenerse la integridad estructural de las barras de combustible y una geometría que permita la refrigeración.
- Ningún suceso debería dar lugar a temperaturas, presiones o diferencias de presión dentro de la contención que excedan los valores usados como base de diseño de la contención.

Consideraciones sobre los accidentes graves y los que sobrepasan la base de diseño

4.104. Los accidentes más graves que los ABD reciben el nombre de accidentes que sobrepasan la base de diseño. Pueden tener una serie de consecuencias como las siguientes:

- Que estén dentro de la envolvente de los criterios de aceptación conservadores aplicables a los ABD, aunque para demostrarlo puede que sea necesario un análisis basado en estimaciones óptimas.
- Que excedan los criterios de aceptación conservadores relativos a los ABD, pero sin tener por resultados, a juzgar por un análisis basado en estimaciones óptimas, daños significativos en el combustible o el rebase de los límites de fallos del circuito primario.
- Que, a causa de fallos múltiples y/o errores del operador, los sistemas de seguridad no ejecuten una o más de sus funciones, dando lugar a un deterioro significativo del núcleo que comprometa la integridad de las restantes barreras contra la emisión de material radiactivo de la central. Éstos reciben el nombre de accidentes graves. Los accidentes graves podrían cobrar más auge y causar:
 - deterioro del núcleo y fallo del circuito primario, pero no de la contención, o
 - deterioro del núcleo y fallo del circuito primario y de la contención, originando una gran emisión de material radiactivo al medio ambiente, y poniendo a prueba las medidas externas de respuesta a emergencias.

4.105. El análisis de seguridad debería intentar cuantificar un margen de seguridad de la central y demostrar que existe un cierto grado de defensa en profundidad para esta clase de accidentes. Ello debería incluir las siguientes medidas cuando sean razonablemente posibles:

- Impedir la escalada de sucesos para que no provoquen accidentes graves, controlar la progresión de los accidentes graves y limitar las emisiones de material radiactivo previendo el uso de equipos adicionales y procedimientos de gestión de accidentes.
- Mitigar las consecuencias radiológicas que puedan producirse previendo planes de respuesta a emergencias dentro y fuera del emplazamiento.

En cuanto a las secuencias hipotéticas de accidentes graves (p. ej. fusión del núcleo a alta presión en los reactores de agua a presión) que pudieran conducir a un fallo rápido de la contención, debería demostrarse que es posible descartarlas con un alto grado de confianza.

Selección de los accidentes graves para el análisis de seguridad

4.106. En el análisis de los accidentes graves se debería considerar un conjunto de secuencias representativas en las que los sistemas de seguridad hayan funcionado mal y algunas barreras contra la emisión de material radiactivo hayan fallado, o hayan sufrido derivaciones. Estas secuencias deberían seleccionarse añadiendo más fallos o respuestas incorrectas del operador a las secuencias de accidente base de diseño (para incluir el fallo del sistema de seguridad) y a las secuencias dominantes de accidente derivadas del APS.

4.107. Las secuencias de sucesos significativos que pudieran dar lugar a accidentes graves se deberían definir aplicando una combinación de métodos deterministas y probabilistas, así como sólidos criterios técnicos.

4.108. El modo más riguroso de determinar las secuencias de accidentes graves es emplear los resultados del APS de nivel 1 (véase el párrafo 4.124). No obstante, también se podrían definir secuencias representativas o envolventes a partir de la comprensión de los fenómenos físicos que entrañan las secuencias de accidentes graves, los márgenes existentes en el diseño, y el grado de redundancia de sistemas subsistente en los casos de ABD.

4.109. Ejemplos de sucesos iniciadores de accidentes graves son los siguientes:

- Pérdida completa de eliminación del calor residual del núcleo del reactor,
- LOCA con pérdida completa de refrigeración de emergencia del núcleo,
- Pérdida completa del suministro eléctrico durante un largo período de tiempo.

4.110. Los detalles de las secuencias de accidentes graves que han de ser analizadas diferirán en función del diseño de los sistemas de seguridad del reactor.

4.111. Al evaluar los accidentes graves se deberían tener en cuenta todas las capacidades de diseño de la central, incluido el uso de algunos sistemas, tanto de seguridad como no de seguridad, más allá de su función originalmente prevista, para hacer que el accidente potencialmente grave retorne a un estado controlado y/o mitigar sus consecuencias. Si se reconoce valor al uso extraordinario de sistemas, debería haber una base razonable para contar con que dichos sistemas pueden ser utilizados, y se utilizarán, en la forma analizada.

Métodos y supuestos para el análisis de los accidentes graves

4.112. No existe un acuerdo generalizado acerca del mejor método para el análisis de los accidentes graves y los criterios de aceptación asociados. Sin embargo, hay una clara tendencia a adoptar los criterios siguientes, o similares, en el caso de los diseños de nuevos reactores avanzados. El análisis de los accidentes graves debería realizarse generalmente aplicando supuestos, datos, métodos y criterios de decisión basados en estimaciones óptimas. Cuando esto no sea posible, deberían adoptarse hipótesis razonablemente conservadoras que tengan en cuenta las incertidumbres en la comprensión de los procesos físicos que se están modelizando.

4.113. En el análisis de los accidentes graves se debería modelizar la amplia gama de procesos físicos que podrían ocurrir como consecuencia del deterioro del núcleo y que podrían originar una emisión de material radiactivo al medio ambiente. Esta gama debería incluir, según el caso:

- Los procesos de degradación del núcleo y la fusión del combustible;
- Las interacciones combustible-refrigerante (incluidas las explosiones de vapor);
- La retención en la vasija del material fundido;
- El paso del material fundido a través de la vasija;
- La distribución del calor en el interior del circuito primario;
- La eyección a gran presión de material fundido / calentamiento directo de la contención;
- La generación y combustión de hidrógeno;
- El fallo o derivación de la contención;
- La interacción núcleo-hormigón;

- La emisión y transporte de productos de fisión;
- La capacidad de refrigerar el núcleo fundido, dentro y fuera de la vasija.

4.114. El análisis requeriría generalmente una aproximación en varios niveles con empleo de diferentes códigos, incluidos códigos detallados de análisis de los sistemas y de la contención, códigos más simplificados de evaluación del riesgo y de efectos en forma separada, así como estudios del término fuente y el impacto radiológico. El empleo de una selección completa de códigos dará la seguridad de analizar adecuadamente todos los fenómenos previstos.

4.115. La evaluación debería servir para asegurarse de que el núcleo del reactor, el circuito primario y la contención se han modelizado con exactitud. Estos modelos son particularmente importantes para el análisis y son decisivos para determinar el curso del accidente.

Criterios de aceptación

4.116. Los criterios de aceptación relativos a los accidentes graves se formulan habitualmente como criterios de riesgo (criterios probabilistas de seguridad). Estos criterios se examinan en los párrafos 4.219 a 4.231. Ahora bien, no existe acuerdo general sobre cuáles deberían ser estos criterios.

En algunos países se han especificado también criterios de aceptación deterministas, por lo general conforme a las líneas siguientes:

- No debería ocurrir un fallo de la contención en el corto plazo, después de un accidente grave,
- No debería haber efectos sobre la salud en el corto plazo después de un accidente grave,
- Los efectos sobre la salud a largo plazo/la emisión de ^{137}Cs después de un accidente grave deberían quedar por debajo de los límites prescritos.

Consideración de los accidentes graves en el diseño

4.117. Los objetivos del análisis de los accidentes graves deberían ser:

- Evaluar la capacidad del diseño para resistir los accidentes graves y descubrir puntos vulnerables particulares. Ello supone la evaluación de los equipos que podrían utilizarse en la gestión de los accidentes, así como de la instrumentación que podría emplearse para monitorizar el curso del accidente.

- Evaluar la necesidad de dispositivos que podrían incorporarse al diseño¹⁷ de la central para prever defensa en profundidad en caso de accidentes graves.
- Especificar las medidas de gestión de accidentes que podrían adoptarse para mitigar los efectos de los accidentes.
- Establecer un programa de gestión de accidentes para aplicarlo en los casos de accidentes que sobrepasen la base de diseño y en situaciones de accidente grave.
- Proporcionar información de entrada para la planificación contra emergencias fuera del emplazamiento.

4.118. Cuando se trate de centrales nuevas, los accidentes graves deberían considerarse en la fase de diseño. Pero para las centrales que ya estén en funcionamiento debería prepararse un programa de gestión de accidentes graves que prevea el pleno uso de todos los equipos y procedimientos disponibles a fin de mitigar las consecuencias del accidente. Entre esas medidas podrían figurar el empleo de sistemas alternativos o diversos, procedimientos y métodos para hacer uso de equipos no cualificados como de seguridad, y el empleo de equipos externos para reemplazar temporalmente componentes normales. En otra publicación del OIEA [9] se dan detalles sobre el establecimiento y la aplicación de los programas de gestión de accidentes.

4.119. El APS debería servir para evaluar la efectividad de los dispositivos de diseño indicados y de las medidas de gestión de accidentes en cuanto a reducción del riesgo.

Planificación para emergencias

4.120. El análisis de los accidentes graves debería suministrar también datos a las autoridades civiles para la planificación y respuesta a emergencias fuera del emplazamiento.

¹⁷ Estos dispositivos previstos en el diseño podrían ser, entre otros, los siguientes:

- Colector del núcleo o zona de dispersión del núcleo y hormigón de la losa resistente a los daños por fusión del núcleo.
- Recombinadores de hidrógeno dimensionados para enfrentarse a la tasa de generación de hidrógeno que podría darse tras un accidente grave.
- Sistema de venteo de la contención dotado de filtros que funcionaría durante largo tiempo para impedir el fallo de la contención por sobrepresión tras un accidente grave.

4.121. Los resultados del análisis de los accidentes graves deberían servir para especificar los términos fuente que podrían usarse como base para la planificación relativa a emergencias exteriores.

4.122. Los términos fuente podrían emplearse también para demostrar la efectividad del uso de refugios, la ingestión de pastillas de yoduro potásico, las restricciones sobre alimentos y la evacuación.

ANÁLISIS PROBABILISTA DE SEGURIDAD

Introducción

4.123. El análisis probabilista de seguridad tecnológica proporciona un método completo y estructurado para la determinación de escenarios de accidente y la deducción de estimaciones cuantitativas de los riesgos. Los APS de las centrales nucleares se realizan generalmente a tres niveles, como sigue:

4.124. **APS de nivel 1**, en el que se determina la secuencia de sucesos que pueden originar daños en el núcleo, se estima la frecuencia de los daños al núcleo, y se obtienen ideas claras sobre las fortalezas y debilidades de los sistemas y procedimientos de seguridad previstos para impedir el deterioro del núcleo.

4.125. **APS de nivel 2**, en el que se determinan las maneras en que pueden ocurrir emisiones radiactivas de la central y se estima su magnitud y frecuencia. Este análisis aporta precisiones adicionales sobre la importancia relativa de las medidas de prevención y mitigación de accidentes como, por ejemplo, el uso de la contención del reactor.

4.126. **APS de nivel 3**, en el que se estiman los riesgos para la salud pública y otros riesgos sociales como la contaminación de tierras o de alimentos.

4.127. Se han realizado ya los APS de nivel 1 referentes a la mayor parte de las centrales nucleares de todo el mundo. Sin embargo, en los últimos años la norma que está surgiendo es la de realizar APS de nivel 2 para tipos múltiples de centrales nucleares. Hasta el momento, se han realizado relativamente pocos APS de nivel 3.

Uso del APS como parte del proceso de toma de decisiones.

4.128. Los resultados del APS deberían usarse como parte del proceso de diseño para evaluar el grado de seguridad de la central. Al tomar decisiones a este respecto se deberían tener en cuenta las precisiones aportadas por el APS juntamente con las derivadas del análisis determinista. Éste debería ser un proceso iterativo con el fin de cerciorarse de que se cumplen los requisitos y los criterios nacionales, que el diseño (según se especifica en el párrafo 4.139) está bien equilibrado y que el riesgo es el más bajo que puede razonablemente alcanzarse.

4.129. Los resultados del APS deberían servir para detectar los puntos débiles del diseño o el funcionamiento de la central. Estas debilidades se suelen descubrir considerando las aportaciones al riesgo provenientes de grupos de sucesos iniciadores o de la calibración de la importancia que tienen para el riesgo total los sistemas de seguridad y las contribuciones debidas a errores humanos. Cuando los resultados del APS indiquen que podrían efectuarse cambios en el diseño o en el funcionamiento de la central para reducir el riesgo, dichos cambios deberían incorporarse en la medida en que sean razonablemente realizables, habida cuenta de los costos y de los beneficios relativos de cualquier modificación.

4.130. Además, los resultados del APS deberían compararse con los criterios probabilistas de seguridad, cuando éstos hayan sido definidos para la central. Esto debería realizarse con respecto a todos los criterios probabilistas establecidos para la central, incluso los relativos a fiabilidad de los sistemas, deterioro del núcleo, emisiones de material radiactivo, efectos sobre la salud de los trabajadores, efectos sobre la salud pública y consecuencias fuera del emplazamiento, tales como la contaminación de tierras y las restricciones sobre alimentos.

4.131. Los resultados del APS deberían emplearse para establecer los procedimientos de operación durante accidentes y proporcionar información de partida para las especificaciones técnicas de la central. En particular, los resultados del APS deberían utilizarse para investigar las contribuciones al riesgo que podrían resultar de retirar del servicio componentes de equipo con fines de mantenimiento o prueba, así como la adecuación de la frecuencia de las actividades de vigilancia y prueba. El APS debería confirmar que los tiempos permitidos de puesta fuera de servicio no aumentan el riesgo de forma inaceptable, e indicar qué combinaciones de equipos fuera de servicio deberían evitarse.

4.132. Los resultados del APS de nivel 2 deberían servir para determinar si se han adoptado disposiciones suficientes con el fin de mitigar los efectos de un deterioro del núcleo, caso de que ocurriera. A este respecto debería considerarse si la contención es suficientemente sólida y los sistemas protectores como los de mezcla y recombinación del hidrógeno, los rociadores de la contención, y los sistemas de venteo de la contención, proporcionan un nivel adecuado de protección para prevenir una gran emisión de material radiactivo al medio ambiente. Además, el APS de nivel 2 debería utilizarse para determinar las medidas de gestión de accidentes que podrían ponerse en práctica a fin de mitigar los efectos de la fusión del núcleo. Esto podría incluir la especificación de las medidas adicionales que podrían tomarse para inyectar agua en la contención del reactor.

4.133. Los resultados de los APS de los niveles 2 y 3, si se dispone de ellos, deberían ponerse en conocimiento de las autoridades civiles como aporte de información técnica para las medidas de planificación sobre emergencias fuera del emplazamiento.

Requisitos aplicables a un APS

4.134. El APS debería emplearse a lo largo del diseño y del funcionamiento de la central como ayuda en el proceso de toma de decisiones relativas a la seguridad de la misma.

4.135. En el caso de una central nueva, el APS debería iniciarse preferiblemente en la fase de diseño conceptual, para comprobar que el grado de redundancia y diversidad previsto en los sistemas de seguridad es el adecuado, continuar a lo largo de la fase de diseño más minucioso para evaluar cuestiones más detalladas, y servir de apoyo para el buen funcionamiento de la central. Durante la fase de diseño debería existir un proceso iterativo que garantice que las precisiones detalladas resultantes del APS se incorporen a la labor de diseño.

4.136. Si se trata de una central ya existente, el APS debería realizarse como parte de una evaluación periódica de la seguridad, o bien como apoyo a las razones de seguridad tecnológica que avalen las modificaciones propuestas. Aunque los requisitos del APS siguen siendo los mismos, la base de datos puede ser diferente. Además, cuenta habida de la edad de la central, la vida operacional restante, el costo de las modificaciones propuestas y otras consideraciones afines, surgirán diferencias acerca de qué cambios sería razonable incorporar para reducir el riesgo.

4.137. El APS debería referirse al diseño o al modo de funcionar el diseño de la central, ya sea en realidad o según lo previsto, lo que debería especificarse claramente como punto de partida del análisis. El estado de la central puede fijarse tal como era en una fecha dada, o como será cuando se hayan concluido las modificaciones acordadas.

4.138. El APS debería proponerse como objetivos: determinar todas las secuencias de fallo que contribuyan al riesgo, determinar si hay puntos débiles en el diseño o el funcionamiento de la central; y evaluar la necesidad de modificaciones para disminuir el impacto de tales puntos débiles en la seguridad. Si el análisis no incluye todas las contribuciones al riesgo (por ejemplo, si omite sucesos externos o estados de parada), podrán ser incorrectas las conclusiones que se deduzcan sobre el nivel de riesgo de la central, el equilibrio de los sistemas de seguridad previstos y la necesidad de modificaciones en el diseño o el funcionamiento para disminuir el riesgo.

4.139. El APS debería determinar si los sistemas de seguridad cuentan con un grado adecuado de redundancia y diversidad, si la defensa en profundidad es suficiente y si el diseño en su conjunto está equilibrado. En un diseño equilibrado el APS debería poner de manifiesto que:

- Ningún dispositivo concreto previsto en el diseño contribuye desproporcionadamente al riesgo;
- Ningún grupo de sucesos iniciadores contribuye desproporcionadamente al riesgo;
- La consecución de un nivel general bajo de riesgo no depende de factores que impliquen incertidumbres significativas;
- Los dos primeros niveles de defensa soportan la carga primordial requerida para la seguridad;
- En cada nivel de defensa, ninguno de los sistemas de seguridad es desproporcionadamente más importante que los demás.

Una falta de equilibrio indica generalmente que existen oportunidades para una reducción del riesgo razonablemente realizable.

Alcance del APS

4.140. El APS debería estudiar las contribuciones al riesgo provenientes de todos los modos de funcionamiento de la central. No obstante, puede ser conveniente analizar por separado (y no hasta el mismo nivel) los regímenes de funcionamiento a potencia y de parada.

4.141. Si el APS se realiza solamente hasta el nivel 1, el núcleo es, por definición, el tema central del análisis. Si el APS se realiza hasta los niveles 2 ó 3, se pueden incluir en él las contribuciones al riesgo procedentes de otras fuentes de material radiactivo presentes en el emplazamiento, por ejemplo el combustible gastado y los desechos radiactivos. Estas fuentes ajenas al núcleo deberían ser incluidas también cuando lo que se quiere es examinar el riesgo total causado por la central para una persona próxima al emplazamiento.

4.142. En el APS se debería tomar como punto de partida el conjunto completo de los SIP, incluidos los de origen interno y externo. El análisis debería entonces proseguir para determinar la gama completa de secuencias de fallo que podrían contribuir al riesgo. Estas secuencias deberían comprender los fallos de componentes, la indisponibilidad de componentes durante actividades de prueba o de mantenimiento, los errores humanos, los fallos de causa común y, de ser posible, tener en cuenta el envejecimiento de los componentes.

Métodos de APS

4.143. Hasta la fecha se han realizado gran número de APS para una amplia variedad de diseños de centrales nucleares. En consecuencia, los métodos de APS están muy desarrollados, en particular los referentes al APS de nivel 1. Es preciso reconocer que el proceso de APS entraña incertidumbres. Las incertidumbres no son exclusivas del APS, se dan también en los análisis deterministas de seguridad. Sin embargo, los métodos APS ofrecen posibilidades de reconocer y cuantificar una gran parte de estas incertidumbres. Los métodos empleados en todo nuevo APS que se realice, deberían ajustarse a las mejores prácticas internacionales en uso.

4.144. En el proceso de APS se debería utilizar preferiblemente, de principio a fin, métodos basados en estimaciones óptimas. Esto incluiría el análisis realizado para respaldar los criterios de buen resultado de los sistemas de seguridad, la modelización de los fenómenos que podrían ocurrir en el interior de la contención como consecuencia del deterioro del núcleo, y el transporte del material radiactivo emitido al medio ambiente. Cuando esto no sea posible, deberían adoptarse supuestos razonablemente conservadores.

APS de nivel 1: Análisis de la frecuencia de deterioro del núcleo

4.145. El objetivo del APS de nivel 1 debería ser determinar la frecuencia global de deterioro del núcleo. Ello requiere una definición de lo que constituye deterioro del núcleo y la traslación de esta definición a los criterios

de fallo de los sistemas de seguridad. En la Ref. [10] se ofrece más información sobre los procedimientos para realizar un APS de nivel 1. En el análisis se debería especificar las secuencias de fallo que más contribuyen a dicha frecuencia, determinar los sistemas de seguridad más importantes para prevenir el deterioro del núcleo y determinar si es posible introducir modificaciones en el diseño o en el funcionamiento de la central para reducir el riesgo.

Sucesos iniciadores postulados

4.146. El punto de partida del APS debería ser la lista completa de SIP que podrían comprometer directamente, o en combinación con otros fallos, la seguridad nuclear. Los fallos consecutivos que se incluyen en el análisis determinista se tienen en cuenta, en el APS, al analizar la secuencia de sucesos y los sistemas.

4.147. El conjunto de SIP considerados debería comprender todos los sucesos externos e internos, incluso los de baja frecuencia, que pudieran ocurrir pero que no se tuvieron en cuenta al diseñar la central.

4.148. El análisis debería incluir los SIP que pudieran ocurrir en todos los modos de funcionamiento de la central y originar una emisión de material radiactivo de cualquiera de las fuentes presentes en el emplazamiento.

Especificación de los requisitos relativos a los sistemas de seguridad

4.149. Se deberían especificar, por cada uno de los SIP definidos, las funciones de seguridad que tienen que ejecutarse para impedir daños al núcleo. Estas funciones de seguridad son las mismas que las consideradas en el análisis base de diseño — esto es, la detección del suceso iniciador, la parada del reactor, la eliminación del calor residual y la protección de la contención. Sin embargo, los límites por encima de los cuales habría que considerar que la función de seguridad tecnológica ha fallado serían por regla general realistas, a diferencia de los límites conservadores definidos en el análisis base de diseño.

4.150. Deberían especificarse los sistemas de seguridad necesarios para cumplir esas funciones. Ello debería basarse en el análisis de transitorios con arreglo a estimaciones óptimas en vez del análisis conservador realizado para el análisis base de diseño. Debería especificarse el número de conjuntos de sistemas redundantes y diversos que se requieren para el funcionamiento.

4.151. Se pueden determinar los SIP que requieren las mismas (o muy parecidas) intervenciones de sistemas de seguridad. Para reducir el trabajo de análisis, es habitual agrupar estos SIP y analizarlos conjuntamente en el APS. (Ello es similar, pero no idéntico, al agrupamiento para el análisis determinista a que se refieren los párrafos 4.75 a 4.77). El grupo de sucesos iniciadores es representado entonces por el suceso iniciador que impone la respuesta más exigente a los sistemas de seguridad y se considera que la frecuencia es la suma de la de cada suceso iniciador del grupo. Cuando se agrupen los SIP, el agrupamiento debería realizarse de tal modo que no dé lugar a un grado inaceptable de pesimismo en el análisis. Esto podría suceder, por ejemplo, cuando el suceso representativo seleccionado tenga una frecuencia baja y todos los demás sucesos del grupo requieran prestaciones significativamente menos rigurosas de los sistemas de seguridad, pero con una suma de frecuencias mucho mayor.

Análisis de la secuencia de sucesos

4.152. En el análisis de la secuencia de sucesos se adoptan modelos lógicos para los grupos de sucesos iniciadores con el fin de determinar las secuencias de fallo que pueden ocurrir y causar el deterioro del núcleo. Estos modelos lógicos empiezan con la función de seguridad fundamental y estudian las funciones de seguridad requeridas por el grupo de sucesos iniciadores, los sistemas de seguridad y los distintos componentes de los sistemas de seguridad. Los modelos lógicos permiten determinar cómo se pueden combinar los fallos de componentes para conducir al fallo de la función de seguridad y al deterioro del núcleo.

4.153. El análisis de la secuencia de sucesos realizado para un grupo de sucesos iniciadores debería tratar de definir todas las combinaciones posibles de buen resultado o de fallo de los equipos de los sistemas de seguridad cuya consecuencia sería no poder mantener la central dentro de límites seguros, de tal modo que ocurriría un deterioro del núcleo.

4.154. En los APS más al uso, el estudio de la secuencia de sucesos se realiza mediante un análisis combinado de árboles de sucesos y árboles de fallos, ya que se ha constatado empíricamente que ésta es la forma más efectiva de manejar los extensos modelos lógicos necesarios para una central nuclear. No obstante, se puede efectuar el análisis utilizando solamente árboles de fallos o árboles de sucesos y, para el análisis de sucesos específicos, se pueden aplicar técnicas de análisis dinámico dependiente del tiempo.

4.155. Debería efectuarse una evaluación sistemática para especificar los fallos de los equipos de los sistemas de seguridad (y de los equipos relacionados o no relacionados con la seguridad, si estos fallos pudieran afectar a la secuencia) que podrían ocurrir como consecuencia del suceso iniciador; estos fallos se deberían incorporar en los modelos lógicos que representen las secuencias de sucesos posibles.

4.156. El análisis de la secuencia de sucesos debería abarcar todas las combinaciones posibles de equipos de los sistemas de seguridad que puedan intervenir para realizar las funciones de seguridad requeridas.

4.157. Puesto que algunos de los sistemas de seguridad existentes en una central nuclear comparten sistemas comunes de activación o sistemas comunes de apoyo tales como el suministro eléctrico, los equipos de instrumentación y control, y los sistemas de refrigeración, ello origina dependencias funcionales entre los sistemas de seguridad. Debería efectuarse una evaluación sistemática del diseño y funcionamiento de la central para cerciorarse de que tales interdependencias han sido definidas y modelizadas explícitamente en el análisis de la secuencia de sucesos o en el análisis de los sistemas.

Análisis de fallos de los sistemas de seguridad

4.158. El análisis de la secuencia de sucesos debería descender hasta el nivel de cada suceso básico particular. Estos sucesos básicos consisten generalmente en fallos de componentes, indisponibilidad de componentes durante actividades de mantenimiento o prueba, fallos de causa común en equipos redundantes y errores del operador.

4.159. En el análisis de fallos de los sistemas se deberían considerar todos los modos importantes de fallo de los distintos componentes de equipos de los sistemas de seguridad. Normalmente estos modos de fallo se habrían determinado ya gracias al análisis de modos de fallo y sus efectos que se realiza como parte de la evaluación del diseño. También se deberían incluir en el modelo de los sistemas todos los fallos consecutivos al SIP (si no se hubieran tenido ya plenamente en cuenta en los modelos de secuencias de sucesos).

4.160. Deberían determinarse todos los sistemas de apoyo necesarios e incluirse en el análisis de fallos de los sistemas, y las interdependencias que surjan por la existencia de sistemas de apoyo comunes se deberían representar explícitamente en los modelos lógicos.

4.161. A lo largo de la vida de la central pueden retirarse del servicio componentes determinados o conjuntos de equipos para pruebas, mantenimiento o reparaciones, y ello reducirá la disponibilidad del sistema de seguridad para realizar sus funciones. Tales retiradas deberían ser tenidas en cuenta explícitamente en el APS. Ello puede hacerse bien introduciendo sucesos básicos en los modelos lógicos para representar las indisponibilidades de equipo, o bien realizando múltiples procesos de APS.

Datos

4.162. Para cuantificar el análisis se necesitan datos sobre los siguientes temas:

- Frecuencias de los sucesos iniciadores,
- Probabilidades de fallo de los equipos,
- Duración y frecuencia de las retiradas de servicio de equipos,
- Probabilidades de fallos de causa común,
- Probabilidades de errores humanos.

4.163. Las frecuencias de los sucesos iniciadores y las probabilidades de fallo de equipos empleadas deberían ser las apropiadas para el diseño o el funcionamiento de la central. Deberían utilizarse, en la medida de lo posible, los datos específicos de la central. Cuando ello no sea posible, deberían usarse los datos resultantes del funcionamiento de centrales similares. Incluso, de no ser esto posible, deberían emplearse datos genéricos, siempre que pueda demostrarse que son relevantes. En cuanto a los sucesos iniciadores de baja frecuencia, debería aplicarse un buen criterio técnico.

4.164. Al especificar las tasas de fallo de equipos, deberían precisarse los límites de los equipos e incluirse todos los modos de fallo que sean relevantes. En el caso de una bomba, ello comprende los fallos de arranque, los fallos de funcionamiento durante el tiempo de trabajo especificado y las fugas en los sellos de la bomba.

4.165. Los datos estadísticos usados deberían abarcar todas las causas significativas de sucesos iniciadores y todos los modos relevantes de fallo de equipos.

4.166. Respecto de algunos de los temas considerados en el APS, en particular la frecuencia de sucesos iniciadores poco probables, tales como fallos de la vasija de presión o terremotos graves, no hay experiencia operacional apropiada. Si se considera que estos sucesos no suponen una contribución

significativa al riesgo, pueden descartarse, siempre que se aporte la correspondiente justificación. De no ser así, debería hacerse una buena apreciación técnica de sus frecuencias y exponerse las bases de tal apreciación. En particular, los métodos para realizar evaluaciones probabilistas del riesgo sísmico están bien establecidos y pueden ser adaptados a cualquier emplazamiento.

Fallos de causa común

4.167. Existe la posibilidad de que los componentes redundantes de los equipos de un sistema de seguridad fallen debido a una causa común y esto limita la fiabilidad del sistema. Tales fallos de causa común (FCC) pueden ser modelizados en el análisis a nivel del sistema de seguridad o a nivel de cada componente. Un modo de hacerlo es modelizar el FCC a nivel del sistema de seguridad introduciendo un suceso básico en el modelo lógico que representa el FCC del sistema. Hay una serie de enfoques para estimar la probabilidad del FCC, entre los que figura la utilización de datos derivados de la experiencia operacional y modelos teóricos tales como los métodos del factor beta y de las múltiples letras griegas.

4.168. Se deberían modelizar en el análisis los fallos de causa común que puedan ocurrir en sistemas de seguridad redundantes. Debería presentarse una justificación de los modelos de FCC y de los datos empleados en el APS. Siempre que ello sea posible, debería tenerse en cuenta la experiencia operacional de sistemas similares.

4.169. Los análisis previos y la experiencia operacional indican que hay un límite de la probabilidad de fallo de los sistemas de seguridad no diversos, que podría situarse en el intervalo de 10^{-3} a 10^{-5} fallos por demanda de actuación, en función del nivel de redundancia existente y de otros factores operacionales y de diseño. Ello debería quedar reflejado en el análisis.

Análisis de la fiabilidad humana

4.170. Los errores humanos pueden afectar tanto a la causa como a la frecuencia de una secuencia de sucesos. Pueden ocurrir antes, durante o después del inicio de la secuencia de sucesos y mitigar o agravar un accidente. Deberían modelizarse en el APS. Los datos sobre fiabilidad humana deberían obtenerse a partir de fuentes tales como los informes sobre sucesos ocurridos, los informes de mantenimiento, los informes de APS y las observaciones realizadas en simuladores.

4.171. Los errores humanos que puedan conducir a sucesos iniciadores se deberían especificar e incluir como parte de la frecuencia de sucesos iniciadores.

4.172. Los errores humanos que puedan originar fallos de los sistemas de seguridad o pérdida de funciones críticas de seguridad deberían modelizarse explícitamente en la secuencia de sucesos y en el análisis de fallos de los sistemas de seguridad.

4.173. Las probabilidades de error humano adoptadas deberían reflejar los factores que puedan influir en el comportamiento del operador, en particular el grado de estrés, el tiempo disponible para realizar la tarea, la disponibilidad de procedimientos operacionales, el nivel de capacitación y las condiciones ambientales. Todos ellos deberían quedar especificados en el análisis de tareas realizado como parte de la evaluación del diseño.

Cuantificación del análisis

4.174. El modelo lógico construido debería cuantificarse, utilizando los datos para determinar la frecuencia total de deterioro del núcleo y las contribuciones de los grupos de sucesos iniciadores. En la actualidad existe una serie de códigos de computación que pueden usarse para realizar este análisis.

4.175. En la cuantificación del análisis debería estimarse por deducción la importancia de los grupos de sucesos iniciadores, de los fallos de componentes, del fallo de los sistemas de seguridad y de los errores del operador, a fin de descubrir la procedencia de las contribuciones al riesgo y localizar posibles puntos débiles en el diseño o el funcionamiento de los sistemas de seguridad. Al efecto podrían emplearse, cuando proceda, mediciones cuantitativas de la importancia (como las de Birnbaum y Fussell-Vesely — véase la Ref. [10]). Ello debería ser respaldado por estudios de sensibilidad, cuando haya incertidumbres en los modelos y los datos.

Resultados del análisis de la frecuencia de daños al núcleo

4.176. Los resultados del análisis deberían ser evaluados para poder confiar en que proporcionan una representación adecuada del riesgo dimanante de la central. Si hay aspectos en los que se considere que las estimaciones del riesgo son excesivamente conservadoras u optimistas, deberían revisarse los análisis para hacerlos más realistas. Puede darse un conservadurismo excesivo si los criterios de buen resultado de los sistemas de seguridad se fundan en un

análisis conservador de transitorios base de diseño y en criterios conservadores de buen cumplimiento de las funciones críticas de seguridad, en vez de fundarse en las estimaciones óptimas recomendadas para el APS. Puede darse un optimismo excesivo si se descartan inadecuadamente sucesos iniciadores potenciales.

4.177. Los resultados del análisis deberían compararse con los criterios de seguridad relativos a la frecuencia de daños al núcleo propuestos para la central (cuando éstos hayan sido especificados). Si la frecuencia de daños al núcleo estimada para la central es inaceptablemente alta, se deberían introducir modificaciones en su diseño o su funcionamiento para reducir el riesgo.

4.178. Aun en el caso de que la frecuencia de daños al núcleo sea aceptablemente baja, los resultados del APS deberían ser examinados sistemáticamente para descubrir cualquier punto débil relativo en el diseño y el funcionamiento de la central, así como especificar las mejoras que podrían hacerse para reducir la frecuencia de daños al núcleo. Estas modificaciones deberían hacerse cuando sean razonablemente realizables. La apreciación de lo que sea razonablemente realizable dependerá de que el reactor esté en fase de diseño o de funcionamiento, y del costo de las modificaciones. Este proceso debería repetirse para intentar reducir la frecuencia de daños al núcleo hasta un nivel igual o inferior al objetivo de diseño (cuando éste haya sido definido), y para conseguir un diseño equilibrado.

APS de nivel 2: Análisis de la progresión de un accidente desde el daño al núcleo hasta la emisión de material radiactivo

4.179. En esta parte del análisis se considera la progresión del accidente desde el comienzo del deterioro del núcleo y se estudian los fenómenos que podrían ocurrir hasta llegar al fallo de la contención y a la emisión de material radiactivo al medio ambiente. En la Ref. [11] figura información detallada sobre los procedimientos para realizar un APS de nivel 2.

4.180. En el análisis se estudia la efectividad del diseño y las medidas de gestión de accidentes adoptadas para mitigar los efectos del deterioro del núcleo, y se formulan estimaciones de la frecuencia de una gran emisión de material radiactivo al medio ambiente, que pueden ser comparadas con los criterios probabilistas (si han sido definidos).

Definición de los estados de deterioro de la central

4.181. Las secuencias de sucesos especificadas en un APS de nivel 1 que pudieran originar daños al núcleo deberían agruparse en estados de deterioro de la central (EDC), que se definen en función de los factores que influyen en la respuesta de la contención o en las emisiones de material radiactivo al medio ambiente. Entre estos factores figuran generalmente el tipo de suceso iniciador ocurrido, la presión del sistema de refrigeración del reactor, el estado de los sistemas de refrigeración de emergencia del núcleo y de protección de la contención, y la integridad de la contención.

Modelización de la progresión del deterioro del núcleo

4.182. En el análisis de la progresión del accidente desde el deterioro del núcleo hasta la emisión de material radiactivo se deberían modelizar los fenómenos significativos que pongan en riesgo la integridad de la contención o influyan en la emisión. Estos fenómenos se indican en el párrafo 4.113 y se describen con mayor detalle en la bibliografía (véanse, por ejemplo, los informes del OIEA y de la AEN de la OCDE sobre APS de nivel 2, Refs. [11,12], respectivamente).

4.183. En el análisis se debería seguir un método lógico que modelice la progresión de las secuencias de sucesos desde el deterioro del núcleo hasta la emisión radiológica. Esto se hace usualmente mediante un análisis del árbol de sucesos en que se modeliza la secuencia del accidente en varios intervalos temporales y se formula un conjunto de preguntas nodales para modelizar la secuencia de sucesos que tiene lugar. Es necesario respaldar la construcción del árbol de sucesos con cálculos termohidráulicos y la modelización de la emisión de productos de fisión y su transporte dentro de la contención.

4.184. El análisis del árbol de sucesos debería incluir un número de intervalos temporales y nodos suficiente para permitir el examen de los fenómenos significativos que pudieran ocurrir dentro de la contención. La nueva norma que se está adoptando es especificar unos 20 o 30 nodos, aunque algunos análisis han incluido muchos más (p. ej. NUREG-1150 [13]). Estas preguntas nodales serán las mismas con respecto a todos los árboles de sucesos trazados para cada uno de los EDC; sin embargo, los árboles de sucesos reales diferirán en sus detalles para cada uno de los estados definidos, como consecuencia de las diferentes situaciones iniciales caracterizadas por el EDC.

4.185. Los puntos finales de los árboles de sucesos indican la secuencia de sucesos que ha ocurrido y el estado de la contención. Las posibilidades son que la contención esté intacta o que haya fallado. Los posibles modos de fallo son: derivación, fallo del aislamiento (estos dos modos están modelizados en la definición de EDC), fugas, roturas o fusión que atraviese la losa de base. La liberación resultante de material radiactivo también dependerá de que el fallo de la contención haya ocurrido en fase temprana o tardía de la secuencia de sucesos.

Datos

4.186. Los datos de interés para la cuantificación del análisis del árbol de sucesos son las probabilidades condicionales en los puntos de ramificación. Hay una considerable incertidumbre en cuanto a los fenómenos que podrían ocurrir y, por consiguiente, las probabilidades adoptadas se basan frecuentemente en apreciaciones de expertos.

4.187. La evaluación debería confirmar que las bases para la formulación de esas apreciaciones de expertos son sólidas y que se ha explicado el fundamento de la apreciación y demostrado su validez en todo lo posible. Para ello debería tenerse en cuenta el análisis termohidráulico realizado, los análisis de otras centrales similares y los datos de investigación que sean aplicables. Al cuantificar los árboles de sucesos de la contención se deberían tener en cuenta las interdependencias de los distintos fenómenos que están siendo modelizados.

Análisis del comportamiento de la contención

4.188. Una cuestión importante que hay que examinar es cómo se comportará la contención frente a las cargas que actúen sobre ella a causa de un deterioro del núcleo y cómo ocurrirá el fallo.

4.189. En el análisis debería tratarse la derivación directa de la contención (resultante, por ejemplo, de la rotura de un tubo del generador de vapor o de un LOCA en sistemas interconectados con descarga fuera de la contención) y el fallo del sistema de aislamiento de la contención. Normalmente estos supuestos se incluirían en la definición de los EDC.

4.190. Debería realizarse un análisis estructural para determinar cómo se comportará la contención frente a las condiciones de presión y temperatura que podrían producirse a causa de explosiones de vapor, gases no condensables

o combustiones de hidrógeno. Este examen debería basarse en el diseño real de la contención teniendo en cuenta las puertas, penetraciones, juntas de estanqueidad y otras posibles áreas débiles. Deberían especificarse los modos posibles de fallo de la contención y estimarse la probabilidad condicional de fallo de la contención en función de la presión y la temperatura. Esta información puede servir después para estimar las probabilidades condicionales de fallo empleadas para cuantificar los árboles de sucesos.

4.191. También debería realizarse un análisis para determinar cómo puede fallar la losa base de la contención a consecuencia de la interacción del núcleo fundido y el hormigón que tendría lugar tras una ruptura de la vasija de presión. Deberían hacerse estimaciones de la probabilidad condicional de fallo de la losa en función del nivel de calor residual y de la refrigeración disponible para el material fundido. Habría que prestar especial atención en el caso en que la losa de la contención tenga compartimentos adicionales superiores, de modo que la penetración de la losa pudiera originar una emisión radiactiva por vías que carezcan de filtración.

Análisis del término fuente

4.192. Generalmente, en el análisis de los árboles de sucesos hay un gran número de puntos finales y éstos se suelen agrupar en categorías de emisión y/o de términos fuente con similares características radiológicas y consecuencias fuera del emplazamiento.

4.193. La definición de las categorías de emisión debería incluir factores tales como la cantidad de cada uno de los isótopos considerados, el momento, duración, localización, contenido energético y distribución del tamaño de partículas.

4.194. Los términos fuente deberían determinarse para cada una de las categorías de descarga definidas. A este respecto se deberían tener en cuenta los factores que afectan al término fuente, entre ellos la volatilidad de los radionucleidos, las emisiones desde el combustible, la retención de productos de fisión en el sistema de refrigeración del reactor y la retención de productos de fisión en el interior de la contención.

4.195. La frecuencia de cada una de las categorías de emisión debería calcularse sumando las frecuencias correspondientes a cada uno de los puntos finales de los árboles de sucesos asignados a esa categoría. Cuando el APS incluya las emisiones de todas las fuentes de material radiactivo presentes en el

emplazamiento, deberían tenerse en cuenta en este punto las emisiones procedentes de las fuentes exteriores al núcleo del reactor. Ello puede entrañar la definición de categorías adicionales de emisión que generalmente tendrían menor impacto fuera del emplazamiento pero mayor frecuencia que las correspondientes a un núcleo deteriorado.

Resultados del APS de nivel 2

4.196. Los resultados del APS de nivel 2 generalmente se presentan en forma de tabla de categorías de términos fuente o de categorías de emisión junto con sus frecuencias. Las categorías de término fuente y/o de descarga se definen con arreglo a su composición de radionucleidos (reunidos en grupos de productos de fisión según sus características físicas y químicas comunes), así como a las características de la emisión (momento en que ocurre tras el inicio del accidente, duración, altura y contenido energético). A partir de esta información se puede deducir la frecuencia de una emisión grande o de una emisión grande y temprana para compararla con los criterios probabilistas (si han sido definidos). Grande se define como un valor mayor que una cantidad determinada de material radiactivo, a menudo especificada en forma de fracción del inventario radiactivo del núcleo.

4.197. Al igual que otras partes del APS, los resultados del análisis de nivel 2 deberían usarse para determinar las principales contribuciones al riesgo y las modificaciones que pueden introducirse en el diseño o el funcionamiento de la central para disminuir el riesgo. A este respecto se deberían tener en cuenta las importantes incertidumbres fenomenológicas inherentes a un APS de nivel 2. Esas modificaciones podrían referirse a sistemas de control del hidrógeno (a fin de que tengan una capacidad adecuada para responder a la tasa de generación de hidrógeno tras el deterioro del núcleo), los sistemas de venteo provistos de filtros en la contención para prevenir sobrepresiones prolongadas en ella, o los sistemas específicos para la refrigeración del núcleo fundido. Tales modificaciones deberían incorporarse al diseño cuando sea razonable realizarlas, habida cuenta de los costos y beneficios.

Gestión de accidentes en el emplazamiento

4.198. En el transcurso del accidente el operador puede tomar medidas para impedir su progresión o para reducir sus efectos. Ejemplos de tales medidas de gestión de accidentes que frecuentemente se incluyen en el análisis son la apertura de las válvulas de alivio para reducir la presión en el circuito primario y evitar la expulsión a alta presión de material fundido de la vasija del reactor,

así como la aportación de agua a la contención para que sirva como medio refrigerante una vez que el núcleo fundido se haya derramado desde el circuito primario.

4.199. El APS de nivel 2 debería emplearse para determinar qué medidas de gestión de accidentes son posibles con el fin de mitigar los efectos de una fusión del núcleo. Estas medidas deberían incluir las disposiciones que sea posible adoptar para respaldar la función de la contención o limitar las emisiones de material radiactivo que pudieran ocurrir. Tales medidas de gestión de accidentes deberían incorporarse a las instrucciones de operación de emergencia de la central, y se debería impartir capacitación a los operadores de la misma que tengan la responsabilidad de ejecutarlas. Las medidas de gestión de accidentes graves deberían ser compatibles con los equipos, la instrumentación y los medios de ayuda para el diagnóstico que los operadores de la central puedan razonablemente utilizar en tales circunstancias.

APS de nivel 3: Análisis de las consecuencias fuera del emplazamiento

4.200. En el análisis de las consecuencias fuera del emplazamiento se modeliza la emisión de radionucleidos desde la central nuclear, su transferencia a través del medio ambiente y sus consecuencias para la salud pública y la economía. En la Ref. [14]. figura información más detallada sobre los procedimientos para realizar un APS de nivel 3. El análisis debería a) proporcionar estimaciones del riesgo individual de muerte de un miembro de la población que viva cerca del emplazamiento, b) estudiar una serie de consecuencias fuera del emplazamiento, entre ellas los efectos tempranos y tardíos en la salud de los miembros de la población y c) considerar otras consecuencias económicas.

Agrupación de términos fuente

4.201. Como se expone en los párrafos 4.192 a 4.196 supra, las secuencias de fallo definidas en el APS de nivel 2 se agrupan normalmente en categorías de emisión, que tienen características similares en cuanto a su problemática de dispersión atmosférica y consecuencias fuera del emplazamiento. El conjunto de las categorías de emisión definidas debería representar el espectro de las emisiones de material radiactivo que pudiera originar la central. Estas categorías se definen normalmente atendiendo a la composición de los radionucleidos emitidos, clasificados según su volatilidad. Además, la categoría de emisión debería definir también el tiempo que transcurre desde que ocurre el suceso iniciador hasta que comienza la emisión, y la duración de la misma, puesto que son datos relevantes para la planificación de emergencia fuera del

emplazamiento. La frecuencia de la categoría de emisión debería calcularse a partir de la suma de todos los puntos finales de los árboles de sucesos de la contención pertenecientes a la categoría de la emisión.

Modelización de la dispersión atmosférica

4.202. Existe cierto número de códigos de computación para realizar el análisis de las consecuencias fuera del emplazamiento. Estos códigos requieren como entrada datos específicos sobre la central y el emplazamiento, entre ellos los referentes a categorías y frecuencias de emisiones así como datos meteorológicos, demográficos, agrícolas y económicos sobre el emplazamiento y sus alrededores. Los códigos modelizan el transporte de radionucleidos en el medio ambiente incluso su dispersión atmosférica, depósito, resuspensión, vías en la cadena alimentaria y vías modelo de exposición (radiactividad de la nube, inhalación, contaminación, depósito sobre el terreno, resuspensión e ingestión), con el fin de determinar los efectos sobre la salud de la población y las consecuencias económicas fuera del emplazamiento. El OIEA ha llevado a cabo un examen de los códigos disponibles para el análisis de las consecuencias fuera del emplazamiento, (véase la Ref. [14]).

Datos meteorológicos

4.203. Deberían especificarse los datos meteorológicos del emplazamiento. Éstos deberían basarse en los datos recogidos en las proximidades del emplazamiento a lo largo de una serie de años, e incluir generalmente la dirección y velocidad del viento, la clase de estabilidad, la pluviometría y profundidad de la capa de mezcla. (Los datos precisos dependerían del código empleado).

Datos demográficos, agrícolas y económicos

4.204. Deberían especificarse los datos demográficos, agrícolas y económicos del emplazamiento. Estos datos se basarían normalmente en la información nacional, complementada con datos de encuestas locales cerca del emplazamiento. Los datos necesarios dependerían de los efectos sobre la salud y los factores económicos que se seleccionen para incluirlos en el análisis. La forma de disponer esta información para su procesamiento dependerá de las necesidades específicas del código de computación empleado.

Resultados de las estimaciones del riesgo social

4.205. Los resultados de las estimaciones del riesgo social deberían compararse con los criterios de riesgo cuando éstos hayan sido definidos para la central.

4.206. Los resultados de las estimaciones del riesgo social deberían ponerse en conocimiento de las autoridades civiles como aportes técnicos a su proceso de toma de decisiones sobre las medidas de planificación para emergencias fuera del emplazamiento.

Planificación para emergencias fuera del emplazamiento

4.207. Por planificación y preparación para emergencias se entienden las actividades que pueden realizarse dentro y fuera del emplazamiento de la central para proteger a los trabajadores y a los miembros de la población contra los efectos de una emisión de material radiactivo de la central. La estrategia de las contramedidas se debería investigar aplicando APS de nivel 3, si se dispone de él. Este análisis debería incluir un examen de los beneficios de medidas a corto plazo como uso de refugios, evacuación y toma de pastillas de yoduro potásico, así como de la necesidad de contramedidas a largo plazo tales como las restricciones sobre alimentos, el realojamiento y la descontaminación de tierras. En este análisis se debería considerar también la forma de iniciación de las contramedidas — si se toman automáticamente, o en función del estado de la central, o sobre la base de la dosis.

4.208. Los resultados del APS de nivel 3 deberían usarse como aporte para la preparación del plan de emergencia y como medio de evaluar la eficacia relativa de los elementos integrantes de la planificación para emergencias.

Validación del APS

4.209. Este análisis requiere el uso de numerosos métodos de cálculo. Éstos van desde los modelos lógicos de árboles de sucesos y de fallos empleados para analizar las secuencias de sucesos, hasta los modelos de los fenómenos que pudieran ocurrir dentro de la contención a continuación del deterioro del núcleo, y los modelos de transporte de radionucleidos en el medio ambiente, para determinar sus efectos sobre la salud y la economía. Estos métodos de cálculo deberían ser validados para demostrar que son una representación adecuada de los procesos que tengan lugar. El tema se trata en la sección sobre evaluación de los códigos de computación empleados, que figura más adelante.

4.210. Se está convirtiendo en práctica normal que la entidad explotadora encargue un examen independiente por homólogos del APS a un organismo exterior, frecuentemente de otro país, para asegurarse con cierto grado de confianza de que el alcance, la modelización y los datos son los adecuados, así como de que están en conformidad con las mejores prácticas al uso en materia de APS a nivel mundial.

Utilización del APS

Presentación de los resultados del APS

4.211. Los resultados del APS deberían ser examinados para determinar las secuencias de fallos que más contribuyan al riesgo. En algunos casos, el APS puede indicar que una de las contribuciones es dominante, pero exámenes posteriores pueden sugerir que esa posición dominante se debe más a supuestos excesivamente conservadores en esa parte del APS que a un efecto relativo del diseño del reactor. En tal caso, debería considerarse la posibilidad de revisar dichas partes del análisis a fin de proporcionar una mejor estimación del riesgo.

Un APS vivo

4.212. El APS debería utilizarse a lo largo de la vida de la central como fuente de datos de entrada en el proceso de toma de decisiones. Durante la vida operacional de una central nuclear se suelen hacer modificaciones en el diseño de sus sistemas de seguridad o en su forma de funcionamiento, por ejemplo un cambio en su configuración durante períodos de mantenimiento y pruebas. Estas modificaciones podrían repercutir en el nivel de riesgo de la central. En el curso de su funcionamiento se obtendrán datos estadísticos sobre las frecuencias de sucesos iniciadores y las probabilidades de fallo de los componentes. Asimismo, pueden aparecer nueva información y métodos y herramientas más perfeccionados, que tal vez modifiquen algunos de los supuestos hechos en el análisis y, por consiguiente, las estimaciones del riesgo resultantes del APS.

4.213. En consecuencia, el APS debería mantenerse suficientemente actualizado durante toda la vida de la central para que sea útil en el proceso de toma de decisiones. En esa puesta al día se deberían tener en cuenta los cambios en el diseño y el funcionamiento de la central, la nueva información técnica, los métodos y herramientas más perfeccionados que vayan apareciendo y los nuevos datos deducidos del funcionamiento de la central. El

estado del APS debería examinarse regularmente para cerciorarse de que sigue siendo un modelo representativo de la central.

4.214. Los datos deberían ser recopilados por los operadores a la largo de la vida de la central para comprobar o actualizar el análisis. Entre ellos se deberían incluir los datos estadísticos sobre frecuencias de sucesos iniciadores, tasas de fallo de los componentes y tiempos de indisponibilidad durante los períodos de prueba, mantenimiento o reparación. El análisis debería ser evaluado a la luz de los nuevos datos.

4.215. Se debería impulsar la elaboración de un APS vivo como ayuda en el proceso de toma de decisiones durante el funcionamiento normal de la central. Ello incluye actividades tales como la planificación de las paradas de mantenimiento, en cuyo caso el APS podría servir como ayuda para asegurarse de que el riesgo dimanante de estas actividades es adecuadamente bajo. La experiencia demuestra que un APS vivo de esa naturaleza puede ser de gran ayuda para la entidad explotadora, y su uso está generalmente bien visto por los órganos reguladores.

Limitaciones del APS

4.216. El APS es una pieza clave en la evaluación del diseño y el proceso de análisis de seguridad tecnológica, ya que proporciona un modelo de riesgo integrado para la central en su totalidad y permite una evaluación congruente tanto de la frecuencia como de las consecuencias de los posibles escenarios de accidente. No obstante, el APS tiene limitaciones que es preciso entender.

4.217. En particular, el APS no debería considerarse como un sustitutivo de la evaluación del diseño de la obra de ingeniería ni del enfoque determinista del diseño. Más bien, el APS debería verse como una herramienta que proporciona apreciaciones claras sobre el nivel de riesgo dimanante de la central. Estas apreciaciones deberían utilizarse en el proceso de toma de decisiones para complementar las derivadas del análisis determinista.

4.218. En los modelos y los datos empleados en el APS existen incertidumbres. Esta incertidumbre es relativamente menor en cuanto a las probabilidades de fallo de componentes deducidas de una gran base de datos o de la experiencia operacional pertinente. Sin embargo, puede ser mucho mayor, e incluso imposible de cuantificar en varios otros aspectos, en particular los siguientes:

- Frecuencias de sucesos iniciadores y tasas de fallo de componentes cuando no existan datos de experiencia operacional.
- Frecuencia y movimientos del suelo asociados a grandes sismos.
- Modelización de fallos de causa común.
- Modelización de errores humanos.
- Modelización de los fenómenos que podrían ocurrir en accidentes graves.
- Estimación de las consecuencias fuera del emplazamiento de las emisiones de material radiactivo de la central.

Es necesario reconocer esta incertidumbre a la hora de utilizar los resultados del APS en el proceso de toma de decisiones. Los resultados del APS deberían contar con el respaldo de un análisis de incertidumbres o, por lo menos, de estudios de sensibilidad.

Criterios probabilistas de seguridad

Establecimiento de los criterios

4.219. Cuando los resultados del APS vayan a usarse como apoyo en el proceso de toma de decisiones debería establecerse un marco formal para hacerlo. Los detalles de este proceso dependerán de la finalidad de la aplicación concreta del APS, la naturaleza de la decisión y los resultados del APS que se utilicen. Cuando vayan a utilizarse los resultados numéricos del APS, deberían establecerse algunos valores de referencia con los cuales comparar estos resultados.

4.220. Cuando el fin del APS sea determinar los factores dominantes que contribuyen al riesgo o elegir entre varias opciones de diseño y configuraciones de la central, puede no ser necesario un valor de referencia.

4.221. No obstante, cuando el fin del APS sea servir para llegar a un juicio racional sobre si i) es aceptable el riesgo calculado, ii) es aceptable un cambio propuesto en el diseño o el funcionamiento de la central, o iii) si es necesario un cambio para reducir el nivel de riesgo, se deberían establecer criterios probabilistas de seguridad para dar orientación a los responsables del diseño, los operadores y las instancias reguladoras sobre el nivel de seguridad tecnológica que se desea para la central. Estos criterios también servirán para definir las metas que tendrán que alcanzar esos diseñadores, operadores y reguladores en el cumplimiento de sus respectivas funciones para la producción de energía nucleoelectrónica segura.

4.222. Un APS proporcionará medidas numéricas del riesgo a varios niveles, conforme al nivel de consecuencias calculado. Pueden establecerse criterios de seguridad probabilistas en relación con cualquiera de esas medidas o con todas ellas como se indica seguidamente:

- La probabilidad de fallo de las funciones de seguridad o de los sistemas de seguridad (nivel 0);
- La frecuencia de deterioro del núcleo (nivel 1);
- La frecuencia de una emisión específica (p. ej. cantidad, isótopos) de material radiactivo de la central o la frecuencia en función de la magnitud de la emisión (nivel 2);
- La frecuencia de efectos específicos sobre la salud de miembros de la población o las consecuencias medioambientales (nivel 3).

4.223. En la Ref. [15] se presenta un posible marco para la especificación de los criterios probabilistas de seguridad en el que se define un umbral de tolerabilidad por encima del cual el nivel de riesgo sería intolerable, y un objetivo de diseño, por debajo del cual el riesgo sería generalmente aceptable. Entre estos dos niveles hay una región en la que el riesgo sería aceptable sólo si se han tomado todas las medidas razonablemente factibles para reducir el riesgo. Aunque este enfoque ha sido adoptado en algunos países, no hay consenso internacional sobre su aplicación y es más habitual encontrar los criterios probabilistas de seguridad tecnológica formulados como objetivos, metas, fines perseguidos, directrices o valores orientativos de referencia. Además, no hay consenso internacional sobre los valores numéricos de los niveles de riesgo que corresponden al umbral de tolerabilidad o a los objetivos del diseño.

Valores numéricos

4.224. Basándose en la experiencia actual de diseño y funcionamiento de centrales nucleares, el INSAG ha propuesto valores numéricos que pueden alcanzarse con los diseños existentes y los diseños que se proyectan de dichas centrales.

4.225. *Probabilidad de fallo de una función o de un sistema de seguridad:* Pueden fijarse objetivos probabilistas a nivel de una función o de un sistema de seguridad. Son útiles para comprobar la adecuación del grado de redundancia y diversidad previsto. Tales objetivos serán específicos del diseño de cada central, por lo que no se da aquí ninguna orientación. La evaluación de la seguridad debería servir para comprobar si estos objetivos se han cumplido. En caso negativo, el diseño puede todavía ser aceptable siempre que se hayan

satisfecho criterios de más alto nivel; no obstante, debería prestarse especial atención a los sistemas de seguridad en cuestión para ver si puede introducirse alguna mejora razonablemente factible.

4.226. *Frecuencia de deterioro del núcleo*: A este efecto, el INSAG (Ref. [14]) ha propuesto los siguientes objetivos:

- 10^{-4} por reactor-año para las centrales existentes,
- 10^{-5} por reactor-año para las centrales futuras.

4.227. La frecuencia de daños al núcleo es la medida del riesgo más común, puesto que la mayoría de las centrales nucleares han sido sometidas a un APS de nivel 1, por lo menos, y la metodología está bien establecida. En muchos países, estos valores numéricos se han utilizado, ya sea oficial u oficiosamente, como criterios probabilistas de seguridad.

4.228. *Gran emisión de material radiactivo fuera del emplazamiento*: Una gran emisión de material radiactivo, que tuviera graves consecuencias para la sociedad y requiriese la puesta en práctica de medidas de emergencia fuera del emplazamiento, puede definirse de varias maneras, entre ellas las siguientes:

- En forma de cantidades absolutas (en Bq) de los nucleidos más significativos emitidos,
- En forma de una fracción del inventario del núcleo,
- En forma de dosis especificada para la persona más expuesta fuera del emplazamiento,
- En forma de emisión que tenga consecuencias inaceptables.

4.229. El INSAG ha propuesto también criterios probabilistas de seguridad para una gran emisión radiactiva [4]. Los objetivos que fija son los siguientes:

- 10^{-5} por reactor-año para las centrales existentes,
- 10^{-6} por reactor-año para las centrales futuras¹⁸.

¹⁸ En la publicación INSAG-3 Rev.1 [4], más bien que criterios probabilistas de seguridad, se establece como objetivo para las centrales nucleares futuras la práctica eliminación de las secuencias de accidentes que pudieran dar lugar a grandes emisiones radiactivas tempranas, mientras que los accidentes graves que pudieran conllevar fallos tardíos de la contención serían considerados en la fase de diseño con supuestos realistas y un análisis basado en estimaciones óptimas, de forma que sus consecuencias requerirían solamente medidas de protección limitadas en el espacio y el tiempo.

4.230. Aunque no hay consenso sobre lo que constituye una gran emisión fuera del emplazamiento, en varios países se han especificado criterios numéricos similares.

4.231. *Efectos sobre la salud de miembros de la población:* El INSAG no ha dado ninguna orientación sobre los objetivos referentes a los efectos sobre la salud de miembros de la población. En algunos países se adopta para el riesgo de muerte de un miembro de la población un objetivo de 10^{-6} por reactor-año.

ESTUDIOS DE SENSIBILIDAD Y ANÁLISIS DE INCERTIDUMBRES

4.232. La utilización de códigos basados en estimaciones óptimas, recomendada para los análisis de seguridad tanto deterministas como probabilistas debería complementarse con estudios de sensibilidad y/o análisis de incertidumbres.

4.233. A fin de determinar los parámetros importantes necesarios para el análisis y demostrar que no hay cambio brusco en el resultado del análisis para una variación realista de los datos de entrada (efectos de corte abrupto), se deberían efectuar estudios de sensibilidad, que incluyen la variación sistemática de las variables y los parámetros de modelización usados como aporte de entrada al código.

4.234. Los estudios de incertidumbres en el contexto del análisis determinista de seguridad se entienden como combinaciones estadísticas de la influencia de las condiciones de la central, los modelos de cálculo y los fenómenos asociados sobre los resultados. Estos estudios deberían servir para confirmar que los parámetros reales de la central estarán dentro de los límites marcados por los resultados del cálculo más la incertidumbre asociada, con un alto grado especificado de confianza. Para estimar las incertidumbres se usa generalmente una combinación de estudios de sensibilidad, comparaciones entre códigos, comparaciones entre códigos y datos y apreciaciones de expertos.

4.235. Debería prepararse también para el APS un análisis de incertidumbres, dado que es un componente clave del mismo. La determinación y análisis de incertidumbres es una virtud fundamental del APS. Las incertidumbres también están presentes en el análisis determinista, pero no son habitualmente consideradas ni analizadas. Más bien, se recurre deliberadamente al conservadurismo en un intento de responder a la incertidumbre. No obstante, el grado de incertidumbre en los análisis deterministas no es uniforme y puede

dar lugar a análisis discordantes. El valor de la metodología APS reside en que complementa el enfoque determinista y permite expresar completamente las incertidumbres. En tal caso, las incertidumbres deberían reflejar también intervalos de probabilidad de los sucesos iniciadores y de probabilidad de fallo de los componentes.

EVALUACIÓN DE LOS CÓDIGOS DE CÁLCULO EMPLEADOS

4.236. En el análisis de seguridad se emplea un gran número de códigos. Entre ellos figuran generalmente:

- Códigos de análisis radiológico para estimar las dosis a trabajadores,
- Códigos de física neutrónica para modelizar el comportamiento del núcleo del reactor,
- Códigos del comportamiento del combustible, con las que se modeliza el comportamiento de los elementos combustibles en funcionamiento normal y después de accidentes,
- Códigos termohidráulicos para modelizar el comportamiento del núcleo del reactor y los sistemas de refrigeración conexos durante el funcionamiento normal y después de accidentes,
- Códigos termohidráulicos para modelizar el comportamiento de la presión y la temperatura en la contención después de un LOCA o una rotura en una tubería del secundario,
- Códigos estructurales para modelizar el comportamiento tensión-deformación de los componentes y estructuras sometidos a cargas y a combinaciones de cargas,
- Códigos de análisis de accidentes graves con los que se modeliza la progresión de la secuencia de un accidente desde el deterioro del núcleo hasta el fallo de la contención,
- Códigos de análisis radiológico para modelizar el transporte de material radiactivo dentro de la central, y desde ella, con el fin de determinar sus efectos sobre los trabajadores y los miembros de la población,
- Códigos probabilistas con los que se establece un modelo lógico para definir las secuencias de accidente que podrían ocurrir a raíz de un SIP y estimar sus frecuencias.

4.237. Muchos de los códigos de cálculo que se elaboran en la actualidad combinan varios de los modelos anteriores en la misma versión.

4.238. Todos los códigos de computación empleados en el análisis de seguridad deberían validarse y verificarse. Los métodos utilizados en cada código de cálculo deberían ser los adecuados para el fin perseguido, y las ecuaciones físicas y lógicas determinantes deberían estar correctamente aplicadas en el código.

4.239. En lo referente a los códigos de computación, debería confirmarse que:

- Los modelos físicos usados para describir los procesos están justificados, junto con las hipótesis simplificadoras asociadas.
- Las correlaciones utilizadas para representar los procesos físicos están justificadas y sus límites de aplicabilidad, especificados.
- Los límites de aplicación del código se han precisado. Esto es importante cuando el método de cálculo se ha concebido solamente para modelizar procesos físicos a la largo de un intervalo definido, y no debería aplicarse fuera de este intervalo.
- Los métodos numéricos utilizados aportarían normalmente una solución suficientemente exacta.
- Se ha seguido un planteamiento sistemático en el diseño, codificación, prueba y documentación del código de computación.
- La codificación fuente ha sido evaluada en relación con la especificación del código. (Se reconoce que esto puede no ser realizable en el caso de códigos muy extensos).

4.240. En cuanto a la información de salida de los códigos, debería confirmarse que sus predicciones se han comparado con:

- Los datos experimentales referentes a los fenómenos significativos modelizados. Esto debería incluir una comparación con efectos considerados por separado y experimentos “integrales” de más alcance.
- Los datos de la central, incluidas las pruebas realizadas durante la puesta en servicio o la puesta en marcha, y en el curso de sucesos operacionales o accidentes.
- Otros códigos elaborados independientemente y que sigan métodos diferentes. Esto es particularmente importante para la modelización de fenómenos en accidentes graves.
- Problemas estándar y/o referentes numéricos con resultados suficientemente exactos.

4.241. Todo código debería ser validado para cada aplicación hecha en el análisis de seguridad tecnológica.

4.242. Cabe señalar que existe ya un programa de validación para algunos de los códigos elaborados. Ahora bien, este programa puede ser incompleto en el caso de códigos que estén en preparación o que modelicen algunos fenómenos de accidentes graves cuya comprensión no es completa.

4.243. Respecto a los usuarios del código, debería cuidarse de que:

- Hayan recibido la capacitación adecuada y comprendan el código,
- Tengan suficiente experiencia en el uso del código y entiendan a fondo su uso y limitaciones,
- Dispongan de directrices adecuadas para el uso del código,
- Hayan empleado (siempre que sea posible) el código en problemas normales antes de comenzar el trabajo de análisis de seguridad.

4.244. Con respecto al empleo del código de cálculo, debería confirmarse que:

- La nodalización y los modelos de la central proporcionan una buena representación del comportamiento de la misma,
- Los datos de entrada son correctos,
- La información de salida del código se entiende y usa correctamente.

5. VERIFICACIÓN INDEPENDIENTE

5.1. La finalidad de la verificación independiente de la seguridad tecnológica es determinar que la evaluación en esa materia satisface los requisitos aplicables. Puede ser práctico dividir la verificación en fases que se ejecuten en las distintas etapas significativas del diseño, pero siempre debería realizarse, cuando se haya concluido el diseño, una verificación final independiente de la evaluación de la seguridad.

5.2. La verificación independiente puede realizarse siguiendo en gran medida los métodos de evaluación de la seguridad examinados en las Secciones 2 a 4 de esta Guía de Seguridad. Sin embargo, el alcance de la verificación independiente podría ser menor que el de la evaluación de la seguridad, puesto que se centraría sólo en los temas y requisitos de seguridad más significativos, en vez de en todos ellos.

5.3. Las verificaciones independientes las llevan a cabo separadamente el propietario-entidad explotadora de la central, el cual generalmente realiza un examen independiente de la entidad responsable del diseño, y el órgano regulador.

5.4. El propietario es totalmente responsable de su verificación independiente, incluso si confía partes de la misma a otras entidades.

5.5. Las actividades de evaluación independiente del diseño son parte del programa global de GC y constituyen un tema de interés primordial en el curso del diseño de una central nuclear. No obstante, como se representa en la Fig.1, la verificación independiente se considera una comprobación adicional por separado con el fin de garantizar un diseño apropiado y seguro. El grupo encargado de la verificación independiente puede tener en cuenta, al determinar la extensión y alcance de su verificación, todo examen de GC previamente realizado.

5.6. Como se ha señalado anteriormente, esta Guía de Seguridad trata fundamentalmente de las actividades de verificación del diseño que se realizan antes de empezar la construcción de la central y se centra en las actividades llevadas a cabo por la entidad diseñadora o por quien actúe en su nombre. Sin embargo, podría aplicarse por analogía a otras actividades de verificación posteriores.

5.7. La verificación de la evaluación de la seguridad debería ser realizada por expertos familiarizados con los adelantos actuales en materia de tecnología de reactores y análisis de seguridad. Los verificadores deberían ser independientes de los diseñadores de la central.

5.8. Los encargados de la verificación independiente deberían confirmar que el proceso de evaluación de la seguridad es el adecuado. Deberían disponer de todos los documentos relevantes de diseño, incluidos los modelos de cálculo, datos y supuestos. Además, deberían tener libre acceso al emplazamiento de la central con objeto de visitar las áreas de importancia crucial y confirmar que en la evaluación de la seguridad se representa adecuadamente la instalación física real.

5.9. A continuación figura como ejemplo una lista, no exhaustiva, de los temas sujetos a examen:

- Los SIP seleccionados,
- Las normas industriales aplicadas,
- Las cuestiones relevantes de evaluación de la seguridad tecnológica y la protección radiológica,
- Las condiciones iniciales más desfavorables de la central supuestas para el suceso iniciador, con el fin de englobar todos los casos similares,
- La combinación de los distintos sucesos y sus efectos en cuanto a fallos,
- La especificación de los fallos consecutivos,
- El funcionamiento supuesto de los sistemas y componentes de seguridad y de los no clasificados como de seguridad en el transcurso de los sucesos,
- La actuación supuesta del operador,
- La selección de los códigos de computación validados aplicables al análisis en cuestión,
- Los datos de fiabilidad y su aplicabilidad al análisis en cuestión,
- La construcción de los árboles de sucesos y los árboles de fallos en el APS,
- Los fallos de causa común,
- El uso de un modelo de dispersión atmosférica para cada forma particular de emisión radiactiva,
- El análisis de incertidumbres,
- La adecuación del proceso de análisis de los sucesos que sobrepasen la base de diseño.

5.10. Debería realizarse una comprobación independiente de una selección de los cálculos hechos con ayuda de computadora, para cerciorarse de que el análisis es correcto. Si no se ha realizado una verificación y validación suficiente del código original, se debería usar otro código para verificar su exactitud.

REFERENCIAS

- [1] ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA, Seguridad de las centrales nucleares: Diseño, Colección de Normas de Seguridad No. NS-R-1, OIEA, Viena (2004).
- [2] ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA, Seguridad de las instalaciones nucleares, Colección Seguridad No. 110, OIEA, Viena (1993).
- [3] GRUPO INTERNACIONAL ASESOR EN SEGURIDAD NUCLEAR, La defensa en profundidad en seguridad nuclear, INSAG-10, OIEA, Viena (1997).
- [4] GRUPO INTERNACIONAL ASESOR EN SEGURIDAD NUCLEAR, Basic Safety Principles for Nuclear Power Plants 75-INSAG-3 Rev.1, INSAG-12, OIEA, Viena (1999).
- [5] ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA, Quality Assurance for Safety in Nuclear Power Plants and Other Nuclear Installations, Colección Seguridad No. 50-C/SG-Q, OIEA, Viena (1996).
- [6] ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA, Software for Computer Based Systems Important to Safety in Nuclear Power Plants, Colección de Normas de Seguridad No. NS-G-1.1, OIEA, Viena (2000).
- [7] ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA, Application of the Single Failure Criterion, Colección Seguridad No. 50-P-1, OIEA, Viena (1990).
- [8] ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA, Límites y condiciones operacionales y procedimientos de operación en las centrales nucleares, Colección de Normas de Seguridad No. NS-G-2.2, OIEA, Viena (en preparación).
- [9] ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA, Accident Management Programmes in Nuclear Power Plants: A Guidebook, Colección de Informes Técnicos No. 368, OIEA, Viena (1994).
- [10] ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA, Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 1), Colección Seguridad No. 50-P-4, OIEA, Viena (1992).
- [11] ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA, Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 2), Colección Seguridad No. 50-P-8, OIEA, Viena (1995).
- [12] AGENCIA PARA LA ENERGÍA NUCLEAR DE LA OCDE, Level 2 PSA Methodology and Severe Accident Management, OECD/GD(97)198, OCDE, París (1997)
- [13] COMISIÓN REGULADORA NUCLEAR DE LOS ESTADOS UNIDOS, Severe Accident Risk: An Assessment for Five US Nuclear Power Plants, Rep. NUREG-1150, Division of Systems Research, USNRC, Washington, DC (1990).
- [14] ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA, Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 3), Colección Seguridad No. 50-P-12, OIEA, Viena (1996).

- [15] ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA, The Role of Probabilistic Safety Assessment and Probabilistic Safety Criteria in Nuclear Power Plant Safety, Colección Seguridad No. 106, OIEA, Viena (1992).

COLABORADORES EN LA REDACCIÓN Y REVISIÓN

| | |
|----------------|---|
| Couch, D.P. | Laboratorio Nacional del Pacífico Noroeste (Estados Unidos de América) |
| Del Nero, G. | Agenzia Nazionale per la Protezione dell'Ambiente (Italia) |
| De Munk, P. | Ministerio de Asuntos Sociales, Departamento de Seguridad Nuclear (Países Bajos) |
| Fil, N. | OKB Hidropross (Federación de Rusia) |
| Foskolos, K. | Instituto Paul Scherrer (Suiza) |
| Gasparini, M. | Organismo Internacional de Energía Atómica |
| Misak, J. | Organismo Internacional de Energía Atómica |
| Kabanov, L. | Centro Internacional Ruso de Seguridad Nuclear de Minatom (Federación de Rusia) |
| Krishnan, V.S. | Atomic Energy of Canada Ltd. (Canadá) |
| Krugmann, U. | Siemens AG/KWU Erlangen (Alemania) |
| Lee, J.H. | Instituto de Seguridad Nuclear de Corea (República de Corea) |
| Omoto, A. | Compañía de Energía Eléctrica de Tokio (Japón) |
| Petrangeli, G. | Agenzia Nazionale per la Protezione dell'Ambiente (Italia) |
| Rohar, S. | Autoridad Reguladora Nuclear (Eslovaquia) |
| Shepherd, C.H. | Inspección de Instalaciones Nucleares (Reino Unido) |
| Simon, M. | Gesellschaft für Anlagen- und Reaktorsicherheit mbH (Alemania) |
| Vidard, M. | Electricité de France (Francia) |

Vine, G.

Instituto de Investigación de la Energía Eléctrica
(Estados Unidos de América)

Wilson, J.N.

Comisión Reguladora Nuclear
(Estados Unidos de América)

ÓRGANOS ENCARGADOS DE APROBAR LAS NORMAS DE SEGURIDAD

Comité sobre Normas de Seguridad Nuclear

Alemania: Wendling, R.D.; *Argentina:* Sajaroff, P.; *Bélgica:* Govaerts, P. (Presidente); *Brasil:* Salati de Almeida, I.P.; *Canadá:* Malek, I.; *China:* Zhao, Y.; *España:* Lequerica, I.; *Estados Unidos de América:* Murphy, J.; *Federación de Rusia:* Baklushin, R.P.; *Finlandia:* Reiman, L.; *Francia:* Saint Raymond, P.; *India:* Venkat Raj, V.; *Italia:* Del Nero, G.; *Japón:* Hirano, M.; *México:* Delgado Guardado, J.L.; *Países Bajos:* de Munk, P.; *Pakistán:* Hashimi, J.A.; *Reino Unido:* Hall, A.; *República de Corea:* Lee, J.-I.; *Suecia:* Jende, E.; *Suiza:* Aberli, W.; *Ucrania:* Mikolaichuk, O.; *Agencia para la Energía Nuclear de la OCDE:* Royen J.; *Comisión Europea:* Gómez-Gómez, J.A.; *OIEA:* Hughes, P. (Coordinador); *Organización Internacional de Normalización:* d'Ardenne, W.

Comisión sobre Normas de Seguridad

Alemania: Renneberg, W., Wendling, R.D.; *Argentina:* D'Amato, E.; *Brasil:* Caubit da Silva, A.; *Canadá:* Bishop, A., Duncan, R.M.; *China:* Zhao, C.; *España:* Martín Marquínez, A.; *Estados Unidos de América:* Travers, W.D.; *Federación de Rusia:* Vishnevskiy, Y.G.; *Francia:* Lacoste, A.-C., Gauvain, J.; *India:* Sukhatme, S.P.; *Japón:* Suda, N.; *Reino Unido:* Williams, L.G. (Presidente), Pape, R.; *República de Corea:* Kim, S.-J.; *Suecia:* Holm, L.-E.; *Suiza:* Jeschki, W.; *Ucrania:* Smyshlayaev, O.Y.; *Agencia para la Energía Nuclear de la OCDE:* Shimomura, K.; *Comisión Internacional de Protección Radiológica:* Clarke, R.H.; *OIEA:* Karbassioun, A. (Coordinador).

ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA
VIENA
ISBN 978-92-0-313509-2
ISSN 1020-5837