

La publicación SSR-2/1 (Rev. 1) sustituye a la presente publicación.

# COLECCIÓN DE NORMAS DE SEGURIDAD DEL OIEA

Seguridad de  
las centrales nucleares:  
Diseño

## REQUISITOS

Nº NS-R-1



**IAEA**

Organismo Internacional de Energía Atómica

## PUBLICACIONES DEL OIEA RELACIONADAS CON LA SEGURIDAD

### NORMAS DE SEGURIDAD DEL OIEA

Con arreglo al artículo III de su Estatuto, el OIEA está autorizado para establecer normas de seguridad para la protección contra la radiación ionizante y proveer a la aplicación de esas normas a las actividades nucleares pacíficas.

Las publicaciones de reglamentación conexas mediante las cuales el OIEA establece normas y medidas de seguridad figuran en la **Colección de Normas de Seguridad del OIEA**. Esta Colección abarca seguridad nuclear, seguridad radiológica, seguridad del transporte y seguridad de los desechos, así como seguridad en términos generales (es decir, pertinente a dos o más de las cuatro esferas). Dentro de esta Colección se incluyen las categorías de **Nociones fundamentales de seguridad**, **Requisitos de seguridad** y **Guías de seguridad**.

Las **Nociones fundamentales de seguridad** (cubierta azul) presentan los objetivos, conceptos y principios básicos de seguridad y protección en el desarrollo y la aplicación de la energía nuclear con fines pacíficos.

Los **Requisitos de seguridad** (cubierta roja) señalan los requisitos que se han de cumplir para garantizar la seguridad. Estos requisitos, en cuya formulación se emplea generalmente la forma “deberá(n)” o expresiones como “habrá que”, “hay que”, “habrá de”, “se deberá” (en inglés “shall”), se rigen por los objetivos y principios enunciados en las Nociones fundamentales de seguridad.

Las **Guías de seguridad** (cubierta verde) recomiendan acciones, condiciones o procedimientos para cumplir con los requisitos de seguridad. En la formulación de las recomendaciones de las Guías de seguridad se emplea generalmente la forma “debería(n)” o expresiones como “conviene”, “se recomienda”, “es aconsejable” (en inglés “should”), para indicar que es necesario tomar las medidas recomendadas u otras medidas equivalentes para cumplir con los requisitos.

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.

Se puede obtener información sobre el programa de Normas de seguridad del OIEA (incluidas ediciones en otros idiomas además del inglés) en el sitio del OIEA en Internet:

[www-ns.iaea.org/standards/](http://www-ns.iaea.org/standards/)

o solicitándola por escrito a la siguiente dirección: Sección de Coordinación de la Seguridad, OIEA, P.O. Box 100, A-1400 Viena (Austria).

### OTRAS PUBLICACIONES DEL OIEA RELACIONADAS CON LA SEGURIDAD

Con arreglo a las disposiciones del artículo III y del párrafo C del artículo VIII de su Estatuto, el Organismo facilita y fomenta el intercambio de información relacionada con las actividades nucleares pacíficas y sirve de intermediario para ello entre sus Estados Miembros.

Informes sobre la seguridad y protección de las actividades nucleares se publican en otras colecciones, particularmente en la **Colección de Informes de Seguridad del OIEA**, con carácter informativo. En los informes de seguridad se suelen describir buenas prácticas y ofrecer ejemplos prácticos y métodos detallados que pueden utilizarse para cumplir con los requisitos de seguridad. En dichos informes no se establecen requisitos ni se formulan recomendaciones.

Otras colecciones del OIEA que incluyen publicaciones relacionadas con la seguridad son la **Colección de Informes Técnicos**, la **Colección de Informes de Evaluaciones Radiológicas**, la **Colección INSAG**, la **Colección TECDOC**, la **Colección de Normas de Seguridad Provisionales**, la **Colección de Cursos de Capacitación**, la **Colección de Servicios del OIEA** y la **Colección de Manuales de Informática**, así como las que aparecen bajo los títulos de **Practical Radiation Safety Manuals** y **Practical Radiation Technical Manuals**. El OIEA también edita informes sobre accidentes radiológicos y otras publicaciones especiales.

La publicación SSR-2/1 (Rev. 1) sustituye a la presente publicación.

SEGURIDAD DE  
LAS CENTRALES NUCLEARES:  
DISEÑO

## La publicación SSR-2/1 (Rev. 1) sustituye a la presente publicación.

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

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

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”.

© OIEA, 2004

Para copiar o traducir el material informativo de la presente publicación se deberá solicitar por escrito el correspondiente permiso al Organismo Internacional de Energía Atómica, Wagramer Strasse 5, Apartado de Correos 100, A-1400 Viena, Austria.

Impreso por el OIEA en Austria  
Julio de 2004  
STI/PUB/1099

La publicación SSR-2/1 (Rev. 1) sustituye a la presente publicación.

COLECCIÓN DE NORMAS DE SEGURIDAD N° NS-R-1

SEGURIDAD DE  
LAS CENTRALES NUCLEARES:  
DISEÑO

REQUISITOS DE SEGURIDAD

ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA  
VIENA, 2004

La publicación SSR-2/1 (Rev. 1) sustituye a la presente publicación.

ESTA GUÍA DE LA COLLECCIÓN DE NORMAS DE SEGURIDAD  
SE PUBLICA TAMBIÉN EN FRANCÉS, INGLÉS Y RUSO

SEGURIDAD DE LAS CENTRALES NUCLEARES: DISEÑO  
OIEA, VIENA, 2004  
STI/PUB/1099  
ISBN 92-0-307004-4  
ISSN 1020-525X

## PRÓLOGO

**por 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 asesores supervisan la elaboración de las normas de seguridad: la Comisión Asesora sobre Normas de Seguridad (ACSS); el Comité Asesor sobre normas de seguridad nuclear (NUSSAC); el Comité Asesor sobre normas de seguridad radiológica (RASSAC); el Comité Asesor sobre normas de seguridad en el transporte (TRANSSAC); y el Comité Asesor sobre normas de seguridad de los desechos (WASSAC). 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. 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, tendrá que cumplir 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 incumben 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 hayan de ser dictaminados por expertos atendiendo a las circunstancias particulares de cada caso.

## La publicación SSR-2/1 (Rev. 1) sustituye a la presente publicación.

Se menciona cuando procede, pero sin tratarla en detalle, la protección física de los materiales fisionables 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 cualesquiera 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 sistemas 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

*Cuando se incluye un apéndice debe considerarse que forma parte integrante del documento y tiene igual validez que el texto principal. En cambio, los anexos, las notas de pie de página y las bibliografías se incluyen para proporcionar información adicional o para dar ejemplos prácticos que podrían ser de utilidad para el usuario.*

*En las Normas de seguridad se emplea el término “deberá(n)” (en inglés “shall”) cuando se enuncian requisitos, deberes y obligaciones. Se utiliza la forma “debería(n)” o “debe(n)” (en inglés “should”) para indicar recomendaciones de una opción deseable.*

*La versión inglesa es la versión autorizada del texto. El presente documento fue traducido por el Consejo de Seguridad Nuclear de España. El Organismo reconoce con agradecimiento el apoyo prestado.*



## ÍNDICE

1.	INTRODUCCIÓN .....	1
	Antecedentes (1.1) .....	1
	Objetivo (1.2–1.4) .....	1
	Alcance (1.5–1.7) .....	2
	Estructura (1.8) .....	3
2.	CONCEPTOS Y OBJETIVOS DE SEGURIDAD .....	3
	Objetivos de seguridad (2.1–2.8) .....	3
	Concepto de defensa en profundidad (2.9–2.11) .....	5
3.	REQUISITOS PARA LA GESTIÓN DE LA SEGURIDAD .....	7
	Responsabilidades en materia de gestión (3.1) .....	7
	Gestión del diseño (3.2–3.5) .....	8
	Actividades de ingeniería probadas (3.6–3.8) .....	9
	Experiencia operacional e investigación de la seguridad (3.9) .....	9
	Evaluación de la seguridad (3.10–3.12) .....	9
	Verificación independiente de la evaluación de la seguridad (3.13) .....	10
	Garantía de calidad (3.14–3.16) .....	10
4.	REQUISITOS TÉCNICOS PRINCIPALES .....	11
	Requisitos para la defensa en profundidad (4.1–4.4) .....	11
	Funciones de seguridad (4.5–4.7) .....	12
	Prevención de accidentes y características de seguridad de las centrales (4.8) .....	12
	Protección radiológica y criterios de aceptación (4.9–4.13) .....	13
5.	REQUISITOS PARA EL DISEÑO DE LAS CENTRALES .....	14
	Clasificación en función de la seguridad (5.1–5.3) .....	14
	Base general de diseño (5.4–5.31) .....	14
	Diseño para lograr la fiabilidad de las estructuras, sistemas y componentes (5.32–5.42) .....	21
	Disposiciones para los ensayos, el mantenimiento, la reparación, la inspección y la vigilancia en servicio (5.43–5.44) .....	23

**La publicación SSR-2/1 (Rev. 1) sustituye a la presente publicación.**

Cualificación del equipo (5.45–5.46) .....	24
Envejecimiento (5.47) .....	24
Factores humanos (5.48–5.56) .....	25
Otras consideraciones de diseño (5.57–5.68) .....	26
Análisis de seguridad (5.69–5.73) .....	29
6. REQUISITOS PARA EL DISEÑO DE SISTEMAS DE CENTRALES .	30
Núcleo del reactor y sistemas conexos (6.1–6.20) .....	30
Sistema de refrigeración del reactor (6.21–6.42) .....	34
Sistema de contención (6.43–6.67) .....	38
Instrumentación y control (6.68–6.86) .....	42
Centro de control de emergencias (6.87) .....	47
Sistema eléctrico de emergencia (6.88–6.89) .....	47
Sistemas de control y tratamiento de desechos radiactivos (6.90–6.95) .....	47
Sistemas de manipulación y almacenamiento del combustible (6.96–6.98) .....	49
Protección radiológica (6.99–6.106) .....	50
APÉNDICE I: SUCESOS INICIADORES POSTULADOS .....	53
APÉNDICE II: REDUNDANCIA, DIVERSIDAD E INDEPENDENCIA ...	57
REFERENCIAS .....	61
ANEXO: FUNCIONES DE SEGURIDAD PARA REACTORES DE AGUA EN EBULLICIÓN, REACTORES DE AGUA A PRESIÓN Y REACTORES DE TUBOS DE PRESIÓN .....	62
GLOSARIO .....	65
COLABORADORES EN LA REDACCIÓN Y EXAMEN .....	69
ÓRGANOS ASESORES PARA LA APROBACIÓN DE LAS NORMAS DE SEGURIDAD .....	71

## 1. INTRODUCCIÓN

### ANTECEDENTES

1.1. La presente publicación sustituye al Código sobre la seguridad de las centrales nucleares: Diseño (Colección Seguridad N° 50-C-D (Rev. 1), publicado en 1988). En ella se tienen en cuenta los adelantos relacionados con la seguridad de las centrales nucleares desde que se llevó a cabo la última revisión del Código de diseño. Esos adelantos incluyen la publicación de las Nociones fundamentales de seguridad: Seguridad de las instalaciones nucleares [1], así como la actual revisión de diversas normas de seguridad y otras publicaciones relacionadas con la seguridad. El objetivo de los requisitos para la seguridad nuclear es garantizar la protección adecuada del personal del emplazamiento, del público en general y del medio ambiente, contra los efectos de la radiación ionizante procedente de las centrales nucleares. Se reconoce que tanto los avances de la tecnología y del conocimiento científico como la seguridad nuclear y lo que se considera como protección adecuada, no son conceptos estáticos. Los requisitos de seguridad varían con esos avances y la presente publicación refleja el consenso actual.

### OBJETIVO

1.2. La presente publicación de Requisitos de seguridad tiene en cuenta los avances en los requisitos de seguridad, incluido, por ejemplo, el estudio de accidentes graves en el proceso de diseño. Entre otros temas a los que se ha prestado una atención más detallada cabe citar la gestión de la seguridad, la gestión del diseño, los efectos derivados del envejecimiento y el deterioro de la central, los sistemas informáticos de seguridad, los riesgos externos e internos, los factores humanos, la retroinformación sobre experiencia operacional, y la verificación y evaluación de la seguridad.

1.3. En la presente publicación se establecen requisitos de seguridad que definen los elementos necesarios para garantizar la seguridad nuclear. Dichos requisitos son aplicables a las funciones de seguridad y a las estructuras, sistemas y componentes conexos, así como a los procedimientos de importancia para la seguridad de las centrales nucleares. Se espera que esta publicación se utilice principalmente para centrales nucleares fijas emplazadas en tierra, con reactores refrigerados por agua, diseñadas para la generación de electricidad o para otras aplicaciones de la producción de calor (como calefacción urbana o desalinización). Se reconoce que en el caso de otros tipos de reactores que incorporen avances innovadores en futuros sistemas,

## La publicación SSR-2/1 (Rev. 1) sustituye a la presente publicación.

algunos de los requisitos pueden o bien no ser aplicables, o bien requerir la aplicación de ciertos criterios en su interpretación. Diversas Guías de seguridad facilitarán orientación para la interpretación y aplicación de dichos requisitos.

1.4. Esta publicación está concebida para su uso por organizaciones que diseñen, fabriquen, construyan y exploten centrales nucleares, así como por órganos reguladores.

### ALCANCE

1.5. En la presente publicación se establecen los requisitos de diseño de las estructuras, sistemas y componentes de importancia para la seguridad, a fin de lograr un funcionamiento seguro de una central nuclear y para impedir o atenuar las consecuencias de sucesos que pudieran poner en peligro la seguridad. También se establecen requisitos para una evaluación exhaustiva de la seguridad, que se lleva a cabo con objeto de determinar los posibles riesgos derivados del funcionamiento de la central en sus diversos estados (estados operacionales y condiciones de accidente). El proceso de evaluación de la seguridad incluye las técnicas complementarias de análisis determinista de la seguridad y análisis probabilista de la seguridad. Dichos análisis requieren un estudio de los sucesos iniciadores postulados (SIP), que incluye muchos factores que, aislados o en combinación, pueden afectar a la seguridad, y que asimismo pueden:

- tener origen en las operaciones de explotación de la central nuclear;
- ser resultado de actividades humanas;
- guardar relación directa con la central nuclear y con su entorno.

1.6. En esta publicación se tienen en cuenta también sucesos que son sumamente improbables, como los accidentes graves que pueden producir importantes emisiones radiactivas, y para los cuales sería adecuado y factible que se incorporaran en el diseño medidas preventivas o de atenuación.

1.7. En esta publicación no se tienen en cuenta:

- sucesos externos naturales o imputables al hombre que son extremadamente improbables (como el impacto de un meteorito o de un satélite artificial);
- accidentes industriales convencionales que en ningún caso podrían afectar a la seguridad de la central nuclear; o
- efectos no radiológicos derivados de la explotación de centrales nucleares, lo que puede depender de reglamentaciones nacionales independientes.

## ESTRUCTURA

1.8. Esta publicación de Requisitos de seguridad se basa en la relación entre los principios y objetivos de seguridad, y en requisitos y criterios de seguridad. La Sección 2 trata en detalle los principios, objetivos y conceptos de seguridad que constituyen la base para establecer los requisitos de seguridad que deben cumplirse en el diseño de la central. Los objetivos de seguridad (que figuran en cursiva en la Sección 2) están tomados de la publicación Seguridad de las instalaciones nucleares, de la colección Nociones fundamentales de seguridad [1]. La Sección 3 contiene los requisitos principales que debe aplicar la organización encargada del diseño en la gestión del proceso de diseño, así como otros requisitos para la evaluación de seguridad, para la garantía de calidad y para el uso de prácticas de ingeniería probadas y experiencia operacional. La Sección 4 incluye los requisitos técnicos principales y más generales para la defensa en profundidad y la protección radiológica. La Sección 5 se ocupa de los requisitos para el diseño general de la central, que complementan los requisitos principales con el fin de garantizar que se cumplen los objetivos de seguridad. La Sección 6 contiene requisitos de diseño aplicables a los sistemas específicos de la central, tales como el núcleo del reactor, los sistemas de refrigeración y los sistemas de contención. En el Apéndice I se estudia en detalle la definición y aplicación del concepto de suceso iniciador postulado. En el Apéndice II se examina la aplicación de la redundancia, la diversidad y la independencia como medidas para aumentar la fiabilidad y para brindar protección contra los fallos debidos a causas comunes. En el Anexo se estudian a fondo las funciones de seguridad para los reactores.

## 2. CONCEPTOS Y OBJETIVOS DE SEGURIDAD

### OBJETIVOS DE SEGURIDAD

2.1. La publicación Nociones fundamentales de seguridad: Seguridad de las instalaciones nucleares [1] establece tres objetivos fundamentales de seguridad, de los cuales pueden deducirse los requisitos para reducir al mínimo los riesgos asociados con las centrales nucleares. Los párrs. 2.2. a 2.6., que figuran a continuación, están copiados directamente de los párrs. 203 a 207 de la publicación Seguridad de las instalaciones nucleares.

2.2. **“Objetivo general de seguridad nuclear:** *Proteger de efectos dañinos a las personas, a la sociedad y al medio ambiente creando y manteniendo en las instalaciones nucleares defensas eficaces contra los riesgos radiológicos.*

2.3. A este objetivo general de seguridad nuclear contribuyen dos objetivos de seguridad complementarios que tratan de la protección radiológica y de los aspectos técnicos. Su dependencia es biunívoca: los aspectos técnicos junto con medidas administrativas y de procedimiento garantizan la defensa contra los riesgos debidos a las radiaciones ionizantes.

2.4. **Objetivo de protección radiológica:** *Garantizar que, en todas las situaciones operacionales, la exposición a la radiación dentro de la instalación o debida a cualquier liberación planificada de sustancias radiactivas de la misma, se mantenga por debajo de los límites prescritos y reducida al valor más bajo que pueda razonablemente alcanzarse, así como garantizar la atenuación de las consecuencias radiológicas de cualesquiera accidentes.*

2.5. **Objetivo de seguridad técnica:** *Adoptar todas las medidas razonablemente posibles para evitar accidentes en instalaciones nucleares y atenuar sus consecuencias, en caso de que se produzcan; garantizar con un elevado grado de confianza que, para todos los accidentes posibles considerados en el diseño de la instalación, incluso los de muy baja probabilidad, cualquier consecuencia radiológica sea poco importante y por debajo de los límites prescritos; y garantizar que la probabilidad de accidentes con serias consecuencias radiológicas sea sumamente pequeña.*

2.6. Los objetivos de seguridad requieren que las instalaciones nucleares se diseñen y exploten de manera que se mantengan todas las fuentes de exposición a las radiaciones bajo un control técnico y administrativo estricto. Ahora bien, el objetivo de protección radiológica no excluye una exposición limitada de las personas ni la liberación de cantidades legalmente autorizadas de sustancias radiactivas al medio ambiente en situaciones operacionales. Dichas liberaciones y exposiciones, no obstante, deben mantenerse estrictamente controladas y cumplir los límites operacionales y las normas de protección radiológica.”

2.7. Para lograr esos tres objetivos de seguridad, en el diseño de una central nuclear se lleva a cabo un análisis de seguridad exhaustivo que identifique todas las fuentes de exposición y evalúe las dosis de radiación que podrían recibir los trabajadores de la instalación y el público en general, así como los posibles efectos sobre el medio ambiente (véase el párr. 4.9). El análisis de seguridad examina: 1) todas las modalidades operacionales normales previstas de la central; 2) el comportamiento de la central en caso de incidentes operacionales previstos; 3) los accidentes base de diseño; y 4) las secuencias de sucesos que puede originar un accidente grave. Sobre la base de ese análisis puede establecerse la solidez del diseño técnico para hacer frente a los accidentes y a los sucesos iniciadores postulados, puede demostrarse la eficacia de los sistemas de seguridad y la de los sistemas y componentes

relacionados con la seguridad, y pueden establecerse medidas de respuesta en casos de emergencia.

2.8. Aunque se adopten medidas para controlar la exposición a la radiación, en todas las situaciones operacionales, a los niveles más bajos que puedan razonablemente alcanzarse (principio ALARA), y para reducir al mínimo la probabilidad de un accidente que pueda conducir a la pérdida del control normal de la fuente de radiación, existe una probabilidad residual de que ocurra un accidente. En consecuencia, han de adoptarse medidas para garantizar que se atenúan las consecuencias radiológicas. Dichas medidas incluyen: elementos técnicos de seguridad; procedimientos para la gestión de accidentes en el emplazamiento, establecidos por la entidad explotadora; y posibles medidas de intervención fuera del emplazamiento, establecidas por las autoridades pertinentes con objeto de atenuar la exposición a la radiación en caso de accidente. En el diseño para la seguridad de una central nuclear se aplica el principio de que los estados de la central que podrían originar grandes dosis de radiación o liberaciones de radiación, tendrían probabilidades bajísimas, y de que los estados de probabilidad relativamente elevada no tendrían consecuencias radiológicas, o éstas serían leves. Un objetivo esencial es que la necesidad de aplicar medidas de intervención externa pueda limitarse o incluso eliminarse desde el punto de vista técnico, aunque las autoridades nacionales consideren necesario aplicar tales medidas.

## CONCEPTO DE DEFENSA EN PROFUNDIDAD

2.9. El concepto de defensa en profundidad, tal como se aplica a todas las actividades de seguridad, ya se relacionen con la organización, el comportamiento o el diseño, garantiza que dichas actividades estén sujetas a disposiciones parcialmente superpuestas, de modo que si hubiese un fallo, sería detectado, compensado o corregido mediante la aplicación de las medidas adecuadas. El concepto ha sido estudiado con más detalle desde 1988 [2, 3]. La aplicación del concepto de defensa en profundidad mediante las actividades de diseño y explotación proporciona una protección gradual contra una amplia variedad de fenómenos transitorios, accidentes e incidentes operacionales previstos, incluidos los producidos por fallos del equipo o por actuaciones humanas dentro de la central, y por los sucesos que puedan ocurrir fuera de ella.

2.10. La aplicación del concepto de defensa en profundidad en el diseño de una central incluye una serie de niveles de defensa (elementos inherentes, equipo, y procedimientos) con el fin de evitar accidentes y asegurar la adecuada protección en caso de que falle dicha prevención.

## La publicación SSR-2/1 (Rev. 1) sustituye a la presente publicación.

- 1) La finalidad del primer nivel de defensa es impedir las desviaciones del funcionamiento normal y evitar fallos en el sistema. Esto exige que la central sea diseñada, construida, mantenida y explotada correcta y rigurosamente, con arreglo a niveles de calidad y prácticas de ingeniería adecuados, tales como la aplicación de criterios de redundancia, independencia y diversidad. Para lograr ese objetivo se presta gran atención a la selección de los materiales y códigos de diseño adecuados, y al control de la fabricación de componentes y de la construcción de la central. Las opciones de diseño que pueden contribuir a reducir la probabilidad de riesgos internos (por ejemplo, controlar la respuesta a un suceso iniciador postulado (SIP)), reducir las consecuencias de un SIP determinado, o reducir la posible liberación del término de fuente tras un accidente, contribuyen a este nivel de defensa. También se presta atención a los procedimientos relacionados con el diseño, fabricación, construcción e inspección de la central en servicio, a las actividades de mantenimiento y ensayo, a la facilidad de acceso para realizar dichas actividades, así como a la forma en que se explota la central y se aprovecha la experiencia de explotación. Este proceso completo está apoyado por un análisis detallado que determina los requisitos operacionales y de mantenimiento de la central.
- 2) La finalidad del segundo nivel de defensa es detectar e interrumpir las desviaciones respecto de las condiciones de funcionamiento normal para evitar que los incidentes operacionales previstos se agraven hasta convertirse en condiciones de accidente. Esto supone el reconocimiento de que ocurrirán SIP durante la vida útil de la central, pese a las precauciones adoptadas para evitarlos. Este escalón requiere la presencia de sistemas específicos determinados en el análisis de seguridad, y la definición de procedimientos de explotación para evitar o minimizar el daño resultante de dichos SIP.
- 3) Para el tercer nivel de defensa se supone que, aunque sea muy improbable, es posible que ciertos incidentes operacionales previstos no queden interrumpidos por un nivel precedente y pueda producirse un suceso más grave. Estos sucesos improbables se anticipan en la base de diseño de la central, y se facilitan elementos inherentes de seguridad, criterios de “fallo sin riesgo” en el diseño, equipo adicional y procedimientos para controlar sus consecuencias y lograr estados de la central estables y aceptables tras esos sucesos. Esto crea al requisito de que se proporcionen los elementos técnicos de seguridad necesarios para llevar a la central, en primer lugar a un estado controlado, y posteriormente a un estado de parada de seguridad, manteniendo al menos una barrera de confinamiento del material radiactivo.
- 4) La finalidad del cuarto nivel de defensa es abordar casos de accidentes graves en los que pueda superarse la base de diseño, y garantizar que la liberación de material radiactivo se mantenga al nivel más bajo posible. El objetivo más importante de este nivel es la protección de la función de confinamiento. Esto



puede lograrse aplicando medidas y procedimientos complementarios para evitar la progresión del accidente, atenuando las consecuencias de determinados accidentes graves, y aplicando además procedimientos de gestión de accidentes. La protección proporcionada por el confinamiento puede demostrarse utilizando los mejores métodos de estimación.

- 5) El quinto y último nivel de defensa tiene como objetivo atenuar las consecuencias radiológicas de las posibles liberaciones de materiales radiactivos que puedan producirse en condiciones de accidente. Esto requiere disponer de un centro de control de emergencias adecuadamente equipado, y elaborar planes de respuesta a emergencias tanto en el emplazamiento como fuera de él.

2.11. Un aspecto importante de la aplicación de la defensa en profundidad es la introducción en el diseño de una serie de barreras físicas que confinen el material radiactivo a lugares especificados. El número de barreras físicas necesarias dependerá de los posibles riesgos internos y externos, y de las posibles consecuencias de los fallos. En el caso de los reactores refrigerados por agua, las barreras pueden incluir el propio combustible, las vainas del combustible, la barrera del sistema de refrigeración del reactor y la contención.

### **3. REQUISITOS PARA LA GESTIÓN DE LA SEGURIDAD**

#### **RESPONSABILIDADES EN MATERIA DE GESTIÓN**

3.1. Recae en la entidad explotadora la responsabilidad general de la seguridad. Sin embargo, todas las organizaciones que participan en actividades de importancia para la seguridad tienen la responsabilidad de garantizar que se otorga la más alta prioridad a las cuestiones relacionadas con la seguridad. La organización encargada del diseño deberá asegurarse de que la instalación esté diseñada para cumplir los requisitos de la entidad explotadora, incluidos los requisitos normalizados de la compañía eléctrica; que tenga en cuenta las técnicas más avanzadas en cuestión de seguridad; que cumpla las especificaciones de diseño y del análisis de seguridad; que satisfaga los requisitos de las reglamentaciones nacionales; que cumpla los requisitos de un programa eficaz de garantía de calidad y que se estudie adecuadamente cualquier modificación del diseño. Así pues, la organización encargada del diseño deberá:

- 1) disponer de una clara asignación de responsabilidades con estructuras de autoridad y comunicación correspondientes;

- 2) garantizar que disponga de personal suficiente, técnicamente cualificado y adecuadamente capacitado a todos los niveles;
- 3) establecer relaciones claras entre los grupos que participan en las diferentes etapas del diseño, y entre los diseñadores, instaladores, suministradores, constructores y contratistas, según proceda;
- 4) elaborar procedimientos bien concebidos y exigir su estricto cumplimiento;
- 5) examinar, controlar y auditar de modo periódico todas las cuestiones de diseño relacionadas con la seguridad; y
- 6) garantizar que se mantiene una cultura de seguridad.

## GESTIÓN DEL DISEÑO

3.2. En la gestión del diseño para una central nuclear se deberá garantizar que las estructuras, sistemas y componentes de importancia para la seguridad tengan las características, especificaciones y composición material adecuadas, para que puedan llevarse a cabo las funciones de seguridad y para que la central pueda funcionar con la seguridad y la fiabilidad necesarias durante toda su vida útil, teniendo como principales objetivos la prevención de accidentes, la protección del personal del emplazamiento, del público en general y del medio ambiente.

3.3. La gestión del diseño deberá asegurar que se cumplan los requisitos establecidos por la entidad explotadora, y que se tengan adecuadamente en cuenta las capacidades y limitaciones humanas del personal. La organización encargada del diseño deberá facilitar información adecuada sobre el diseño de seguridad para garantizar la explotación y el mantenimiento seguros de la central, de forma que puedan llevarse a cabo posteriormente modificaciones y actividades recomendadas para su incorporación en los procedimientos administrativos y operacionales de la central (por ejemplo, límites y condiciones operacionales).

3.4. En la gestión del diseño se deberá tener en cuenta los resultados de los análisis de seguridad complementarios, deterministas y probabilistas, de modo que haya un proceso interactivo que garantice que se preste la atención debida a la prevención de accidentes y a la atenuación de sus consecuencias.

3.5. En la gestión del diseño se deberá asegurar que la generación de desechos radiactivos se mantenga al nivel más bajo posible, en términos tanto de actividad como de volumen, mediante la adopción de medidas de diseño y de prácticas operacionales y de clausura adecuadas.

## ACTIVIDADES DE INGENIERÍA PROBADAS

3.6. Siempre que sea posible, las estructuras, sistemas y componentes de importancia para la seguridad deberán diseñarse de conformidad con las normas más recientes o actualmente en vigor; deberán tener un diseño probado en aplicaciones anteriores análogas y seleccionarse de modo que estén en consonancia con los objetivos de viabilidad de la central necesarios para la seguridad. Cuando se utilicen códigos y normas como reglas de diseño, deberán examinarse y evaluarse para determinar su aplicabilidad, idoneidad y suficiencia, y deberán complementarse o modificarse según sea necesario para garantizar que la calidad final corresponda a la función de seguridad que han de desempeñar.

3.7. Cuando se introduzca un diseño o característica no probada o cuando haya una desviación de una actividad de ingeniería establecida, deberá demostrarse que la seguridad es la adecuada recurriendo a programas auxiliares de investigación apropiados o al examen de la experiencia operacional resultante de otras aplicaciones pertinentes. El dispositivo deberá someterse también a los ensayos adecuados antes de ponerlo en servicio, y deberá someterse a vigilancia mientras esté en servicio, para verificar que se logra el comportamiento previsto.

3.8. En la selección del equipo se deberá tener en cuenta tanto su funcionamiento espúreo como los modos de fallo inseguros (por ejemplo, la ausencia de disparo cuando éste sea necesario). Cuando sea de esperar y haya que tener en cuenta en el diseño el fallo de una estructura, sistema o componente, se otorgará preferencia al equipo que presente un modo pronosticable de fallo y que facilite su reparación o sustitución.

## EXPERIENCIA OPERACIONAL E INVESTIGACIÓN DE LA SEGURIDAD

3.9. En el diseño se deberá tener en cuenta la experiencia operacional pertinente adquirida en centrales en funcionamiento y los resultados de los programas de investigación pertinentes.

## EVALUACIÓN DE LA SEGURIDAD

3.10. Deberá llevarse a cabo una evaluación exhaustiva de la seguridad para confirmar que el diseño, tal como ha sido entregado para la fabricación, para la construcción, y una vez construido, cumple los requisitos de seguridad establecidos al iniciar el proceso de diseño.

3.11. La evaluación de la seguridad deberá formar parte del proceso de diseño, con una iteración entre el diseño y las actividades analíticas confirmatorias, e incrementar su alcance y su grado de detalle a medida que avanza el programa de diseño.

3.12. La evaluación de la seguridad se basará en los datos extraídos del análisis de la seguridad, en la experiencia operacional previa, en los resultados de la investigación de apoyo y en prácticas de ingeniería probadas.

#### VERIFICACIÓN INDEPENDIENTE DE LA EVALUACIÓN DE LA SEGURIDAD

3.13. 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.

#### GARANTÍA DE CALIDAD<sup>1</sup>

3.14. Deberá elaborarse y aplicarse un programa de garantía de calidad que incluya los arreglos generales para la gestión, el comportamiento y la evaluación del diseño de la central. Dicho programa deberá completarse con planos más detallados para cada estructura, sistema y componente, a fin de asegurar en todo momento la calidad del diseño.

3.15. El diseño, incluidos los cambios posteriores o las mejoras de seguridad, se llevará a cabo de conformidad con procedimientos establecidos que requieran códigos y normas de ingeniería adecuados, y deberá incorporar requisitos aplicables y bases de diseño. Se determinarán y controlarán las interfaces de diseño.

3.16. La idoneidad del diseño, incluidos los instrumentos de diseño y los insumos y productos del diseño, deberá ser verificada o validada por personas o grupos distintos de aquellos que originalmente llevaron a cabo el trabajo. La verificación, validación y aprobación deberán completarse antes de que se realice el diseño detallado.

---

<sup>1</sup> Véanse otras orientaciones en la Ref. [4].

## 4. REQUISITOS TÉCNICOS PRINCIPALES

### REQUISITOS PARA LA DEFENSA EN PROFUNDIDAD

4.1. En el proceso de diseño deberá incluirse el criterio de defensa en profundidad, tal como ha sido descrita en la Sección 2. En consecuencia, en el diseño se deberá:

- 1) proporcionar múltiples barreras físicas para impedir la liberación incontrolada de materiales radiactivos en el medio ambiente;
- 2) adoptar un enfoque prudente, y la construcción deberá ser de gran calidad, para que se reduzcan al mínimo los fallos y desviaciones de la central respecto de su funcionamiento normal, y se eviten los accidentes;
- 3) proporcionar medios para controlar el comportamiento de la central durante un SIP y después del mismo, utilizando elementos de ingeniería inherentes; por ejemplo, en el diseño deberán reducirse al mínimo o excluirse los transitorios incontrolados, en la medida de lo posible;
- 4) introducir medios para el control complementario de la central, mediante el uso de dispositivos automáticos para activar los sistemas de seguridad, con el fin de reducir al mínimo las acciones del operador en la fase temprana de un SIP, y mediante las propias acciones del operador;
- 5) prever equipo y procedimientos para controlar la progresión de un accidente y limitar sus consecuencias, en la medida en que sea posible; y
- 6) contar con medios múltiples para que se lleven a cabo cada una de las funciones fundamentales de seguridad, por ejemplo, el control de la reactividad, la eliminación del calor y el confinamiento de materiales radiactivos, garantizando así la eficacia de las barreras y atenuando las consecuencias de los SIP.

4.2. Para conseguir que se mantenga el concepto general de seguridad de la defensa en profundidad, el diseño deberá realizarse de modo que se evite en lo posible:

- 1) acciones que pongan en peligro la integridad de las barreras físicas;
- 2) el fallo de una barrera como resultado de acciones que la hayan puesto en peligro;
- 3) el fallo de una barrera como consecuencia del fallo de otra barrera.

4.3. El diseño deberá realizarse de modo que el primer nivel de defensa, o como máximo el segundo, puedan evitar la progresión de las condiciones de accidente para todos los SIP, excepto los más improbables.

4.4. En el diseño se deberá tener en cuenta que la existencia de niveles múltiples de defensa no es una base suficiente para que continúe el funcionamiento en régimen de

potencia cuando falla un nivel de defensa. Todos los niveles de defensa deberán estar disponibles en todo momento, aunque pueden hacerse algunas excepciones para otras modalidades operacionales distintas del funcionamiento en régimen de potencia.

#### FUNCIONES DE SEGURIDAD

4.5. El objetivo del enfoque de seguridad será: proporcionar los medios adecuados para mantener la central en una situación de explotación normal; asegurar la respuesta adecuada a corto plazo inmediatamente después de un SIP; facilitar la gestión de la central en caso de accidente base de diseño y después de él, así como en las condiciones de accidente seleccionadas que superen las de los accidentes base de diseño.

4.6. Para garantizar la seguridad deberán llevarse a cabo las siguientes funciones fundamentales de seguridad en situaciones operacionales, en caso de accidente base de diseño y después de él y, en la medida de lo posible, cuando surjan condiciones de accidente seleccionadas que superen las de los accidentes base de diseño:

- 1) control de la reactividad;
- 2) eliminación del calor del núcleo del reactor; y
- 3) confinamiento de los materiales radiactivos y control de las descargas operacionales, así como limitación de las liberaciones accidentales.

En el Anexo figura un ejemplo de una subdivisión detallada de esas tres funciones fundamentales de seguridad.

4.7. Deberá aplicarse un enfoque sistemático para identificar las estructuras, sistemas y componentes que son necesarios para cumplir las funciones de seguridad en los diversos momentos, después de un SIP.

#### PREVENCIÓN DE ACCIDENTES Y CARACTERÍSTICAS DE SEGURIDAD DE LAS CENTRALES

4.8. La central deberá diseñarse de modo que se reduzca a un mínimo la sensibilidad frente a los SIP. La respuesta prevista de la central ante cualquier SIP será una de las opciones indicadas en los apartados siguientes, dentro de lo razonablemente alcanzable (por orden de importancia):

- 1) un SIP no produce efectos de importancia relacionados con la seguridad, o produce solamente una evolución de la central hacia una situación de seguridad por sus características intrínsecas; o

- 2) tras un SIP, la central vuelve a una situación de seguridad mediante la actuación de elementos de seguridad pasivos, o mediante la actuación de sistemas de seguridad que funcionan continuamente en las condiciones necesarias para controlar el SIP; o
- 3) tras un SIP, la central vuelve a una situación de seguridad mediante la actuación de sistemas de seguridad que deben ponerse en servicio en respuesta al SIP; o
- 4) tras un SIP, la central vuelve a una situación de seguridad por medio de acciones de procedimiento concretas.

## PROTECCIÓN RADIOLÓGICA Y CRITERIOS DE ACEPTACIÓN

4.9. Con el fin de lograr los tres objetivos de seguridad enunciados en los párrs. 2.2 a 2.5, en el diseño de una instalación nuclear deberán identificarse y examinarse adecuadamente todas las fuentes de radiación reales y potenciales, y se adoptarán medidas para asegurar que las fuentes se mantengan bajo estricto control técnico y administrativo.

4.10. Asimismo se adoptarán medidas para conseguir que se logren los objetivos de protección radiológica y seguridad técnica enunciados en los párrs. 2.4 y 2.5, y que las dosis de radiación que reciba el personal del emplazamiento y el público en general, en todas las situaciones operacionales, incluidas las actividades de mantenimiento y clausura, no superen los límites prescritos y sean tan bajas como sea razonablemente posible.

4.11. El objetivo del diseño será la prevención o, en el caso de que ésta falle, la atenuación de las exposiciones a la radiación resultante de accidentes base de diseño y de otros accidentes graves. Se adoptarán disposiciones para que las dosis potenciales de radiación al público en general y al personal del emplazamiento no superen los límites aceptables y sean tan bajas como sea razonablemente posible.

4.12. Los estados de la central que pudieran originar dosis de radiación o liberaciones de material radiactivo elevadas, deberán tener una probabilidad muy baja, y se velará por que las posibles consecuencias radiológicas de los estados de la central que impliquen una probabilidad elevada sean muy reducidas. Los criterios de aceptación radiológica para el diseño de una central nuclear se especificarán sobre la base de esos requisitos.

4.13. Normalmente hay un número limitado de conjuntos de criterios de aceptación radiológica, y es práctica común asociarlos con las categorías de estados de las centrales. Entre esas categorías se incluyen generalmente las de funcionamiento

normal, incidentes operacionales previstos, accidentes base de diseño y accidentes graves. Los criterios de aceptación radiológica para esas categorías deberán cumplir, como nivel mínimo de seguridad, los requisitos del órgano regulador.

## 5. REQUISITOS PARA EL DISEÑO DE LAS CENTRALES

### CLASIFICACIÓN EN FUNCIÓN DE LA SEGURIDAD

5.1. Todas las estructuras, sistemas y componentes, incluidos los programas informáticos de instrumentación y control (I+C) que sean elementos de importancia para la seguridad, deberán en primer lugar determinarse y después clasificarse sobre la base de su función e importancia para la seguridad, y se diseñarán, construirán y mantendrán de modo que su calidad y fiabilidad estén en consonancia con su clasificación.

5.2. El método para determinar la importancia para la seguridad de una estructura, un sistema o un componente, se basará principalmente en métodos deterministas, complementados, cuando proceda, por métodos probabilistas y criterios de ingeniería, teniendo en cuenta factores tales como:

- 1) la función o funciones para la seguridad que debe desempeñar el elemento de que se trate;
- 2) las consecuencias del incumplimiento de su función;
- 3) la probabilidad de que dicho elemento deba llevar a cabo una función de seguridad;
- 4) el tiempo después de un SIP o el período durante el cual deberá funcionar.

5.3. Se introducirán interfaces de diseño adecuado entre las estructuras, sistemas y componentes de diferentes clases, para lograr que cualquier fallo en un sistema que pertenece a una clase más baja no se propague a un sistema de una clase más alta.

### BASE GENERAL DE DISEÑO

5.4. En la base de diseño se deberá especificar los medios necesarios de la central para hacer frente a una determinada gama de situaciones operacionales y accidentes base de diseño, con sujeción a los requisitos definidos en materia de protección radiológica. En la base de diseño se deberá incluir las especificaciones para el



funcionamiento normal, los estados de la central creados por los SIP, la clasificación de la seguridad, las hipótesis importantes y, en algunos casos, los métodos de análisis en particular.

5.5. Deberán aplicarse medidas de diseño prudentes, e incorporarse en las bases de diseño prácticas tecnológicas razonables para el funcionamiento normal, los incidentes operacionales previstos y los accidentes base de diseño, de modo que se logre un alto grado de certeza de que el núcleo del reactor no sufrirá daños importantes, y de que las dosis de radiación permanecerán dentro de los límites prescritos, y serán ALARA.

5.6. Tanto en la base de diseño como en el diseño se tendrá en cuenta el comportamiento de la central en accidentes concretos que excedan de los accidentes base de diseño, incluidos determinados accidentes graves. Los métodos e hipótesis utilizados para esas evaluaciones se basarán en la mejor estimación posible.

### **Categorías de estados de centrales**

5.7. Los estados de la central deberán definirse y agruparse en un número limitado de categorías según su probabilidad de aparición. Las categorías suelen incluir normalmente: el funcionamiento normal, los incidentes operacionales previstos, los accidentes base de diseño y los accidentes graves. Se asignarán a cada categoría criterios de aceptación en los que se tenga en cuenta que los SIP frecuentes deberán tener consecuencias radiológicas leves o no tenerlas en absoluto, y que los sucesos que pueden originar consecuencias graves deberán tener una probabilidad muy baja.

### **Sucesos iniciadores postulados**

5.8. En el diseño de la central deberá tenerse en cuenta que pueden surgir complicaciones en todos los niveles de defensa en profundidad, y deberán adoptarse medidas de diseño para tener la certeza de que se realizan las funciones de seguridad y de que es posible cumplir los objetivos de seguridad. Tales complicaciones se derivan de los SIP, que se seleccionan aplicando técnicas deterministas o probabilistas, o bien una combinación de ambas. Normalmente no se considera en el diseño que puedan ocurrir simultáneamente sucesos independientes, cada uno con una probabilidad baja.

### **Sucesos internos**

5.9. Deberá llevarse a cabo un análisis de los SIP (véase el Apéndice I) para determinar todos los sucesos internos que puedan afectar a la seguridad de la central. Entre ellos se pueden incluir fallos o mal funcionamiento del equipo.

### *Incendios y explosiones*

5.10. Las estructuras, sistemas y componentes de importancia para la seguridad deberán diseñarse y situarse de modo que, sin infringir otros requisitos de seguridad, se reduzca al mínimo tanto la probabilidad como los efectos de los incendios y de las explosiones ocasionados por sucesos externos o internos. Deberá mantenerse la capacidad de parada, de eliminación del calor residual, de confinamiento de los materiales radiactivos y de supervisión del estado de la central. Dichos requisitos se satisfarán mediante la adecuada incorporación de piezas redundantes, de sistemas diversos, de separación física y de diseño para la operación segura en caso de fallo, de modo que se logren los siguientes objetivos:

- 1) evitar que se declaren incendios;
- 2) detectar y extinguir rápidamente los incendios que se hayan declarado, limitando así los daños;
- 3) evitar la propagación de incendios que no hayan sido extinguidos, reduciendo así al mínimo sus efectos en las funciones esenciales de la central.

5.11. Deberá llevarse a cabo un análisis del riesgo de incendios en la central para determinar las características necesarias de las barreras contra incendios, y se deberá disponer de sistemas de detección y de extinción de incendios que tengan la capacidad necesaria.

5.12. La activación de los sistemas de extinción de incendios será automática cuando corresponda, y éstos deberán diseñarse y situarse de modo que su rotura, su funcionamiento en falso o su entrada fortuita en funcionamiento no perjudiquen apreciablemente la capacidad de las estructuras, sistemas y componentes de importancia para la seguridad, y no afecten simultáneamente a los grupos redundantes de seguridad, neutralizando así las medidas adoptadas para cumplir con el criterio de “fallo único”.

5.13. Siempre que sea posible se deberán utilizar en toda la central materiales incombustibles, retardadores del fuego y resistentes al calor, en particular en lugares tales como en la contención y la sala de control.

### *Otros riesgos internos*

5.14. En el diseño de la central deberá tenerse en cuenta la posibilidad de riesgos internos tales como inundaciones, impacto de proyectiles, latiguo de las tuberías, descarga o liberación de fluidos que pueden originar fallos del equipo o de otras instalaciones del emplazamiento. Se adoptarán medidas preventivas y de atenuación

adecuadas para que no se ponga en peligro la seguridad nuclear. Algunos sucesos externos pueden provocar incendios o inundaciones internas y pueden propiciar la generación de proyectiles. En el diseño se tendrá también en cuenta esa interacción entre sucesos externos e internos, cuando proceda.

5.15. Cuando dos sistemas de fluidos que funcionan a presiones diferentes se hallen interconectados, ambos deberán estar diseñados para resistir la mayor presión, o se adoptarán medidas para evitar que se supere la presión del sistema que funciona a presión más baja, en el supuesto de que ocurra un fallo único.

### **Sucesos externos**

5.16. Deberán determinarse los sucesos externos, tanto naturales como imputables al hombre, que influyen en la base de diseño, para la combinación propuesta de central y emplazamiento. Se tendrán en cuenta todos los sucesos que puedan estar asociados a un riesgo radiológico importante. Se utilizará una combinación de métodos probabilistas y deterministas para seleccionar un subconjunto de sucesos externos que la central esté diseñada para soportar, y a partir del cual se determinarán las bases de diseño.

5.17. Entre los sucesos naturales externos que se considerarán cabe citar los definidos en las características del emplazamiento, tales como terremotos, inundaciones, vientos fuertes, tornados, tsunamis (olas sísmicas marinas), y condiciones meteorológicas extremas. Entre los sucesos externos imputables al hombre que deberán tenerse en cuenta cabe incluir los determinados en las características del emplazamiento, de los cuales se han derivado las bases de diseño. La lista de dichos sucesos se someterá en las primeras etapas del proceso de diseño a un nuevo examen para ver si es exhaustiva.

### **Características relacionadas con el emplazamiento<sup>2</sup>**

5.18. Al establecer la base de diseño de una central nuclear deberán tenerse en cuenta las diferentes interacciones entre la central y el medio, incluidos factores tales como población, meteorología, hidrología, geología y sismología. Deberán tenerse en cuenta también la disponibilidad de servicios ubicados fuera del emplazamiento de los que puede depender la seguridad de la central y la protección de la población; por ejemplo, los servicios de suministro de electricidad y los servicios contra incendios.

---

<sup>2</sup> Véanse otras orientaciones en la Ref. [5].

5.19. Deberán evaluarse los proyectos para centrales nucleares situadas en zonas tropicales, polares, áridas o volcánicas, con vistas a identificar características especiales de diseño que puedan ser necesarias como consecuencia de las características del emplazamiento.

### **Combinaciones de sucesos**

5.20. Cuando haya combinaciones de sucesos aleatorios en particular que puedan verosíblemente dar lugar a incidentes operacionales previstos o a condiciones de accidente, deberán considerarse en el diseño. Ciertos sucesos pueden ser consecuencia de otros; por ejemplo, una inundación provocada por un terremoto. Tales efectos consiguientes deberán considerarse como parte del SIP original.

### **Reglas de diseño**

5.21. Las reglas tecnológicas de diseño para las estructuras, sistemas y componentes deberán especificarse y se ajustarán a las prácticas tecnológicas adecuadas aceptadas normalmente en el país (véase el párr. 3.6), o a las normas o prácticas ya utilizadas internacionalmente o establecidas en otro país, cuyo uso sea aplicable, y que también hayan sido aceptadas por el órgano regulador nacional.

5.22. El diseño sísmico de la central deberá proporcionar un margen suficiente de seguridad para protegerla en caso de movimientos sísmicos.

### **Límites de diseño**

5.23. Deberá especificarse un conjunto de límites de diseño que esté en consonancia con los parámetros físicos esenciales para cada estructura, sistema o componente, en situaciones operacionales y en accidentes base de diseño.

### **Estados operacionales**

5.24. La central deberá diseñarse de forma que funcione con seguridad dentro de un ámbito definido de parámetros (por ejemplo de presión, temperatura, energía), y se dará por supuesto que se dispone de un conjunto mínimo de equipos auxiliares del sistema de seguridad (por ejemplo capacidad de alimentación de agua auxiliar y suministro de energía eléctrica de emergencia). En el diseño se deberá tener en cuenta que la respuesta a una amplia gama de incidentes operacionales previstos permita el funcionamiento o la parada seguros, en caso necesario, sin necesidad de recurrir a disposiciones que vayan más allá del primer nivel de defensa en profundidad o como máximo del segundo.

5.25. En el diseño deberá tenerse en cuenta la posibilidad de accidentes en situaciones de parada o de funcionamiento a baja potencia, tales como puesta en marcha, recarga de combustible y mantenimiento, es decir cuando puede verse reducida la disponibilidad de sistemas de seguridad. Deberán especificarse las limitaciones adecuadas sobre la falta de disponibilidad de dichos sistemas.

5.26. En el proceso de diseño se establecerá un conjunto de requisitos y limitaciones para el funcionamiento seguro, que incluya:

- 1) puntos de tarado de los sistemas de seguridad;
- 2) restricciones de sistemas de control y de procedimiento en procesos variables y otros parámetros importantes;
- 3) requisitos para las actividades de mantenimiento, ensayo e inspección de la central con el fin de garantizar que las estructuras, sistemas y componentes funcionan tal como estaba previsto en el diseño, teniendo en cuenta el principio ALARA;
- 4) configuraciones operacionales claramente definidas, incluidas restricciones operacionales en caso de averías de los sistemas de seguridad.

Estos requisitos y limitaciones servirán de base para el establecimiento de límites y condiciones operacionales en virtud de las cuales se autorizará a la entidad explotadora a llevar a cabo las actividades de explotación de la central.

### **Accidentes base de diseño**

5.27. De la lista de SIP que figura en el Apéndice I deberán deducirse un conjunto de accidentes base de diseño, con el fin de establecer condiciones límites según las cuales se diseñarán las estructuras, sistemas y componentes de importancia para la seguridad.

5.28. Cuando se requiera una acción pronta y fiable como respuesta a un SIP, se establecerán disposiciones para iniciar automáticamente las acciones necesarias de los sistemas de seguridad, con el fin de evitar que éste degenera en una situación más grave que pueda poner en peligro la próxima barrera. Cuando no sea necesaria una acción rápida, puede permitirse la activación manual de sistemas u otras acciones del operador, siempre que se realicen con el tiempo suficiente y que se definan los procedimientos adecuados (administrativos, operacionales y de emergencia) para la fiabilidad de dichas acciones.

5.29. Deberán tenerse en cuenta las acciones del operador que puedan ser necesarias para diagnosticar el estado de la central y colocar a ésta en una situación de parada

estable a largo plazo, de forma oportuna, y facilitarse la instrumentación adecuada para supervisar la situación de la central y los controles necesarios para el funcionamiento manual del equipo.

5.30. El equipo necesario para la respuesta manual y para los procesos de recuperación deberá situarse en el lugar más adecuado para que se pueda disponer fácilmente de él en el momento en que se necesite, y para permitir el acceso humano en las condiciones ambientales previstas.

### **Accidentes graves**

5.31. Determinados estados de la central, de probabilidad muy baja, que excedan de las condiciones de accidente base de diseño y que puedan ocurrir por múltiples fallos de los sistemas de seguridad que originen un importante deterioro del núcleo, pueden poner en peligro la integridad de todas las barreras que impiden la liberación del material radiactivo, o gran parte de ellas. Estas secuencias de sucesos se denominan accidentes graves. Deberá prestarse atención a estas secuencias de accidentes graves, utilizando una combinación de criterios tecnológicos y métodos probabilistas, con el fin de determinar las secuencias para las que pueden determinarse medidas preventivas o de atenuación, razonablemente aplicables. Dichas medidas no han de suponer necesariamente la aplicación de prácticas prudentes de ingeniería, utilizadas en la determinación y evaluación de accidentes base de diseño, sino que más bien deberían basarse en hipótesis realistas o aproximativas, o en métodos y criterios analíticos. Sobre la base de la experiencia operacional, de los análisis de seguridad pertinentes y de los resultados de la investigación relacionada con la seguridad, en las actividades de diseño para abordar los casos de accidente grave se tendrá en cuenta lo siguiente:

- 1) Deberán definirse secuencias importantes de sucesos que puedan provocar un accidente grave, utilizando una combinación de métodos probabilistas, métodos deterministas y criterios de ingeniería razonables;
- 2) Dichas secuencias de sucesos se revisarán en función de una serie de criterios encaminados a determinar qué accidentes graves habrá que tener en cuenta en el diseño;
- 3) Se evaluarán y aplicarán, si es posible, las posibles modificaciones del diseño o los cambios de procedimiento que puedan reducir la probabilidad de esos sucesos o atenuar sus consecuencias en caso de que ocurran;
- 4) Deberá prestarse atención a todos los elementos de diseño de la central, incluido el posible uso de algunos sistemas (por ejemplo, sistemas de seguridad y sistemas no relacionados con la seguridad) que vayan más allá de la función a que se destinen originalmente y de los estados operacionales previstos, así

como el uso de otros sistemas provisionales para restablecer un estado controlado de la central y atenuar las consecuencias de un accidente grave, si puede demostrarse que los sistemas son capaces de funcionar en las condiciones ambientales que cabe prever;

- 5) Para centrales con varias unidades, se tendrá en cuenta el uso de los medios de que se disponga, o el apoyo de otras unidades, siempre que no se vea comprometido el funcionamiento seguro de dichas unidades;
- 6) Deberán establecerse procedimientos de gestión de accidentes, teniendo en cuenta los casos de accidentes graves representativos y dominantes.

## DISEÑO PARA LOGRAR LA FIABILIDAD DE LAS ESTRUCTURAS, SISTEMAS Y COMPONENTES

5.32. Las estructuras, sistemas y componentes de importancia para la seguridad se diseñarán de modo que puedan resistir con la suficiente fiabilidad a todos los SIP determinados (véase el Apéndice I).

### **Fallos de causa común**

5.33. Se tendrán en cuenta las posibilidades de fallo de causa común de elementos de importancia para la seguridad con el fin de determinar cuándo deben aplicarse los principios de diversidad, redundancia e independencia para lograr la fiabilidad necesaria.

### **Criterio de fallo único**

5.34. El criterio de fallo único se aplicará a cada grupo de seguridad incorporado en el diseño de la central.

5.35. Para comprobar que una central nuclear se ajusta al criterio del fallo único se analizarán los conjuntos de componentes pertinentes de la manera descrita a continuación. Se supondrá que se produce un fallo único (y los consiguientes efectos de tal fallo) sucesivamente en cada uno de los elementos de un conjunto hasta que se hayan estudiado todos los fallos en ese conjunto. Los análisis de cada conjunto pertinente se realizarán en secuencia hasta que se hayan estudiado todos los conjuntos y todos los fallos. (En la presente publicación de Requisitos de seguridad, las funciones de seguridad o los sistemas que contribuyen a realizar esas funciones, a los cuales hay que aplicar el criterio de redundancia con el fin de lograr la fiabilidad necesaria, se identifican por el concepto “hipótesis de fallo único”.) La hipótesis de fallo único en ese sistema es parte del proceso descrito. Durante el análisis de un fallo único no se supondrá en ningún momento que se produce más de un fallo aleatorio.

5.36. Al aplicar este concepto a un grupo o sistema de seguridad, el funcionamiento en falso se considerará como una modalidad de fallo.

5.37. Se considerará que se ha cumplido el criterio cuando se demuestre que cada grupo de seguridad cumple sus respectivas funciones de seguridad cuando se le aplican los análisis anteriormente mencionados, en las siguientes condiciones:

- 1) cuando se supone que el SIP ha ocasionado daños en el grupo de seguridad; y
- 2) cuando se supone la peor configuración permisible de los sistemas de seguridad que llevan a cabo las funciones de seguridad necesarias, teniendo en cuenta las actividades de mantenimiento, ensayo, inspección y reparación, así como los momentos en que se permita que el equipo esté fuera de servicio.

5.38. El incumplimiento del criterio de fallo único tendrá carácter excepcional, y deberá estar claramente justificado en el análisis de seguridad.

5.39. Al llevar a cabo el análisis de un fallo único puede resultar innecesario suponer el fallo de un componente pasivo diseñado, fabricado, inspeccionado y mantenido en servicio con un nivel de calidad muy elevado, siempre que éste no se vea afectado por el SIP. Sin embargo, cuando se supone que un componente pasivo no falla, tal supuesto analítico deberá justificarse teniendo en cuenta las cargas y las condiciones ambientales, así como el intervalo total de tiempo a partir del suceso iniciador durante el cual sea necesario que funcione dicho componente.

### **Diseño según el principio del “fallo sin riesgo”**

5.40. El principio del “fallo sin riesgo” deberá considerarse e introducirse, cuando sea factible, en el diseño de los sistemas y componentes de importancia para la seguridad de una central. Si un sistema o un componente falla, los sistemas de la central deberán estar diseñados para que ésta pase a un estado seguro sin que sea necesario iniciar ninguna acción.

### **Servicios auxiliares**

5.41. Los servicios auxiliares para el equipo que forme parte de un sistema de importancia para la seguridad deberán considerarse como parte de dicho sistema y clasificarse en consecuencia. Su fiabilidad, redundancia, diversidad e independencia, así como la dotación de dispositivos de aislamiento y ensayo de su capacidad funcional, deberán estar en consonancia con la fiabilidad del sistema al que sirven de apoyo.



Entre los servicios auxiliares necesarios para mantener la central en un estado seguro pueden incluirse el suministro de electricidad, agua de refrigeración y aire comprimido u otros gases, y los medios de lubricación.

### **Interrupción del funcionamiento del equipo**

5.42. El diseño se realizará de modo que, mediante la aplicación de medidas como, por ejemplo, una mayor redundancia, puedan llevarse a cabo actividades razonables de mantenimiento y de ensayo de sistemas de importancia para la seguridad en condiciones de funcionamiento, sin necesidad de parar la central. Deberán tenerse en cuenta las interrupciones de funcionamiento del equipo, incluida la falta de disponibilidad de sistemas o componentes debida a fallos, y se incluirán en esta consideración las consecuencias del mantenimiento anticipado y de las actividades de ensayo y reparación para la fiabilidad de cada sistema individual de seguridad, con el fin de garantizar que la función de seguridad pueda llevarse a cabo con la fiabilidad necesaria. El plazo permitido para las interrupciones de funcionamiento del equipo y para las medidas que haya que adoptar deberá analizarse y definirse para cada caso antes de poner en funcionamiento la central, y se incluirá en las instrucciones de funcionamiento.

### **DISPOSICIONES PARA LOS ENSAYOS, EL MANTENIMIENTO, LA REPARACIÓN, LA INSPECCIÓN Y LA VIGILANCIA EN SERVICIO**

5.43. Las estructuras, sistemas y componentes de importancia para la seguridad, con excepción de los descritos en el párr. 5.44, deberán diseñarse de modo que puedan calibrarse, ensayarse, mantenerse, repararse o reemplazarse, inspeccionarse y vigilarse para comprobar su capacidad funcional durante toda la vida útil de la central con objeto de demostrar que se cumplen los objetivos de fiabilidad. El diseño será tal que permita que estas actividades se vean facilitadas y puedan llevarse a cabo con arreglo a normas acordes con la importancia de las funciones de seguridad que hayan de desempeñar, sin exposición indebida del personal del emplazamiento a las radiaciones.

5.44. Si las estructuras, sistemas y componentes de importancia para la seguridad no pueden diseñarse de modo que sea posible probarlos, inspeccionarlos y vigilarlos en la medida necesaria, se adoptarán los siguientes criterios:

- se especificarán otros métodos alternativos o indirectos, tales como la vigilancia de los elementos de referencia o el uso de métodos de cálculo verificados y validados; y

- se aplicarán márgenes prudentes de seguridad o se adoptarán otras precauciones adecuadas de seguridad para contrarrestar posibles fallos imprevistos.

## CUALIFICACIÓN DEL EQUIPO

5.45. Se adoptará un procedimiento de cualificación para confirmar que los elementos de importancia para la seguridad son capaces de llevar a cabo, a lo largo de toda su vida útil, las funciones que se exigen de ellos, aun estando sujetos a condiciones ambientales de vibración, temperatura, presión, erosión del chorro, interferencia electromagnética, irradiación, humedad o cualquier posible combinación de estos factores, que son los dominantes en una emergencia. Entre las condiciones ambientales que se han de considerar se incluirán las variaciones previstas en el funcionamiento normal, los incidentes operacionales previstos y los accidentes base de diseño. En el programa de cualificación deberán tenerse en cuenta los efectos de envejecimiento causados por diversos factores ambientales (como la vibración, la irradiación y las temperaturas extremas) durante la vida útil prevista del equipo. Cuando el equipo está sometido a sucesos naturales externos y ha de cumplir una función de seguridad durante el suceso o después de él, el programa de cualificación deberá reproducir en la medida de lo posible las condiciones impuestas al equipo, sea mediante un ensayo, un análisis, o una combinación de ambos.

5.46. En el programa de cualificación se incluirá asimismo cualquier condición ambiental inédita que pueda preverse razonablemente y que pueda derivarse de estados operacionales concretos, como por ejemplo, un ensayo periódico del coeficiente de pérdida de la contención. Debería demostrarse en la medida de lo posible que el equipo (como ciertos instrumentos) que debe funcionar en condiciones de accidente grave puede realizar, con una fiabilidad razonable, las funciones previstas en el diseño.

## ENVEJECIMIENTO

5.47. Deberán establecerse en el diseño márgenes adecuados para todas las estructuras, sistemas y componentes de importancia para la seguridad, de forma que se tengan en cuenta los mecanismos pertinentes de envejecimiento y desgaste, y el posible deterioro relacionado con el envejecimiento, con objeto de asegurar la capacidad de la estructura, sistema o componente para realizar la función de seguridad necesaria durante toda su vida útil. Asimismo se tendrán en cuenta los efectos de envejecimiento y desgaste en todas las situaciones de funcionamiento normales, ensayos, mantenimiento, interrupciones ocasionadas por el mantenimiento, estados

de la central en caso de un SIP y posteriores a los SIP. También se adoptarán medidas para la vigilancia, ensayo, recogida de muestras e inspección, con el fin de evaluar los mecanismos de envejecimiento previstos en el diseño e identificar comportamientos o deterioros imprevistos que pudieran ocurrir en servicio.

## FACTORES HUMANOS

### **Diseño para una actuación óptima del operador**

5.48. El diseño deberá ser “fácilmente comprensible para el operador”, y su objetivo será limitar las consecuencias de los errores humanos. Deberá prestarse atención al diseño de la central y a los procedimientos administrativos, operacionales y de emergencia, incluidas las actividades de mantenimiento e inspección, con el fin de facilitar la interfaz entre la central y el personal encargado de su explotación.

5.49. Las zonas de trabajo y el entorno de trabajo del personal del emplazamiento deberán diseñarse con arreglo a principios ergonómicos.

5.50. La consideración sistemática de los factores humanos y la interfaz hombre-máquina se deberá incluir en el proceso de diseño en una fase temprana del desarrollo de éste y proseguir a lo largo de todo el proceso para garantizar una distinción clara y adecuada de funciones entre el personal encargado del funcionamiento y los sistemas automáticos existentes.

5.51. La interfaz hombre-máquina deberá diseñarse de modo que proporcione a los operadores una información amplia pero fácilmente manejable, compatible con el plazo necesario para adoptar decisiones y llevar a cabo acciones. Se adoptarán medidas similares para las salas complementarias de control.

5.52. Deberán incluirse en las fases apropiadas la verificación y validación de aspectos de los factores humanos, para confirmar que el diseño se ajusta adecuadamente a todas las actividades necesarias de los operadores.

5.53. Para facilitar el establecimiento de criterios de diseño para la presentación visual de información y para los controles, se considerará que el operador tiene una función doble: la de un gerente de sistemas, incluida la gestión de accidentes, y la de un operador de equipo.

5.54. En su función de gerente de sistemas, el operador necesita información que le permita:

- 1) evaluar fácilmente el estado general de la central sea cual fuere la situación en que se encuentre, a saber, funcionamiento normal, un incidente operacional previsto o una condición de accidente, y confirmar que se están realizando las acciones automáticas de seguridad previstas en el diseño; y
- 2) determinar las acciones apropiadas, iniciadas por el operador, que convenga adoptar.

5.55. En su función de operador de equipo, se facilitará al operador información suficiente sobre los parámetros correspondientes a los distintos sistemas y equipos de la central, para confirmar que pueden iniciarse con garantía las acciones de seguridad necesarias.

5.56. El diseño deberá encaminarse a promover el éxito de las acciones del operador teniendo en cuenta el tiempo disponible, el medio físico previsto y la presión psicológica sobre el operador. Conviene reducir al mínimo la necesidad de que el operador intervenga en breves plazos de tiempo. Deberá tenerse en cuenta en el diseño que la necesidad de tal intervención sólo es aceptable cuando el autor del diseño pueda demostrar que el operador tiene tiempo suficiente para adoptar una decisión y actuar; que la información que necesita el operador para adoptar la decisión de actuar se presenta de manera simple e inequívoca; y que es aceptable el ambiente físico existente a continuación del suceso en la sala de control o en la sala complementaria de control y en el acceso a dicha sala complementaria de control.

## OTRAS CONSIDERACIONES DE DISEÑO

### **Estructuras, sistemas y componentes compartidos entre reactores**

5.57. Las estructuras, sistemas y componentes de importancia para la seguridad no deberán ser compartidos por dos o más reactores en las centrales nucleares. Si en casos excepcionales dichas estructuras, sistemas y componentes de importancia para la seguridad son compartidos entre dos o más reactores, deberá demostrarse que se cumplen todos los requisitos de seguridad para todos los reactores y en todas las situaciones operacionales (incluido el mantenimiento) y en los accidentes base de diseño. En caso de que se produzcan accidentes graves en uno de los reactores, deberá poder conseguirse una parada ordenada, el enfriamiento, y la eliminación del calor residual de los demás reactores.

### **Sistemas que contienen materiales fisiónables o radiactivos**

5.58. Todos los sistemas de una central nuclear que puedan contener materiales fisiónables o radiactivos deberán diseñarse de modo que quede suficientemente

garantizada la seguridad, tanto en situaciones operacionales como en accidentes base de diseño.

### **Centrales nucleares usadas para la cogeneración, generación de calor o desalación**

5.59. Las centrales nucleares acopladas con unidades de utilización de calor (como por ejemplo, calefacción de distrito) y unidades de desalación de agua deberán diseñarse de modo que se evite el transporte de materiales radiactivos de la central a la unidad de desalación o de calefacción de distrito en condiciones de funcionamiento normal, incidentes operacionales previstos, accidentes base de diseño y accidentes graves.

### **Transporte y almacenamiento del combustible y de los desechos radiactivos**

5.60. El diseño deberá incorporar elementos adecuados para facilitar el transporte y la manipulación del combustible nuevo, del combustible gastado y de los desechos radiactivos. Deberá tenerse en cuenta el acceso a las instalaciones y las posibilidades de levantamiento de cargas y de almacenamiento.

### **Salidas de emergencia y medios de comunicación**

5.61. La central nuclear deberá tener un número suficiente de salidas de emergencia señaladas de un modo claro y duradero, con iluminación de emergencia fiable, ventilación y otras características esenciales para el empleo seguro de esas salidas. Las salidas de emergencia deberán cumplir los requisitos internacionales pertinentes relativos a la delimitación de zonas de radiación y a la protección contra incendios, así como los requisitos nacionales pertinentes de seguridad industrial y seguridad de las centrales.

5.62. Deberán preverse sistemas de alarma y medios de comunicación adecuados de modo que todas las personas que se encuentren en la central y en el emplazamiento puedan recibir aviso e instrucciones, aun en condiciones de accidente.

5.63. Deberá contarse en todo momento con los medios de comunicación necesarios para la seguridad dentro de la central nuclear, en las zonas más próximas y en las entidades fuera del emplazamiento, según lo estipulado en el plan de emergencia. En el diseño deberán tenerse en cuenta estos requisitos y la diversidad de los métodos de comunicación elegidos.

### **Control de accesos**

5.64. La central deberá estar aislada de las zonas circundantes mediante el diseño adecuado de los elementos estructurales de forma que el acceso a sus instalaciones esté permanentemente controlado. En especial, en el diseño de los edificios y en la distribución del emplazamiento se deberán adoptar disposiciones para el personal y/o el equipo de control de los accesos, y deberá prestarse atención a las medidas para impedir la entrada en la central de personas y mercancías no autorizadas.

5.65. Deberá evitarse el acceso no autorizado, o toda clase de interferencia, con estructuras, sistemas y componentes de importancia para la seguridad. Cuando el acceso sea necesario para llevar a cabo actividades de mantenimiento, ensayo o inspección, en el diseño se velará por que puedan llevarse a cabo las actividades necesarias sin reducir notablemente la fiabilidad del equipo de seguridad conexo.

### **Interacciones de sistemas**

5.66. Si hay una probabilidad elevada de que sea preciso que sistemas de importancia para la seguridad funcionen simultáneamente, deberá evaluarse su posible interacción. En el análisis se tendrán en cuenta no sólo las interconexiones físicas, sino también los posibles efectos del funcionamiento, el mal funcionamiento o el fallo de un sistema en el entorno físico de otros sistemas esenciales, con el fin de conseguir que los cambios del entorno no afecten a la fiabilidad de los componentes del sistema en su funcionamiento previsto.

### **Interacciones entre la red eléctrica y la central**

5.67. En el diseño de la central se tendrán en cuenta las interacciones entre la central y la red eléctrica, incluido el número de líneas de suministro de electricidad a la central y la independencia entre ellas, en relación con la fiabilidad necesaria del suministro de electricidad a los sistemas de la central que sean de importancia para la seguridad.

### **Clausura**

5.68. En la fase de diseño deberá prestarse especial atención a la incorporación de elementos que faciliten las actividades de clausura y desmantelamiento de la central. En especial, deberá tenerse en cuenta en el diseño:

- 1) la elección de materiales, de modo que se reduzcan a un mínimo las posibles cantidades de desechos radiactivos y se facilite la descontaminación;

- 2) las posibilidades de acceso que puedan ser necesarias; y
- 3) las instalaciones necesarias para el almacenamiento de los desechos radiactivos generados tanto en la explotación como en la clausura de la central.

## ANÁLISIS DE SEGURIDAD

5.69. 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 párr. 5.7), y que se ha hecho efectiva la defensa en profundidad.

5.70. Deberán verificarse y validarse los programas informáticos, los métodos analíticos y los modelos de central utilizados en el análisis de seguridad, y también se prestará la debida atención a las incertidumbres.

### **Enfoque determinista**

5.71. El análisis determinista de seguridad incluirá los siguientes puntos:

- 1) confirmación de que los límites y condiciones operacionales cumplen los supuestos y lo previsto en el diseño para el funcionamiento normal de la central;
- 2) caracterización de los SIP (véase el Apéndice I) que sean apropiados, teniendo en cuenta el diseño de la central y su ubicación;
- 3) análisis y evaluación de las secuencias de sucesos resultantes de los SIP;
- 4) comparación de los resultados del análisis con los criterios de aceptación radiológica y con los límites de diseño;
- 5) establecimiento y confirmación de la base de diseño; y
- 6) demostración de que es posible afrontar los incidentes operacionales previstos y las condiciones de accidente base de diseño, gracias a la respuesta automática de los sistemas de seguridad, en combinación con las acciones prescritas del operador.

5.72. Deberá verificarse la aplicabilidad de las hipótesis analíticas, los métodos y el grado de precaución. Se actualizará el análisis de seguridad del diseño de la central teniendo en cuenta los cambios de importancia que ocurran en la configuración de la central, la experiencia adquirida en la explotación, los adelantos técnicos y la

comprensión de los fenómenos físicos; el análisis deberá estar en consonancia con la situación actual o “tal como la central está construida”.

### **Enfoque probabilista**

5.73. Deberá llevarse a cabo un análisis probabilista de seguridad de la central con objeto de:

- 1) proporcionar un análisis sistemático que garantice que el diseño cumplirá con los objetivos generales de seguridad;
- 2) demostrar que se ha logrado un diseño equilibrado, de modo que ningún elemento en particular, o ningún SIP contribuya de forma excesiva o considerablemente incierta a un riesgo general, y que la responsabilidad primordial de la seguridad nuclear recaiga en los dos primeros escalones de defensa en profundidad;
- 3) cerciorarse de que se evitarán pequeñas desviaciones de los parámetros de la central que pudieran originar un comportamiento gravemente anormal de la misma (“efectos abismales”);
- 4) proporcionar evaluaciones de las probabilidades de que ocurran averías graves en el núcleo, y evaluaciones de los riesgos de liberaciones importantes de material radiactivo fuera del emplazamiento, que precisen una rápida respuesta, especialmente en caso de liberaciones asociadas con fallos de la contención;
- 5) proporcionar evaluaciones de las probabilidades de que haya riesgos externos y de sus consecuencias, en particular en relación con el emplazamiento de la central;
- 6) determinar sistemas en los que las mejoras de diseño o las modificaciones en los procedimientos operacionales podrían reducir las probabilidades de accidente grave o atenuar sus consecuencias;
- 7) evaluar la idoneidad de los procedimientos de emergencia de la central; y
- 8) verificar que se cumplen los objetivos probabilistas, si los hubiere.

## **6. REQUISITOS PARA EL DISEÑO DE SISTEMAS DE CENTRALES**

### **NÚCLEO DEL REACTOR Y SISTEMAS CONEXOS**

#### **Diseño general**

6.1. El núcleo del reactor y los correspondientes sistemas de protección, control y refrigeración se diseñarán de modo que dispongan de márgenes apropiados para



conseguir que no se superen los límites especificados en el diseño y que se apliquen las normas de seguridad en todas las situaciones operacionales y en accidentes base de diseño, teniendo debidamente en cuenta las incertidumbres existentes.

6.2. El núcleo del reactor y los componentes que forman parte de él, situados en la vasija, se diseñarán y montarán de tal modo que resistan las cargas estáticas y dinámicas previstas en situaciones operacionales, accidentes base de diseño y sucesos externos, de manera que se pueda garantizar la parada del reactor en condiciones de seguridad, se mantenga el reactor en estado subcrítico y se asegure la refrigeración del núcleo.

6.3. Deberá limitarse el grado máximo de reactividad positiva y su velocidad máxima de crecimiento por inserción, en situaciones operacionales y de accidente base de diseño, de modo que no se produzca ningún fallo de la barrera de presión del reactor, que se mantenga la capacidad de refrigeración y que el núcleo del reactor no sufra daños importantes.

6.4. En el diseño deberá asegurarse que se reduzca a un mínimo la probabilidad de recriticidad o de aumento brusco de la reactividad a raíz de un SIP.

6.5. El núcleo del reactor y los correspondientes sistemas de protección, refrigeración y control se diseñarán de forma que permitan llevar a cabo las actividades de inspección y ensayo adecuadas durante la vida útil de la central.

### **Elementos y conjuntos combustibles**

6.6. Los elementos y conjuntos combustibles deberán diseñarse de modo que resistan satisfactoriamente las condiciones de irradiación y ambientales existentes en el núcleo del reactor combinadas con todos los procesos de deterioro que puedan tener lugar en situaciones de funcionamiento normal y en incidentes operacionales previstos.

6.7. El deterioro que ha de tenerse en cuenta será el producido por lo siguiente: la expansión y deformación diferencial; la presión externa del refrigerante; el aumento de la presión interna resultante de los productos de fisión en el elemento combustible; la irradiación del combustible y otros materiales en el conjunto combustible; los cambios de presión y temperatura resultantes de cambios en la demanda de energía; los efectos químicos; las cargas estáticas y dinámicas, incluidas las vibraciones inducidas por flujo y las mecánicas, y los cambios de comportamiento de la transmisión térmica que puedan proceder de deformaciones o efectos químicos. Deberán tenerse en cuenta las inexactitudes de los datos y cálculos y de la fabricación.

6.8. En funcionamiento normal no deberán sobrepasarse los límites de diseño especificados para el combustible, incluidas las fugas admisibles de productos de fisión, y deberá garantizarse que los estados operacionales que puedan derivarse de incidentes operacionales previstos no causen mayor deterioro. Las fugas de productos de fisión deberán quedar restringidas por los límites del diseño y mantenerse en un valor mínimo.

6.9. Los conjuntos combustibles deberán diseñarse de modo que sea posible la adecuada inspección de sus estructuras y componentes después de la irradiación. En caso de accidentes base de diseño, los elementos combustibles deberán permanecer en posición y sin sufrir tal grado de deformación que resulte ineficaz la refrigeración del núcleo después del accidente; no deberán rebasarse los límites especificados para los elementos combustibles en caso de accidente base de diseño.

6.10. Los requisitos anteriormente mencionados para el diseño del reactor y de los elementos combustibles deberán mantenerse también en caso de que se produzcan cambios en la estrategia de gestión del combustible o en los estados operacionales durante la vida útil de la central.

### **Control del núcleo del reactor**

6.11. Deberán cumplirse las disposiciones de los párrs. 6.3 a 6.10 para todos los niveles y distribuciones del flujo neutrónico que puedan producirse en todas las situaciones del núcleo, incluidas las posteriores a la parada, durante la recarga de combustible o posteriormente a la misma, y las originadas por incidentes operacionales previstos y por accidentes base de diseño. Los medios de detección de esas formas de flujo deberán ser tales que no haya zonas en el núcleo en las que puedan incumplirse las disposiciones de los párrs. 6.3 a 6.10 sin posibilidad de descubrirlo. El diseño del núcleo deberá reducir suficientemente la necesidad de que el sistema de control mantenga las formas, los niveles y la estabilidad del flujo dentro de los límites estipulados para todas las situaciones operacionales.

6.12. Deberán establecerse disposiciones para la eliminación de sustancias no radiactivas, incluidos los productos de corrosión que pueden poner en peligro la seguridad del sistema, por ejemplo, atascando los conductos de refrigeración.

### **Parada del reactor**

6.13. Se dispondrá lo necesario para asegurar la capacidad de parar el reactor en las situaciones operacionales y en accidentes base de diseño, y para mantener parado el reactor aún en condiciones de máxima reactividad del núcleo. La efectividad, rapidez

de acción y los márgenes de parada de dichos sistemas deberán ser tales que no se rebasen los límites especificados. Con el fin de controlar la reactividad y regular el flujo en situaciones de funcionamiento a potencia normal, puede utilizarse una parte de los sistemas de parada siempre que la capacidad de parada se mantenga en todo momento dentro de un margen adecuado.

6.14. Para la parada del reactor deberá contarse al menos con dos sistemas distintos, con el fin de lograr diversidad.

6.15. Uno de esos dos sistemas, por lo menos, deberá ser capaz por sí solo de hacer subcrítico rápidamente el reactor nuclear, con un margen adecuado de seguridad en situaciones operacionales y accidentes base de diseño, en caso de fallo único. Con carácter excepcional puede permitirse una recriticidad transitoria siempre que no se rebasen los límites especificados para el combustible y los componentes.

6.16. Uno de esos dos sistemas, por lo menos, deberá ser capaz por sí solo de hacer subcrítico el reactor nuclear en condiciones operacionales normales, en incidentes operacionales previstos y en accidentes base de diseño, y de mantenerlo en dicho estado, con un margen adecuado de seguridad y elevada fiabilidad aun en condiciones de máxima reactividad del núcleo.

6.17. Al juzgar la idoneidad de los sistemas de parada, deberá prestarse atención a los fallos que se pudieran producir en cualquier parte de la central y a consecuencia de los cuales pudiera quedar inoperante un sector de los sistemas de parada (tales como un fallo en la inserción de una barra de control) o que pudieran provocar un fallo por causa común.

6.18. Los sistemas de parada deberán ser adecuados para evitar o hacer frente a aumentos accidentales de reactividad por inserción durante la parada, incluida la recarga de combustible en ese estado. Para cumplir esa disposición deberán tenerse en cuenta las operaciones deliberadas que aumentan la reactividad durante la situación de parada (tales como el desplazamiento del absorbente para operaciones de mantenimiento, la dilución del contenido en boro y la recarga del combustible), conjuntamente con un fallo único en los sistemas de parada.

6.19. Se proveerán sistemas de instrumentación y se especificarán ensayos para garantizar que los sistemas de parada permanezcan en todo momento en la situación estipulada para la condición de la central.

6.20. En el diseño de los dispositivos de control de la reactividad deberán tenerse en cuenta el deterioro y efectos de la irradiación como quemaduras, cambios en las propiedades físicas y producción de gases.

## SISTEMA DE REFRIGERACIÓN DEL REACTOR

### **Diseño del sistema de refrigeración del reactor**

6.21. El sistema de refrigeración del reactor, sus sistemas auxiliares conexos y los sistemas de control y de protección deberán diseñarse con un margen de seguridad suficiente para que las condiciones de diseño de la barrera de presión del refrigerante no se sobrepasen en situaciones operacionales. Deberán tomarse medidas para garantizar que el funcionamiento de los dispositivos de alivio de la presión, aún en situaciones de accidente base de diseño, no ocasionen liberaciones excesivas de material radiactivo procedente de la central. La barrera de presión del refrigerante del reactor deberá estar provista de sistemas de aislamiento adecuado para limitar cualquier pérdida de fluido radiactivo.

6.22. Las partes componentes que contienen el refrigerante del reactor, tales como la vasija de presión del reactor o los tubos de presión, las tuberías y acoplamientos, las válvulas, las conexiones, las bombas, los circuladores e intercambiadores de calor, así como los sistemas de fijación de dichas piezas deberán diseñarse de modo que resistan las cargas estáticas y dinámicas previstas en todas las situaciones operacionales y de accidente base de diseño. Los materiales utilizados en la fabricación de las partes componentes deberán seleccionarse de manera que se reduzca a un mínimo la activación del material.

6.23. La vasija de presión y los tubos de presión del reactor se deberán diseñar y construir para que sean de la más elevada calidad por lo que respecta a selección de materiales, normas de diseño, capacidad de inspección y fabricación.

6.24. La barrera de presión del refrigerante del reactor deberá diseñarse de forma que sea muy improbable que se produzcan fisuras, y que cualquier fisura que se produzca se propague en un medio de elevada resistencia a las fracturas inestables con rápida propagación de las grietas, con el fin de permitir la pronta detección de dichas fisuras (por ejemplo mediante la aplicación del principio de fuga antes de la rotura). Deberán evitarse los diseños y estados de la central que propicien la fragilidad de los componentes de la barrera de presión del refrigerante del reactor.

6.25. En el diseño se deberá tomar en consideración todas las condiciones en que ha de trabajar el material de la barrera en los estados operacionales, incluidos los de mantenimiento y ensayo, y en las situaciones de accidente base de diseño, y se tendrá en cuenta el estado previsto al final de la vida útil de las propiedades afectadas por la erosión, fluencia, fatiga, entorno químico, entorno radiactivo y envejecimiento, así

como cualquier incertidumbre en la determinación del estado inicial de los componentes y la rapidez del posible deterioro.

6.26. Para todas las situaciones operacionales y de accidente base de diseño, los componentes contenidos en el interior del confinamiento a presión del refrigerante del reactor, tales como impulsores de bombas y piezas de válvulas, deberán diseñarse de modo que se reduzca al mínimo la probabilidad de fallo y de desperfectos resultantes de otros componentes del sistema primario de refrigeración importantes para la seguridad, y se deberá tener debidamente en cuenta el deterioro que pueda producirse durante el funcionamiento.

### **Inspección en servicio de la barrera de presión del refrigerante del reactor**

6.27. Los componentes de la barrera de presión del refrigerante del reactor se deberán diseñar, fabricar y disponer de modo que sea posible realizar, durante la vida útil de la central y a intervalos adecuados, las inspecciones y ensayos de la barrera que se consideren adecuados. Deberán adoptarse medidas para realizar un programa de vigilancia de materiales para la barrera de presión del refrigerante del reactor, especialmente en los lugares de irradiación elevada, y para otros componentes de importancia en que así corresponda, con el fin de determinar las consecuencias metalúrgicas de factores tales como la irradiación, la fisuración por tensocorrosión, la fragilización térmica y el envejecimiento de los materiales estructurales.

6.28. Deberá asegurarse la posibilidad de inspeccionar o someter a ensayo, directa o indirectamente, los componentes de la barrera de presión del refrigerante del reactor, según la importancia que para la seguridad tengan tales componentes, para demostrar la inexistencia de defectos que rebasen los límites de admisibilidad o de un deterioro importante de la seguridad.

6.29. Deberán vigilarse los indicadores de la integridad de la barrera de presión del refrigerante del reactor (tales como las fugas). Los resultados de dichas mediciones deberán tenerse en cuenta para determinar qué tipo de inspecciones son necesarias para la seguridad.

6.30. Si el análisis de seguridad de la central nuclear indica que determinados fallos en el sistema secundario de refrigeración pueden tener consecuencias graves, deberá velarse por que sea posible inspeccionar las piezas pertinentes de dicho sistema.

### **Inventario del refrigerante del reactor**

6.31. Se deberán adoptar disposiciones para controlar el inventario y la presión del refrigerante con el fin de que no se rebasen los límites especificados en el diseño en ninguna situación operacional, teniendo en cuenta los cambios volumétricos y las fugas. Los sistemas que llevan a cabo esta función deberán poseer suficiente capacidad (tasa de flujo y volumen de depósito) para cumplir ese requisito. Pueden estar formados por componentes necesarios para los procesos de generación de electricidad o servir exclusivamente para llevar a cabo esa función.

### **Depuración del refrigerante del reactor**

6.32. Deberá disponerse de instalaciones adecuadas para la eliminación de sustancias radiactivas procedentes del refrigerante del reactor, incluidos los productos que activan la corrosión y los productos de fisión fugados del combustible. La capacidad de los sistemas necesarios se basará en los límites especificados en el diseño del combustible para las fugas admisibles, con un margen prudencial para asegurar que la central pueda funcionar con un nivel de actividad de circuito tan bajo como sea razonablemente posible, y que las liberaciones de material radiactivo cumplan con el principio ALARA y no rebasen los límites prescritos.

### **Eliminación del calor residual del núcleo**

6.33. Se deberá disponer de medios para eliminar el calor residual. La función de seguridad de estos medios consistirá en transmitir el calor de desintegración de los productos de fisión y otros calores residuales del núcleo del reactor a una tasa tal que no se rebasen los límites especificados en el diseño del combustible ni los límites de la base de diseño de la barrera de presión del refrigerante del reactor.

6.34. Deberá contarse con elementos de interconexión y aislamiento y otros dispositivos de diseño adecuados (como aparatos de detección de fugas) para cumplir con suficiente fiabilidad los requisitos del párr. 6.33, en caso de fallo único y de interrupción del suministro de energía del exterior al emplazamiento, e incorporarse criterios adecuados de redundancia, diversidad e independencia.

### **Refrigeración de emergencia del núcleo**

6.35. En caso de accidente con pérdida de refrigerante deberá poder refrigerarse el núcleo para reducir al mínimo el deterioro del combustible y limitar la fuga de productos de fisión del combustible. La refrigeración prevista deberá asegurar que:

- 1) los parámetros limitadores de la integridad de la vaina o del combustible (como la temperatura) no excedan de los valores admisibles para accidentes base de diseño (en los diseños de reactores en que ello proceda);
- 2) las posibles reacciones químicas queden limitadas a un nivel admisible;
- 3) las alteraciones del combustible y de las estructuras internas no reduzcan notablemente la eficacia de los medios de refrigeración de emergencia del núcleo;
- y
- 4) la refrigeración del núcleo quede garantizada durante un intervalo de tiempo suficiente.

6.36. Se deberá disponer de elementos (como dispositivos de detección de fugas, interconexiones adecuadas y sistemas de aislamiento), así como de la adecuada redundancia y diversidad de los componentes, para cumplir estos requisitos con suficiente fiabilidad respecto de cada SIP, en el supuesto de un fallo único.

6.37. Deberá prestarse la atención debida a la ampliación de la capacidad de eliminación del calor del núcleo tras un accidente grave.

#### **Inspección y ensayo del sistema de refrigeración de emergencia del núcleo**

6.38. El sistema de refrigeración de emergencia del núcleo se deberá diseñar de modo que sea posible realizar las oportunas inspecciones periódicas de los componentes importantes, y los ensayos periódicos adecuados para comprobar:

- 1) la integridad de la estructura y la estanqueidad de sus componentes;
- 2) la seguridad de funcionamiento y comportamiento en servicio de los componentes activos del sistema en condiciones de funcionamiento normal, en la medida en que sea posible; y
- 3) la seguridad de funcionamiento del conjunto del sistema en los estados de la central especificados en la base de diseño, en la medida de lo posible.

#### **Transmisión térmica a un sumidero final de calor**

6.39. Se proveerán sistemas para la transmisión del calor residual de las estructuras, sistemas y componentes de importancia para la seguridad a un sumidero final de calor. Esta función se deberá desempeñar con niveles de fiabilidad muy altos, en las situaciones operacionales y de accidente base de diseño. Todos los sistemas que contribuyan a la transmisión de calor (sea mediante transporte térmico, sea proporcionando energía, o suministrando fluidos a los sistemas de transporte del calor) deberán diseñarse según la importancia de su respectiva contribución a la función total de transmisión de calor.

6.40. La fiabilidad de los sistemas se conseguirá mediante la elección adecuada de medidas, incluidas el uso de componentes probados, la redundancia, la diversidad, la separación física, las interconexiones y el aislamiento.

6.41. Deberán tenerse en cuenta los fenómenos naturales y los sucesos imputables al hombre en el diseño de los sistemas, en la posible elección de diversidad en los sumideros finales de calor, y en los sistemas de almacenamiento desde los que se suministran fluidos transportadores de calor.

6.42. Deberá prestarse la debida atención a la ampliación de la capacidad de transmisión del calor residual del núcleo a un sumidero final de calor, de forma que se asegure que, en caso de accidente grave, puedan mantenerse temperaturas aceptables en las estructuras, sistemas y componentes de importancia para la función de seguridad del sistema de confinamiento de los materiales radiactivos.

## SISTEMA DE CONTENCIÓN

### **Diseño del sistema de contención**

6.43. Se deberá establecer un sistema de contención con el fin de asegurar que cualquier liberación de materiales radiactivos al entorno en un accidente base de diseño esté por debajo de los límites prescritos. Dicho sistema puede incluir, según los requisitos de diseño: estructuras a prueba de fugas; sistemas conexos para el control de presiones y temperaturas; y elementos para el aislamiento, gestión y eliminación de productos de fisión, hidrógeno, oxígeno, y otras sustancias que podrían liberarse en la atmósfera de la contención.

6.44. En el diseño del sistema de contención deberán tenerse en cuenta todos los accidentes base de diseño especificados. También deberá prestarse atención a la inclusión de elementos para la atenuación de las consecuencias de determinados accidentes graves con el fin de limitar la liberación de material radiactivo al entorno.

### **Resistencia estructural del sistema de contención**

6.45. La resistencia estructural del sistema de contención, incluidas las aberturas y penetraciones de acceso y las válvulas de aislamiento, deberá calcularse con los márgenes de seguridad suficientes, sobre la base de temperaturas y presiones internas (superior e inferior) y de efectos dinámicos tales como los producidos por el impacto de proyectiles y por fuerzas de reacción resultantes de accidentes base de diseño. Deberán tenerse también en cuenta los efectos de otras fuentes potenciales de



energía, incluidas las posibles reacciones químicas y radiolíticas. En el cálculo de la necesaria resistencia estructural de la contención se deberán tener en cuenta los fenómenos naturales y los sucesos imputables al hombre, y convendrá también considerar la adopción de medidas para vigilar el estado del sistema de contención y de sus elementos conexos.

6.46. Se deberá considerar la adopción de medidas para mantener la integridad del sistema de contención en caso de accidente grave. En especial, se tendrán en cuenta los efectos de cualquier combustión previsible de gases inflamables.

#### **Posibilidad de llevar a cabo ensayos manométricos del sistema de contención**

6.47. La estructura de la contención deberá diseñarse y construirse de modo que sea posible realizar un ensayo manométrico a una presión determinada para comprobar su integridad estructural, antes de la entrada en servicio de la central y a lo largo de su vida útil.

#### **Fugas del sistema de contención**

6.48. El sistema de contención deberá diseñarse de modo que no se rebase la tasa máxima de fuga prescrita en accidentes base de diseño. El confinamiento primario de la presión puede estar parcial o totalmente rodeado por un confinamiento secundario para recoger y liberar en forma controlada, o almacenar, los materiales que puedan fugarse del confinamiento primario en caso de accidente base de diseño.

6.49. La estructura de la contención, así como el equipo y los componentes importantes para la estanqueidad del sistema de contención, se deberán diseñar y construir de modo que la tasa de fuga pueda comprobarse a la presión de diseño después de instaladas todas las penetraciones. Deberá ser posible volver a determinar la tasa de fuga del sistema de contención a intervalos periódicos durante la vida útil del reactor, bien a la presión de diseño de la contención, o bien a presiones reducidas que permitan calcular la tasa de fuga a la presión de diseño de la contención.

6.50. Deberá prestarse la atención debida a la capacidad para controlar cualquier fuga de material radiactivo procedente del sistema de contención en caso de accidente grave.

#### **Penetraciones del sistema de contención**

6.51. Deberá reducirse prácticamente al mínimo el número de penetraciones a través de la contención.

6.52. Todas las penetraciones a través de la contención deberán cumplir los mismos requisitos de diseño que la propia estructura de contención. Dichas penetraciones deberán protegerse contra las fuerzas de reacción procedentes del movimiento de las tuberías o de cargas accidentales como las producidas por proyectiles, chorros y latiguo de las tuberías.

6.53. Si con las penetraciones se utilizan juntas herméticas flexibles (como juntas elásticas o penetraciones de cables eléctricos) o fuelles de dilatación, estos elementos deberán diseñarse de modo que sea posible llevar a cabo ensayos de fugas a la presión de diseño de la contención, independientemente de la determinación de la tasa total de fuga de la contención, con el fin de demostrar su integridad durante la vida útil de la central.

6.54. Deberá tenerse debidamente en cuenta la capacidad de las penetraciones para mantenerse en funcionamiento en caso de accidente grave.

#### **Aislamiento del sistema de contención**

6.55. Todo conducto que penetre en la contención como parte de la barrera de presión del refrigerante del reactor o que esté conectado directamente con la atmósfera de la contención, deberá ser automática y fiablemente obturable en caso de accidente base de diseño en que la estanqueidad a las fugas de la contención sea esencial para evitar una liberación de radiactividad al medio ambiente que supere los límites prescritos. Esos conductos deberán ir provistos como mínimo de dos válvulas apropiadas de aislamiento de la contención instaladas en serie (normalmente una en el exterior y otra en el interior de la contención, aunque pueden admitirse otros tipos de instalación según sea el diseño), que puedan ser accionadas independientemente mediante un sistema fiable. Las válvulas de aislamiento deberán situarse lo más cerca posible de la contención. El aislamiento de la contención deberá estar concebido atendiendo al criterio del supuesto de un fallo único. Si la aplicación de este criterio reduce la fiabilidad de un sistema de seguridad que penetre en la contención, pueden utilizarse otros métodos de aislamiento.

6.56. Todo conducto que penetre en la contención primaria del reactor y no forme parte de la barrera de presión del refrigerante ni esté conectado directamente con la atmósfera de la contención deberá tener, como mínimo, una válvula adecuada de aislamiento de la contención. Esta válvula estará situada en el exterior de la contención y lo más cerca posible de ella.

6.57. Deberá tenerse debidamente en cuenta la capacidad de los dispositivos de aislamiento para seguir funcionando en caso de accidente grave.

### **Esclusas del sistema de contención**

6.58. El acceso del personal a la contención se realizará mediante esclusas dotadas de puertas de enclavamiento para asegurar que, como mínimo, una de las puertas permanezca cerrada durante el funcionamiento del reactor y en caso de accidente base de diseño. Cuando se adopten medidas para la entrada de personal para realizar actividades de vigilancia durante ciertas operaciones de baja potencia, deberán especificarse en el diseño disposiciones que garanticen la seguridad del personal en dichas operaciones. Estos requisitos se aplicarán también a las esclusas, donde las hubiere.

6.59 Deberá tenerse debidamente en cuenta la capacidad de las esclusas del sistema de contención para seguir funcionando en caso de accidente grave.

### **Estructuras internas del sistema de contención**

6.60. En el diseño se deberán establecer amplias vías de paso entre compartimentos separados dentro de la contención. Las secciones transversales de los conductos entre compartimentos se deberán dimensionar de modo que las diferencias de presión que tengan lugar durante la igualación manométrica en condiciones de accidente base de diseño no dañen las estructuras que resisten la presión ni otros sistemas de importancia para limitar los efectos de los accidentes base de diseño.

6.61. Deberá tenerse debidamente en cuenta la capacidad de las estructuras internas para resistir los efectos de un accidente grave.

### **Eliminación del calor del sistema de contención**

6.62. Deberá asegurarse la capacidad de eliminar el calor de la contención del reactor. La función de seguridad de dichos medios consistirá en reducir la presión y la temperatura de la contención después de fugas accidentales de fluidos de alta energía, y en mantenerlas dentro de valores bajos admisibles, en caso de accidente base de diseño. El sistema que lleve a cabo la función de eliminar el calor de la contención deberá tener la redundancia y fiabilidad adecuadas para desempeñar esta función en el supuesto de un fallo único.

6.63. Deberá tenerse debidamente en cuenta la capacidad para eliminar el calor de la contención del reactor en caso de accidente grave.

### **Control y limpieza de la atmósfera del sistema de contención**

6.64. Deberá disponerse, cuando sea necesario, de sistemas para controlar los productos de fisión, el hidrógeno, el oxígeno y otras sustancias que puedan liberarse en el interior de la contención del reactor con objeto de:

- 1) reducir la cantidad de productos de fisión que puedan liberarse en el medio ambiente en caso de accidente base de diseño; y
- 2) controlar la concentración de hidrógeno, oxígeno u otras sustancias en la atmósfera de contención en caso de accidente base de diseño, con objeto de evitar explosiones o deflagraciones que pongan en peligro la integridad de la contención.

6.65. Los sistemas de limpieza de la atmósfera de la contención deberán tener una redundancia apropiada en componentes y características de modo que el grupo de seguridad desempeñe adecuadamente sus funciones de seguridad en el supuesto de un fallo único.

6.66. Deberá prestarse la debida atención al control de productos de fisión, hidrógeno y otras sustancias que puedan producirse o liberarse en caso de accidente grave.

### **Cubiertas y revestimientos**

6.67. Las cubiertas y revestimientos de los componentes y estructuras dentro del sistema de contención se deberán escoger cuidadosamente y especificarse sus métodos de aplicación para que desempeñen sus funciones de seguridad y con el fin de reducir a un mínimo la interferencia con otras funciones de seguridad en caso de que se deterioren tales cubiertas y revestimientos.

## **INSTRUMENTACIÓN Y CONTROL**

### **Requisitos generales para los sistemas de instrumentación y control de importancia para la seguridad**

6.68. Se deberá disponer de instrumentación para vigilar las variables y los sistemas de la central en los respectivos intervalos correspondientes a funcionamiento normal, incidentes operacionales previstos, accidentes base de diseño y accidentes graves, con objeto de tener la certeza de conseguir información adecuada sobre las condiciones de la central. Asimismo se deberá disponer de instrumentos para medir todas las principales variables que pueden influir en el proceso de fisión, en la integridad del

núcleo del reactor, en los sistemas de refrigeración de éste y en el sistema de contención, así como para obtener cualquier información sobre la central necesaria para su funcionamiento en condiciones de seguridad y fiabilidad. Se adoptarán disposiciones para el registro automático de las mediciones de cualquier parámetro derivado de importancia para la seguridad, como por ejemplo, el margen de subenfriamiento del agua de refrigeración. La instrumentación deberá ser apta para el medio ambiente propio de los estados de la central que interesen y ser adecuada para medir los parámetros de la central y, por tanto, para clasificar los sucesos a los efectos de la respuesta en caso de emergencia.

6.69. Se deberá disponer también de instrumentos y equipo de registro con el fin de obtener la información básica necesaria para vigilar el curso de accidentes base de diseño y el estado del equipo esencial, así como para prever, cuando ello sea necesario para la seguridad, la ubicación y las cantidades de materiales radiactivos que pudieran escapar de los lugares que se les hubiera asignado en el diseño. La instrumentación y el equipo de registro deberán ser adecuados para proporcionar información que, en la medida de lo posible, permita determinar la condición de la central durante accidentes graves y para la adopción de decisiones durante la gestión de accidentes.

6.70. Se deberá disponer de controles adecuados y fiables para mantener las variables a las que se hace referencia en el párr. 6.68 dentro de límites operacionales especificados.

### **Sala de control**

6.71. Deberá existir una sala de control desde la que pueda hacerse funcionar la central nuclear en condiciones de seguridad en todas las situaciones operacionales, y desde la que puedan tomarse medidas para mantener o restablecer dichas condiciones de seguridad después del inicio de un incidente operacional previsto, de accidentes base de diseño y de accidentes graves. Se adoptarán las medidas adecuadas y se proporcionará información suficiente para proteger a los ocupantes de la sala de control contra los riesgos resultantes, tales como niveles de radiación excesivos como resultado de una condición de accidente o la liberación de material radiactivo o de gases tóxicos o explosivos, que pudieran obstaculizar las medidas necesarias que tome el operador.

6.72. Deberá prestarse especial atención a la tarea de determinar los sucesos que tengan lugar tanto en la sala de control como fuera de ella, que puedan suponer una amenaza directa para su funcionamiento continuo, y en el diseño se deberá prever medidas razonablemente aplicables para reducir al mínimo los efectos de dichos sucesos.

6.73. La disposición de los instrumentos y las modalidades de presentación de la información deberán dar al personal de explotación una idea global adecuada del estado y funcionamiento de la central nuclear. En el diseño de la sala de control deberán tenerse en cuenta los factores ergonómicos.

6.74. Se deberán instalar dispositivos que indiquen de modo eficaz, mediante señales visuales y, si corresponde, también auditivas, toda alteración de los estados operacionales y de los procesos que pueda repercutir en la seguridad.

### **Sala complementaria de control**

6.75. Se deberá disponer de instrumentos y equipo de control suficientes, preferiblemente en un punto único (sala complementaria de control) que esté aislado física y eléctricamente de la sala de control, de modo que se pueda parar el reactor y mantenerlo en ese estado, eliminar el calor residual y realizar la lectura de las variables esenciales de la central si no pueden realizarse desde la sala de control esas funciones fundamentales para la seguridad.

### **Uso de sistemas informáticos en sistemas de importancia para la seguridad**

6.76. Si el diseño se hace de tal modo que un sistema de importancia para la seguridad depende de la actuación fiable de un sistema informático, deberán establecerse normas y prácticas adecuadas para el desarrollo y verificación del equipo y los programas informáticos, que deberán aplicarse a lo largo de la vida útil del sistema, en especial el ciclo de desarrollo de los programas informáticos. Todo el proceso de desarrollo se hará con arreglo a un programa que asegure la calidad adecuada.

6.77. El nivel de fiabilidad necesario deberá estar en consonancia con la importancia del sistema para la seguridad. El nivel necesario de fiabilidad se logrará por medio de una amplia estrategia que utilice diversos medios complementarios (incluido un régimen eficaz de análisis y ensayos) en cada fase del desarrollo del proceso, y una estrategia de validación para confirmar que se cumplen los requisitos especificados en el diseño.

6.78. En el análisis de seguridad para un sistema informático se especificará un grado de fiabilidad moderado para compensar la complejidad inherente de la tecnología y la consiguiente dificultad de los análisis.

### **Control automático**

6.79. Las diversas operaciones de seguridad deberán automatizarse de modo que no sea necesaria la acción del operador en un período justificado a partir del inicio de incidentes operacionales previstos o de accidentes base de diseño. Además, se facilitará al operador la información pertinente para que pueda vigilar las consecuencias de las operaciones automáticas.

### **Funciones del sistema de protección**

6.80. El sistema de protección se deberá diseñar de modo que:

- 1) inicie automáticamente el funcionamiento de sistemas adecuados, entre ellos, si es necesario, los sistemas de parada del reactor, para que no se rebasen los límites especificados de diseño como resultado de incidentes operacionales previstos;
- 2) detecte las condiciones de accidente base de diseño e inicie el funcionamiento de los sistemas necesarios para atenuar las consecuencias de tales accidentes en la base de diseño; y
- 3) pueda contrarrestar las acciones inseguras del sistema de control.

### **Fiabilidad y posibilidad de ensayo del sistema de protección**

6.81. El sistema de protección se deberá diseñar de modo que presente gran fiabilidad funcional y pueda someterse a ensayos periódicos en consonancia con las funciones de seguridad que ha de realizar. La redundancia y la independencia del sistema de protección incorporadas en el diseño deberán ser suficientes para garantizar, como mínimo, que:

- 1) Ningún fallo único provoque la pérdida de su función de protección; y
- 2) La retirada del servicio de cualquier componente o circuito no menoscabe la redundancia mínima necesaria, a menos que se pueda demostrar de otro modo la suficiente fiabilidad de funcionamiento del sistema de protección.

6.82. El sistema de protección se deberá diseñar de modo que los efectos que tengan sobre los circuitos redundantes el funcionamiento normal, los incidentes operacionales previstos y los accidentes base de diseño no causen la pérdida de su función, o bien se deberá demostrar que esa pérdida es aceptable por otras razones. Para impedir en la medida de lo posible la pérdida de la función de protección, se deberán utilizar técnicas adecuadas de diseño como la posibilidad de ensayo, incluida, cuando sea necesario, la posibilidad de autoverificación, el comportamiento seguro en caso de

fallo, la diversidad funcional y la diversidad de diseño de los componentes o de los principios de funcionamiento.

6.83. A menos que la fiabilidad pueda comprobarse por otros medios, el sistema de protección se deberá diseñar de modo que permita realizar ensayos periódicos de su funcionamiento durante la explotación del reactor, incluida la posibilidad de ensayar independientemente los diferentes circuitos para determinar los fallos y pérdidas de redundancia que puedan haber tenido lugar. El diseño deberá permitir que todos los aspectos de funcionalidad, desde el sensor hasta la señal de entrada para el mecanismo final, se puedan poner a prueba mientras estén en funcionamiento.

6.84. El diseño deberá ser tal que reduzca al mínimo la probabilidad de que las acciones del operador incidan negativamente en la eficacia del sistema de protección en condiciones de funcionamiento normal y de incidentes operacionales previstos, sin descartar las acciones apropiadas del operador en caso de accidente base de diseño.

#### **Uso de sistemas informáticos en los sistemas de protección**

6.85. Cuando se prevé utilizar un sistema informático en un sistema de protección, se implantarán los siguientes requisitos para complementar los de los párrs. 6.76 a 6.78:

- 1) se utilizarán la más alta calidad y las mejores prácticas para los equipos y programas informáticos;
- 2) todo el proceso de desarrollo, incluidas las actividades de control, ensayo y puesta en servicio de cambios de diseño, deberá estar sistemáticamente documentado y podrá someterse a revisión;
- 3) con el fin de confirmar la fiabilidad de los sistemas basados en computadoras, deberá llevarse a cabo una evaluación del sistema informático por personal experto independiente de los diseñadores y proveedores; y
- 4) cuando no pueda probarse la necesaria integridad del sistema con un alto nivel de fiabilidad o confianza, se adoptarán otras medidas para asegurar que se cumplen las funciones de protección.

#### **Separación de los sistemas de protección y control**

6.86. Se deberá impedir la interferencia entre el sistema de protección y los sistemas de control evitando su interconexión o mediante un adecuado aislamiento funcional. Si el sistema de protección y cualquiera de los sistemas de control utilizan señales comunes, deberá garantizarse la adecuada separación (por ejemplo, mediante disyuntores adecuados) y deberá demostrarse que se cumplen todos los requisitos de seguridad establecidos en los párrs. 6.80 a 6.85.



## CENTRO DE CONTROL DE EMERGENCIAS

6.87. Deberá establecerse en el emplazamiento un centro de control de emergencias, separado de la sala de control de la central, para que sirva como lugar de reunión del personal encargado de hacer frente a emergencias, el cual, en caso de haberlas, desempeñará allí sus funciones. En ese centro debería disponerse de información acerca de los parámetros importantes y de la situación radiológica de la central y de sus inmediaciones. La sala debería contar con medios de comunicación con la sala de control, con la sala complementaria de control, con otros puntos importantes de la central y con las organizaciones encargadas de hacer frente a las emergencias dentro o fuera del emplazamiento. Se adoptarán las medidas adecuadas para proteger durante un período razonablemente prolongado a los ocupantes contra los riesgos debidos a accidentes graves.

## SISTEMA ELÉCTRICO DE EMERGENCIA

6.88. Como consecuencia de ciertos SIP, diversos sistemas y componentes de importancia para la seguridad necesitarán un suministro de electricidad de emergencia. Se deberá asegurar que el sistema eléctrico de emergencia pueda suministrar la corriente necesaria en cualquier situación operacional, en un accidente base de diseño, o en caso de interrupción del suministro exterior de energía al emplazamiento. La necesidad de electricidad variará según el carácter del SIP, y la índole de la función de seguridad que deberá desempeñarse determinará la selección de los medios que hayan de utilizarse en cada caso, en lo que se refiere, por ejemplo, al número, disponibilidad, duración, capacidad y continuidad de estos medios.

6.89. Los distintos medios utilizados para suministrar corriente eléctrica de emergencia (tales como turbinas de agua, de vapor o de gas, motores diesel o baterías) deberán tener una fiabilidad y una configuración adecuadas a las necesidades de los sistemas de seguridad que se provean, y deberán desempeñar sus funciones en el supuesto de un fallo único. Deberá ser posible asimismo comprobar la capacidad funcional del suministro eléctrico de emergencia.

## SISTEMAS DE CONTROL Y TRATAMIENTO DE DESECHOS RADIATIVOS

6.90. Deberán establecerse sistemas adecuados para tratar los efluentes radiactivos líquidos y gaseosos con el fin de mantener las cantidades y las concentraciones de las descargas radiactivas dentro de los límites prescritos. Se aplicará el principio ALARA.

6.91. Deberán establecerse sistemas adecuados para la manipulación de desechos radiactivos y para el almacenamiento seguro de los mismos en el emplazamiento durante un período de tiempo que esté en consonancia con las vías de eliminación de que dispone el emplazamiento. El transporte de los desechos sólidos desde el emplazamiento se deberá realizar de acuerdo con las decisiones de las autoridades competentes.

### **Control de las liberaciones de líquidos radiactivos en el medio ambiente**

6.92. La central nuclear deberá contar con medios adecuados para controlar la liberación en el medio ambiente de materiales radiactivos en estado líquido de modo que se cumpla el principio ALARA y que se asegure que las emisiones y concentraciones se mantengan dentro de los límites prescritos.

### **Control de los materiales radiactivos en suspensión en el aire**

6.93. Se deberá instalar un sistema de ventilación con capacidad de filtración adecuada que:

- 1) evite la dispersión no permisible de sustancias radiactivas en suspensión en el aire dentro de la central nuclear;
- 2) reduzca la concentración de sustancias radiactivas en suspensión en el aire a niveles compatibles con los requisitos de acceso a la zona determinada;
- 3) mantenga el nivel de sustancias radiactivas en suspensión en el aire dentro de la central por debajo de los límites prescritos, aplicando el principio ALARA en condiciones de funcionamiento normal, incidentes operacionales previstos y accidentes base de diseño; y
- 4) ventile las salas que contengan gases inertes o nocivos sin perjudicar la capacidad de control de las descargas radiactivas.

### **Control de las liberaciones de material radiactivo gaseoso en el medio ambiente**

6.94. Deberá instalarse un sistema de ventilación con sistemas de filtración adecuados para controlar la liberación de sustancias radiactivas en suspensión en el aire al medio ambiente, y para asegurar que se cumpla el principio ALARA y los límites en él establecidos.

6.95. Los sistemas de filtros deberán ser suficientemente fiables y estar diseñados de modo que en las condiciones de funcionamiento previstas se obtengan los factores necesarios de retención. Los sistemas de filtros se diseñarán de modo que pueda comprobarse su eficacia.

## SISTEMAS DE MANIPULACIÓN Y ALMACENAMIENTO DEL COMBUSTIBLE

### **Manipulación y almacenamiento del combustible no irradiado**

6.96. Los sistemas de manipulación y almacenamiento de combustible no irradiado se deberán diseñar de modo que:

- 1) se evite por medios o procedimientos físicos la criticidad, dentro de un margen especificado, de preferencia mediante la utilización de configuraciones geométricamente seguras, incluso en estados de moderación óptima de la central;
- 2) sea posible realizar actividades de mantenimiento, inspecciones y ensayos periódicos adecuados de los componentes de importancia para la seguridad; y
- 3) se reduzca al mínimo la probabilidad de pérdida o deterioro del combustible.

### **Manipulación y almacenamiento del combustible irradiado**

6.97. Los sistemas de manipulación y almacenamiento del combustible irradiado se deberán diseñar de modo que:

- 1) se evite por medios o procedimientos físicos la criticidad, de preferencia mediante la utilización de configuraciones geométricamente seguras, incluso en estados de moderación óptima de la central;
- 2) sea posible la eliminación adecuada del calor en situaciones operacionales y de accidente base de diseño;
- 3) sea posible llevar a cabo inspecciones del combustible irradiado;
- 4) sea posible realizar inspecciones y ensayos periódicos adecuados de los componentes de importancia para la seguridad;
- 5) se evite la caída del combustible gastado durante el transporte;
- 6) se eviten esfuerzos inadmisibles en los elementos o conjuntos combustibles durante su manipulación;
- 7) se evite la caída accidental de objetos pesados tales como los cofres de combustible gastado, grúas u otros objetos que puedan causar daños en los elementos de los conjuntos combustibles;
- 8) sea posible el almacenamiento en condiciones de seguridad de elementos o conjuntos combustibles dañados, o que se sospeche que lo están;
- 9) se disponga de medios de protección radiológica adecuados;
- 10) se identifiquen adecuadamente los módulos individuales de combustible;
- 11) se controlen los niveles de absorbente soluble si se utilizan a efectos de seguridad en caso de criticidad;

- 12) se facilite el mantenimiento y la clausura de las instalaciones de manipulación y almacenamiento del combustible;
- 13) se facilite la descontaminación de las zonas y del equipo de manipulación y almacenamiento del combustible, cuando sea necesario; y
- 14) se asegure la aplicación de procedimientos de funcionamiento y contabilidad adecuados para evitar la pérdida de combustible.

6.98. En el caso de los reactores que empleen un sistema de piscina para el almacenamiento del combustible, en el diseño se deberá prever:

- 1) medios para controlar las condiciones químicas y la radiactividad de cualquier agua en la que se almacene o manipule combustible irradiado;
- 2) medios para vigilar y controlar el nivel de agua en la piscina de almacenamiento del combustible y detectar fugas; y
- 3) medios para evitar el vaciado de la piscina en caso de rotura de tuberías (es decir, medidas antisifón).

## PROTECCIÓN RADIOLÓGICA<sup>3</sup>

### Requisitos generales

6.99. La finalidad de la protección radiológica es impedir las exposiciones a la radiación que sean evitables y mantener las que sean inevitables en el valor más bajo que pueda alcanzarse razonablemente. Tal objetivo se deberá conseguir en la etapa de diseño mediante:

- 1) la adecuada disposición y blindaje de las estructuras, sistemas y componentes que contengan materiales radiactivos;
- 2) la debida atención al diseño de la central y del equipo de modo que se reduzca a un mínimo el número y la duración de las actividades humanas en las zonas expuestas a la radiación y la posibilidad de contaminación del personal del emplazamiento;
- 3) medidas para el tratamiento de materiales radiactivos, en la forma y condiciones adecuadas, bien sea para su eliminación, para su almacenamiento en el emplazamiento o para su eliminación del mismo; y
- 4) disposiciones para reducir la cantidad y la concentración de los materiales radiactivos producidos y dispersados en la central o liberados en el medio ambiente.

---

<sup>3</sup> Véanse otras orientaciones en la Ref. [6].

6.100. Deberá tenerse plenamente en cuenta el posible incremento en función del tiempo de los niveles de radiación en las zonas ocupadas por el personal, así como la necesidad de reducir al mínimo la generación de materiales radiactivos en forma de desechos.

### **Diseño de protección radiológica**

6.101. En el diseño y disposición de la central deberán adoptarse las medidas adecuadas para reducir al mínimo la exposición y contaminación resultantes de todas las fuentes. Tales medidas deberán incluir el adecuado diseño de las estructuras, sistemas y componentes, atendiendo a lo siguiente: minimización de la exposición durante las actividades de mantenimiento e inspección; blindaje contra la radiación directa y dispersa; ventilación y filtración para controlar las sustancias radiactivas en suspensión en el aire; limitación de la activación de los productos de corrosión mediante la adecuada especificación de los materiales; medios de vigilancia radiológica, control de los accesos a la central e instalaciones adecuadas de descontaminación.

6.102. El diseño de los blindajes deberá hacerse de modo que los niveles de radiación en las zonas de operación no rebasen los límites prescritos, y que se faciliten las actividades de mantenimiento e inspección de modo que se reduzca a un mínimo el nivel de exposición del personal encargado de las mismas. Se aplicará el principio ALARA.

6.103. La disposición y los procedimientos de la central deberán permitir el control del acceso a las zonas de radiación y a las de contaminación potencial, así como permitir minimizar la contaminación resultante del tránsito de materiales radiactivos y de personal en el interior de la central. La disposición de ésta deberá hacer posible que el funcionamiento, inspección, mantenimiento y sustitución de componentes, cuando sea necesario, se realicen eficazmente de modo que se reduzca a un mínimo la exposición a la radiación.

6.104. Deberán establecerse instalaciones adecuadas de descontaminación tanto del personal como del equipo, y de manipulación de todo desecho radiactivo procedente de las actividades de descontaminación.

### **Medios de vigilancia radiológica**

6.105. Se deberá disponer de equipo para asegurar una vigilancia radiológica adecuada en las situaciones operacionales, en accidentes base de diseño y, cuando sea posible, durante accidentes graves. Dicho equipo constará de los elementos siguientes:

## La publicación SSR-2/1 (Rev. 1) sustituye a la presente publicación.

- 1) Monitores de tasa de dosis estacionarios para medir la tasa local de dosis de radiación en lugares ocupados normalmente por personal de explotación y en los que los cambios de los niveles de radiación durante el funcionamiento normal o en incidentes operacionales previstos puedan ser tales que convenga limitar el acceso a los mismos durante ciertos intervalos de tiempo. Asimismo deberán instalarse monitores de tasa de dosis estacionarios para indicar el nivel general de radiación en lugares adecuados, en caso de accidentes base de diseño y, cuando sea posible, de accidentes graves. Estos instrumentos deberán transmitir suficiente información a la sala de control o a los puestos de control oportunos de modo que el personal de la central pueda iniciar medidas correctoras cuando sea necesario.
- 2) Monitores para medir la actividad de sustancias radiactivas presentes en la atmósfera de las zonas normalmente ocupadas por el personal y cuando se prevea que los niveles de actividad de las sustancias radiactivas en suspensión en el aire puedan exigir medidas de protección. Estos sistemas deberán transmitir señales a la sala de control, o a otros lugares apropiados, cuando se detecte una concentración elevada de radionucleidos.
- 3) Equipo estacionario e instalaciones de laboratorio para determinar de forma oportuna la concentración de determinados radionucleidos en sistemas de proceso en estado fluido, cuando sea necesario, y en muestras de gas y de líquido tomadas de sistemas de la central o del medio ambiente, en estados operacionales y en condiciones de accidente.
- 4) Equipo estacionario para la vigilancia de los efluentes, antes o durante su liberación en el medio ambiente.
- 5) Instrumentos para medir la contaminación radiactiva de superficies.
- 6) Instalaciones para vigilar las dosis y la contaminación del personal.

6.106. Además de la vigilancia radiológica dentro de la central, se deberán tomar también medidas para determinar las repercusiones radiológicas, si las hubiere, en las cercanías de la central, prestando especial atención a:

- 1) las vías de acceso de las sustancias radiactivas a la población humana, incluida la cadena alimentaria;
- 2) la repercusión radiológica, si la hubiere, en los ecosistemas locales;
- 3) la posible acumulación de materiales radiactivos en el medio ambiente; y
- 4) la posibilidad de que haya vías de descarga no autorizadas.

## Apéndice I

### SUCESOS INICIADORES POSTULADOS

I.1. En el presente apéndice se precisa la definición y aplicación del concepto de suceso iniciador postulado (SIP).

I.2. Un SIP se define como un suceso indicado en el diseño que origina incidentes operacionales previstos o condiciones de accidente. Esto significa que un SIP no es en sí mismo un accidente, sino el suceso que inicia una secuencia y origina una ocurrencia operacional, un accidente base de diseño o un accidente grave, según los fallos adicionales que puedan ocurrir. Como ejemplos podemos citar: fallos de equipo (incluida rotura de tuberías), errores humanos, sucesos imputables al hombre y sucesos naturales.

I.3. Un SIP puede ser de un tipo que tenga consecuencias leves, como el fallo de un componente redundante, o bien puede tener consecuencias graves, como el fallo de una tubería principal del sistema de refrigeración del reactor. Es un objetivo importante del diseño conseguir características de la central que garanticen que la mayoría de los SIP tengan consecuencias poco importantes o, incluso, insignificantes, y que, si el resto se traduce en condiciones de accidente, las consecuencias sean aceptables; o que, si se traduce en accidentes graves, las consecuencias estén limitadas por las características del diseño y la gestión de accidentes.

I.4. Ha de postularse una amplia gama de sucesos con el fin de tener la seguridad de que se han previsto todos los sucesos verosímiles de consecuencias graves potenciales y probabilidad significativa, y de que el diseño de la central puede responder a dichos sucesos. No existen criterios fijos para la selección de los SIP; más bien se trata de un proceso de iteración entre el diseño y el análisis, los criterios de ingeniería y la experiencia resultante del diseño y explotación de centrales nucleares anteriores. La exclusión de una determinada secuencia de sucesos exige justificación.

I.5. El número de SIP que se habrán de utilizar al establecer los requisitos de comportamiento de los elementos de importancia para la seguridad y al evaluar la seguridad global de la central ha de ser limitado para que la tarea sea factible, y esto se consigue circunscribiendo el análisis detallado a cierto número de secuencias representativas de sucesos<sup>4</sup>. Las secuencias representativas de sucesos permiten

---

<sup>4</sup> La expresión “secuencia de sucesos” se utiliza para designar la combinación de un SIP y las acciones consecutivas del operador, o las acciones consecutivas de los elementos de importancia para la seguridad.

determinar los casos envolventes y ofrecen la base para el establecimiento de límites numéricos de diseño para las estructuras, sistemas y componentes de importancia para la seguridad.

I.6. Algunos SIP pueden especificarse de forma determinista, a partir de diferentes factores, como la experiencia resultante de centrales anteriores, los requisitos particulares prescritos por los órganos nacionales que conceden las licencias, o tal vez la magnitud de las consecuencias potenciales. Otros SIP pueden especificarse por métodos sistemáticos, como un análisis probabilista, porque haya características particulares del diseño, de la ubicación de la central o de la experiencia de explotación que permitan cuantificar sus características en forma probabilista.

## TIPOS DE SIP

### **Sucesos internos**

#### *Fallos del equipo*

I.7. Es posible que los sucesos iniciadores sean fallos determinados del equipo que puedan afectar directa o indirectamente a la seguridad de la central. La lista de estos sucesos ha de ser una representación adecuada de todos los fallos previsibles de los sistemas y componentes de la central.

I.8. Los tipos de fallo que deben considerarse dependen de la naturaleza del sistema o componente en cuestión. En el sentido más amplio, un fallo es, bien la pérdida de la capacidad del sistema o componente para cumplir su función, o bien la realización de una función no deseable. Por ejemplo, el fallo de una tubería podría ser una fuga, una rotura o el bloqueo de una vía de flujo. En el caso de un componente activo, por ejemplo una válvula, el fallo podría consistir en que ésta no se abra o no se cierre cuando haga falta, en que se abra o se cierre cuando no haga falta, en que se abra o se cierre parcialmente, o en que se abra o se cierre a la velocidad indebida. En el caso de un dispositivo tal como el transcriptor de un instrumento, el fallo podría revestir la forma de un error situado fuera de la banda de errores permitida, la ausencia de señales de salida, señales de salida máximas constantes, señales de salida erráticas, o una combinación de esos fallos.

I.9. Con el uso cada vez más extendido de sistemas informáticos para funciones de seguridad y funciones de importancia crítica para la seguridad, un fallo del equipo informático o un programa informático incorrecto pueden requerir medidas de control importantes, y es preciso tener en cuenta esa posibilidad.



### *Error humano*

I.10. En muchos casos las consecuencias de los errores humanos serán similares a las de fallos de componentes. Los errores humanos pueden variar desde la ejecución defectuosa o incompleta de operaciones de mantenimiento hasta la fijación incorrecta de los límites del equipo de control o la omisión de acciones o la realización de acciones incorrectas por parte de los operadores (errores de comisión y errores de omisión).

### *Otros sucesos internos*

I.11. Los incendios, explosiones e inundaciones de origen interno pueden tener una influencia importante en las condiciones de seguridad de la central, y normalmente se incluyen en la lista de SIP.

### **Sucesos externos**

I.12. En el Código sobre la seguridad de las centrales nucleares: Emplazamiento, Colección Seguridad N° 50-C-S (Rev. 1) [5], y en las Guías de seguridad correspondientes, se presentan ejemplos de sucesos externos y de la determinación de los datos pertinentes para la base de diseño. Dichos sucesos precisan que en el diseño de la central se incluyan factores de cargas vibratorias adicionales, de impacto y de impulso.

I.13. Si puede inferirse que la probabilidad de fallo de una estructura, sistema o componente de importancia para la seguridad a causa de sucesos externos naturales o imputables al hombre será suficientemente baja gracias al diseño y construcción adecuados, no será necesario incluir en la base de diseño de la central los fallos provocados por dicho suceso.

### **Combinación de sucesos**

I.14. Al combinar sucesos individuales, en el análisis de accidentes deberá procurarse qué combinación determinada se sustente en una base racional. La combinación aleatoria de sucesos puede representar un suceso extremadamente improbable, que en el análisis probabilista de seguridad debería demostrarse que es lo bastante inverosímil como para desecharlo, y no admitirlo como un accidente postulado. En el análisis probabilista de la seguridad, se adoptará un criterio que utilice los mejores métodos analíticos aproximativos en caso de accidentes graves, mientras que en el enfoque analítico de accidentes previstos, con una probabilidad relativamente más alta de ocurrir, se utilizarán criterios prudentes.

I.15. Al determinar los sucesos que es preciso combinar, es útil considerar tres periodos:

- 1) un período largo, anterior al suceso que se considere en particular;
- 2) un período corto, que incluya el suceso y sus efectos a corto plazo; y
- 3) el período de recuperación posterior al suceso.

I.16. Cabe suponer que un suceso que ocurre durante el primero de los períodos indicados anteriormente ha sido corregido antes de que ocurra otro suceso, si se han incorporado en el diseño de la central disposiciones apropiadas para su detección y si el tiempo necesario para aplicar la medida correctora es breve. En tales casos no es necesario considerar las combinaciones de dichos sucesos.

I.17. En cuanto al segundo período de los citados (cuya duración suele ser de horas), es posible que las probabilidades previstas de que ocurra cada suceso en particular sean tales que se considere inverosímil una combinación aleatoria de ellas.

I.18. En cuanto al período de recuperación posterior al suceso (con una duración de días o mayor) puede ser necesario tener en cuenta otros sucesos, según lo que dure el período de recuperación y según la probabilidad prevista de los sucesos. Para el período de recuperación puede ser realista admitir que la gravedad de un suceso que ha de considerarse en una combinación no es tan grande como cabría suponer para el mismo tipo de suceso considerado en un intervalo de tiempo correspondiente a toda la vida útil de la central. Por ejemplo, si en el período de recuperación tras un accidente con pérdida de refrigerante es necesario considerar una combinación aleatoria con un terremoto, cabe suponer que la gravedad sería menor que la gravedad del terremoto considerado en la base de diseño de la central.

## Apéndice II

### REDUNDANCIA, DIVERSIDAD E INDEPENDENCIA

II.1. En el presente apéndice se exponen algunas medidas de diseño que pueden utilizarse, si es necesario en combinación, para lograr y mantener la fiabilidad necesaria según la importancia de las funciones de seguridad que se han de desempeñar dentro de los escalones pertinentes de defensa en profundidad.

II.2. Aunque no pueden establecerse objetivos cuantitativos universales para los requisitos individuales de fiabilidad de cada nivel de defensa en profundidad, debería prestarse la mayor atención al primer nivel. Esto también está en consonancia con el objetivo de la entidad explotadora que debería ser la máxima disponibilidad de la central para la producción de energía.

II.3. Como orientación, o para su uso como criterio de aceptación convenido con el órgano regulador, pueden establecerse límites máximos de no disponibilidad para determinados sistemas de seguridad a fin de garantizar la fiabilidad necesaria con respecto al cumplimiento de las funciones de seguridad.

#### FALLOS DEBIDOS A CAUSA COMÚN

II.4. El fallo de ciertos dispositivos o componentes en la ejecución de sus funciones puede ocurrir como resultado de un suceso o causa de carácter específico. Dichos fallos pueden afectar simultáneamente a algunos elementos diferentes de importancia para la seguridad. El suceso o causa puede ser una deficiencia en el diseño, un defecto de fabricación, un error de funcionamiento o de mantenimiento, un fenómeno natural, un suceso imputable al hombre, o un efecto fortuito de repercusiones múltiples resultantes de cualquier otra operación o fallo en la central.

II.5. Los fallos debidos a causa común pueden ocurrir también cuando algunos componentes del mismo tipo fallan al mismo tiempo. Esto puede deberse a razones tales como alteración de las condiciones ambientales, saturación de señales, errores repetidos de mantenimiento o deficiencias en el diseño.

II.6. Siempre que sea posible, en el diseño se adoptarán las medidas adecuadas para reducir al mínimo los efectos de fallos debidos a causa común, como la aplicación de criterios de redundancia, diversidad e independencia.

## REDUNDANCIA

II.7. La redundancia, es decir, el uso de conjuntos de equipo en número mayor que el mínimo necesario para realizar una función determinada de seguridad, es un valioso principio de diseño para lograr una alta fiabilidad en sistemas de importancia para la seguridad y satisfacer el criterio de fallo único en el caso de los sistemas de seguridad. La redundancia permite soportar el fallo o la no disponibilidad de un conjunto de equipo sin pérdida de la función. Por ejemplo, se pueden prever tres o cuatro bombas para una función determinada, aunque dos de ellas basten para realizar esa función. Para los fines de la redundancia se pueden emplear componentes idénticos o diversos.

## DIVERSIDAD

II.8. La fiabilidad de algunos sistemas puede acrecentarse aplicando el principio de la diversidad para reducir la posibilidad de ciertos fallos debidos a causa común.

II.9. La diversidad se aplica a los sistemas o componentes redundantes que realizan la misma función de seguridad introduciendo en ellos características diferentes. Estas características pueden ser, por ejemplo, principios diferentes de funcionamiento, variables físicas diferentes, condiciones diferentes de funcionamiento o la producción por fabricantes diferentes.

II.10. Si se recurre a la diversidad, deberá tenerse cuidado de garantizar que toda medida de diversidad adoptada logre realmente el aumento deseado de la fiabilidad en el diseño, una vez ejecutado. Por ejemplo, para reducir la posibilidad de fallos debidos a causa común, el autor del diseño deberá examinar las medidas de diversidad aplicadas para detectar rasgos comunes en los materiales, componentes y procesos de fabricación, o sutiles analogías en los principios de funcionamiento o en los dispositivos auxiliares comunes. Si se utilizan componentes o sistemas diversos, debería haber una garantía razonable de que dichas adiciones suponen un beneficio general, teniendo en cuenta desventajas como la complicación adicional en los procedimientos de funcionamiento, mantenimiento y ensayo o el consiguiente uso de equipo de fiabilidad inferior.

## INDEPENDENCIA

II.11. La fiabilidad de los sistemas puede mejorarse aplicando los siguientes principios de independencia en el diseño:

## La publicación SSR-2/1 (Rev. 1) sustituye a la presente publicación.

- mantener la independencia entre los componentes de sistemas redundantes;
- mantener la independencia de los componentes de los sistemas y los efectos de los SIP, de modo que, por ejemplo, un SIP no cause el fallo o la pérdida de efectividad de un sistema de seguridad o una función de seguridad que se requiera para atenuar las consecuencias de ese suceso;
- mantener la independencia apropiada entre los sistemas o componentes de diferentes clases de seguridad; y
- mantener la independencia entre los elementos que sean de importancia para la seguridad y los que no lo sean.

II.12. La independencia en el diseño de los sistemas se consigue recurriendo al aislamiento funcional y a la separación física:

### 1) *Aislamiento funcional*

El aislamiento funcional se utilizará para reducir la probabilidad de una interacción perjudicial entre el equipo y los componentes de sistemas redundantes o conexos debida al funcionamiento normal o anormal o al fallo de cualquier componente de los sistemas.

### 2) *Separación física y disposición de los componentes de la central*

En la disposición de los sistemas y el diseño se deberá tener en cuenta la separación física para lograr una mayor certeza de que se conseguirá la independencia, particularmente en relación con ciertos fallos debidos a causa común.

La separación física incluye:

- separación por geometría (distancia u orientación);
- separación mediante barreras; o
- separación mediante una combinación de ambos tipos de medidas.

La elección de los medios de separación dependerá de los SIP considerados en la base de diseño, por ejemplo, efectos de incendios, explosiones de naturaleza química, impactos de aeronaves, impactos de proyectiles, inundaciones, condiciones extremas de temperatura o de humedad, según corresponda.

II.13. En una central hay ciertas zonas que tienden a ser centros naturales de convergencia de equipo o cableado de distintos grados de importancia para la seguridad. Tales centros pueden ser: penetraciones en la contención, centros de control de motores, cámaras de tendido de cables, salas de equipo, salas de control y

La publicación SSR-2/1 (Rev. 1) sustituye a la presente publicación.

computadoras empleadas para los procesos de la central. Deberán adoptarse, en la medida de lo posible, disposiciones apropiadas para evitar en dichas zonas fallos debidos a causa común.

## REFERENCIAS

- [1] ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA, Seguridad de las instalaciones nucleares, Colección Seguridad N° 110, OIEA, Viena (1993).
- [2] GRUPO INTERNACIONAL ASESOR EN SEGURIDAD NUCLEAR, La defensa en profundidad en seguridad nuclear, INSAG-10, OIEA, Viena (1996).
- [3] GRUPO INTERNACIONAL ASESOR EN SEGURIDAD NUCLEAR, Principios básicos de seguridad para centrales nucleares, 75-INSAG-3 Rev.1, INSAG-12, OIEA, Viena (1999).
- [4] ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA, Garantía de calidad para la seguridad en las centrales nucleares y otras instalaciones nucleares, Código y Guías de seguridad Q1 a Q14, Colección Seguridad N° 50-C/SG-Q, OIEA, Viena (1996).
- [5] ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA, Código sobre la seguridad de las centrales nucleares: Emplazamiento, Colección Seguridad N° 50-C-S (Rev. 1), OIEA, Viena (1988).
- [6] AGENCIA PARA LA ENERGÍA NUCLEAR DE LA ORGANIZACIÓN DE COOPERACIÓN Y DESARROLLO ECONÓMICOS, ORGANISMO INTERNACIONAL DE ENERGÍA ATÓMICA, ORGANIZACIÓN DE LAS NACIONES UNIDAS PARA LA AGRICULTURA Y LA ALIMENTACIÓN, ORGANIZACIÓN INTERNACIONAL DEL TRABAJO, ORGANIZACIÓN MUNDIAL DE LA SALUD, ORGANIZACIÓN PANAMERICANA DE LA SALUD, Normas básicas internacionales de seguridad para la protección contra la radiación ionizante y para la seguridad de las fuentes de radiación, Colección Seguridad N° 115, OIEA, Viena (1996).

## Anexo

### **FUNCIONES DE SEGURIDAD PARA REACTORES DE AGUA EN EBULLICIÓN, REACTORES DE AGUA A PRESIÓN Y REACTORES DE TUBOS DE PRESIÓN**

A-1. El presente anexo ofrece un ejemplo de una subdivisión detallada de las tres funciones fundamentales de seguridad definidas en el párr. 4.6.

A-2. Dichas funciones de seguridad incluyen las necesarias para evitar condiciones de accidente, así como para atenuar sus consecuencias. Pueden cumplirse, según proceda, haciendo uso de las estructuras, los sistemas o los componentes destinados al funcionamiento normal, de los destinados a evitar que los incidentes operacionales previstos originen condiciones de accidente, o de los destinados a atenuar las consecuencias de condiciones de accidente.

A-3. Un estudio de los diversos diseños de reactores pone de manifiesto que los actuales requisitos del diseño de seguridad pueden cumplirse incorporando estructuras, sistemas o componentes que desempeñen las siguientes funciones de seguridad:

- 1) evitar transitorios de reactividad inadmisibles;
- 2) mantener el reactor parado en condiciones de seguridad, una vez realizadas todas las operaciones de parada;
- 3) parar el reactor cuando sea necesario, para evitar que incidentes operacionales previstos originen accidentes base de diseño, y para atenuar las consecuencias de dichos accidentes;
- 4) mantener una cantidad suficiente de refrigerante del reactor para refrigerar el núcleo antes y después de condiciones de accidente no relacionadas con el fallo de la barrera de presión del refrigerante del reactor;
- 5) mantener una cantidad suficiente de refrigerante del reactor para refrigerar el núcleo en todos los casos de SIP considerados en la base de diseño, y después de ellos;
- 6) eliminar el calor del núcleo<sup>1</sup> tras un fallo de la barrera de presión del refrigerante del reactor a fin de limitar el deterioro del combustible;

---

<sup>1</sup> Esta función de seguridad se aplica a la primera etapa de accionamiento del (los) sistema(s) de eliminación del calor. La(s) siguiente(s) etapa(s) está(n) incluida(s) en la función de seguridad (8).



## La publicación SSR-2/1 (Rev. 1) sustituye a la presente publicación.

- 7) eliminar el calor residual (véase la nota 1) en los estados operacionales y las condiciones de accidente en que convenga, manteniendo intacta la barrera de presión del refrigerante del reactor;
- 8) transferir calor procedente de otros sistemas de seguridad al sumidero final de calor<sup>2</sup>;
- 9) garantizar los servicios necesarios (suministros de energía eléctrica, neumática, hidráulica, lubricación) como contribución al sistema de seguridad;
- 10) mantener una integridad aceptable de las vainas del combustible en el núcleo del reactor;
- 11) mantener la integridad de la barrera de presión del refrigerante del reactor;
- 12) limitar la liberación de material radiactivo procedente de la contención del reactor, en condiciones de accidente y después de ellas;
- 13) limitar la exposición a la radiación del público y del personal del emplazamiento en accidentes base de diseño y en determinados accidentes graves que liberan materiales radiactivos procedentes de fuentes situadas fuera de la contención del reactor, y después de ellos;
- 14) limitar la descarga o la liberación de desechos radiactivos y sustancias radiactivas en suspensión en el aire, a valores inferiores a los prescritos en todos los estados operacionales;
- 15) mantener el control de las condiciones ambientales dentro de la central para el funcionamiento de los sistemas de seguridad y para que el personal necesario pueda llevar a cabo operaciones de importancia para la seguridad;
- 16) controlar las liberaciones de material radiactivo procedente del combustible irradiado, transportado o almacenado fuera del sistema de refrigeración del reactor, pero dentro del emplazamiento, en todos los estados operacionales;
- 17) eliminar el calor de desintegración procedente del combustible irradiado almacenado fuera del sistema de refrigeración del reactor, pero dentro del emplazamiento;
- 18) mantener la subcriticidad suficiente del combustible almacenado fuera del sistema de refrigeración del reactor, pero dentro del emplazamiento;
- 19) evitar o limitar las consecuencias del fallo de una estructura, sistema o componente cuando dicho fallo pueda perjudicar una función de seguridad.

A-4. Esta lista de funciones de seguridad puede servir de base para determinar si una estructura, sistema o componente lleva a cabo a una o más funciones de seguridad o contribuye a ellas, así como para asignar un nivel adecuado de importancia a estructuras, sistemas o componentes de seguridad que contribuyen a las diversas funciones de seguridad.

---

<sup>2</sup> Ésta es una función de apoyo para otros sistemas de seguridad cuando éstos deben llevar a cabo sus funciones de seguridad.

## GLOSARIO

**aislamiento funcional** (*functional isolation*). Medidas para evitar que la modalidad de funcionamiento o el fallo de un circuito o sistema influyan en otro.

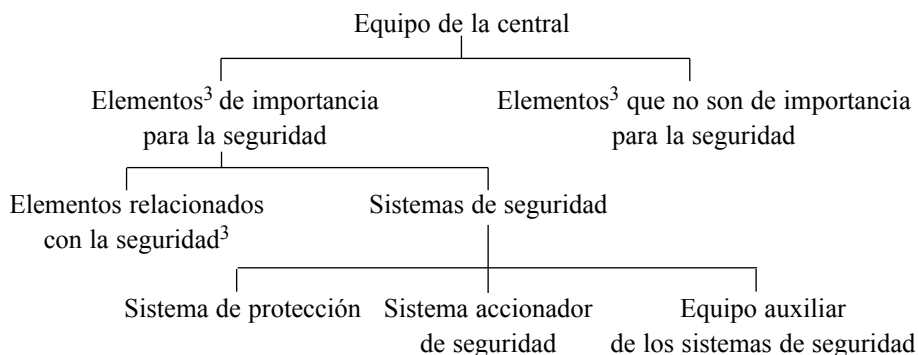
**componente activo** (*active component*). Componente cuyo funcionamiento depende de un factor externo, como un accionamiento, un movimiento mecánico o un suministro de energía.

**componente pasivo** (*passive component*). Componente cuyo funcionamiento no depende de un factor externo como un accionamiento, un movimiento mecánico o un suministro de energía.

**diversidad** (*diversity*). La existencia de dos o más componentes o sistemas redundantes para ejecutar una función determinada, cuando los distintos componentes o sistemas tienen diferentes características para reducir la posibilidad de fallos debidos a causa común.

**elemento de importancia para la seguridad** (*items important to safety*). Elemento que forma parte de un grupo de seguridad y/o cuyo mal funcionamiento o fallo podría originar una exposición a la radiación del personal del emplazamiento o de miembros del público.

**equipo de la central** (*plant equipment*).



<sup>3</sup> En este contexto, por “elemento” se entiende una estructura, sistema o componente.

**estados de la central** (*plant states*).

estados operacionales		condiciones de accidente			
funcionamiento normal	incidentes operacionales previstos	a)	accidentes base de diseño	condiciones que rebasen las de accidente base de diseño	
				b)	accidentes graves
				gestión de accidentes	

- a) Condiciones de accidente que no se consideran explícitamente como accidentes base de diseño pero que están incluidas en ellos.
- b) Condiciones que rebasan las de accidentes base de diseño sin graves daños para el núcleo.

**accidente base de diseño** (*design basis accident*). Condiciones de accidente para hacer frente a las cuales se ha diseñado la central nuclear con arreglo a criterios de diseño establecidos, y en las cuales el deterioro del combustible y la liberación de material radiactivo se mantienen dentro de los límites autorizados.

**accidentes graves** (*severe accidents*). Condiciones de accidente más graves que las de un accidente base de diseño y que ocasionan una degradación significativa del núcleo.

**condiciones de accidente** (*accident conditions*). Alteraciones de una situación operacional normal más graves que los incidentes operacionales previstos; incluyen los accidentes base de diseño y los accidentes graves.

**estados operacionales** (*operational states*). Estados definidos como funcionamiento normal e incidentes operacionales previstos.

**funcionamiento normal** (*normal operation*). Explotación dentro de los límites y condiciones operacionales especificados.

**gestión de accidentes** (*accident management*). Adopción de un conjunto de medidas durante la evolución de condiciones que rebasen las de accidentes base de diseño, a fin de:

- evitar que el suceso degenera en un accidente grave;
- atenuar las consecuencias de un accidente grave; y
- lograr un estado estable y duradero.

**incidente operacional previsto** (*anticipated operational occurrence*). Proceso operacional que se desvía del funcionamiento normal, que se supone que puede ocurrir al menos una vez durante la vida útil de funcionamiento de una instalación, pero que, debido a la existencia de características de diseño adecuadas, no ocasiona daños significativos a los elementos de importancia para la seguridad, ni origina condiciones de accidente.

**fallo debido a causa común** (*common cause failure*). Fallo de dos o más estructuras, sistemas o componentes debido a un único suceso o causa de carácter específico.

**fallo único** (*single failure*). Fallo que produce la pérdida de capacidad de un componente para desempeñar las funciones de seguridad que se le habían asignado, y cualquier fallo que se produce como consecuencia de él.

**función de seguridad** (*safety function*). Función destinada a conseguir un objetivo específico con fines de seguridad.

**grupo de seguridad** (*safety group*). Conjunto de componentes destinados a realizar todas las funciones necesarias para que en el caso de que se produzca un suceso iniciador postulado determinado, se consiga que no se rebasen los límites especificados en la base de diseño para incidentes operacionales previstos y accidentes base de diseño.

**puntos de tarado del sistema de seguridad** (*safety system settings*). Niveles a los que se accionan automáticamente los dispositivos protectores en caso de incidentes operacionales previstos o condiciones de accidente, para evitar que se rebasen los límites de seguridad.

**separación física** (*physical separation*). Separación por disposición geométrica (distancia, orientación, etc.), por barreras adecuadas, o por una combinación de ambas.

**sistema de protección** (*protection system*). Sistema que vigila el funcionamiento de un reactor y que, al detectar una situación anormal, inicia automáticamente acciones para evitar una situación de inseguridad o de posible inseguridad.

**sistema de seguridad** (*safety system*). Sistema de importancia para la seguridad, establecido para lograr la parada del reactor en condiciones de seguridad o la eliminación del calor residual del núcleo, o para limitar las consecuencias de los incidentes operacionales previstos y de los accidentes base de diseño.

**suceso iniciador postulado**<sup>4</sup> (*postulated initiating event*). Suceso indicado en el diseño como capaz de originar incidentes operacionales previstos o condiciones de accidente.

**sumidero final de calor** (*ultimate heat sink*). Medio al que puede transferirse siempre el calor residual, incluso en el caso de que todos los demás medios de eliminación del calor se hayan perdido o resulten insuficientes.

---

<sup>4</sup> Véanse más detalles en el Apéndice I.

## COLABORADORES EN LA REDACCIÓN Y EXAMEN

Allen, P.	Atomic Energy of Canada Limited, Canadá
Cowley, J.S.	Her Majesty's Nuclear Installations Inspectorate, Reino Unido
De Munk, P.	Ministerio de Asuntos Sociales y Empleo, Países Bajos
Feron, F.	Division pour la Sûreté des Installations Nucléaires, Francia
Foskolos, K.	Instituto Paul Scherrer, Suiza
Frisch, W.	Gesellschaft für Anlagen- und Reaktorsicherheit mbH, Alemania
Gasparini, M.	Organismo Internacional de Energía Atómica
Hardin, W.	Nuclear Regulatory Commission, Estados Unidos de América
Kavun, O.	Atomenergoprojekt, Federación de Rusia
Omoto, A.	Compañía de Electricidad de Tokio, Japón
Park, D.	Instituto de Seguridad Nuclear, República de Corea
Price, E.G.	Atomic Energy of Canada Limited, Canadá
Simon, M.	Gesellschaft für Anlagen- und Reaktorsicherheit mbH, Alemania
Tripputi, I.	Ente Nazionale per l'Energia Elettrica, Italia
Vidard, M.	Electricité de France/Septen, Francia

## ÓRGANOS ASESORES PARA LA APROBACIÓN DE LAS NORMAS DE SEGURIDAD

### Comité Asesor sobre normas de seguridad nuclear

*Alemania:* Wendling, R.D., Sengewein, H., Krüger, W.; *Bélgica:* Govaerts, P. (Presidente); *Brasil:* da Silva, A.J.C.; *Canadá:* Wigfull, P.; *China:* Lei, Y., Zhao, Y.; *Estados Unidos de América:* Morris, B.M.; *Federación de Rusia:* Baklushin, R.P.; *Finlandia:* Salminen, P.; *Francia:* Saint Raimond, P.; *India:* Venkat Raj, V.; *Japón:* Tobioka, T.; *Países Bajos:* de Munk, P., Versteeg, J.; *Reino Unido:* Willby, C., Pape, R.P.; *República Checa:* Stuller, J.; *República de Corea:* Moon, P.S.H.; *Suecia:* Viktorsson, C., Jende, E.; *AEN/OCDE:* Frescura, G., Royen, J.; *OIEA:* Lacey, D.J. (Coordinador).

### Comisión Asesora sobre normas de seguridad

*Alemania:* Hennenhöfer, G., Wendling, R.D.; *Argentina:* Beninson, D.; *Australia:* Lokan, K., Burns, P.; *Canadá:* Bishop, A. (Presidente), Duncan, R.M.; *China:* Huang, Q., Zhao, C.; *Eslovaquia:* Lipár, M., Misák, J.; *España:* Alonso, A., Trueba, P.; *Estados Unidos de América:* Travers, W.D., Callan, L.J., Taylor, J.M.; *Francia:* Lacoste, A.-C., Asty, M.; *Japón:* Sumita, K., Sato, K.; *Reino Unido:* Williams, L.G., Harbison, S.A.; *República de Corea:* Lim, Y.K.; *Suecia:* Holm, L.-E.; *Suiza:* Prêtre, S.; *AEN/OCDE:* Frescura, G.; *CIPR:* Valentin, J.; *OIEA:* Karbassioun, A. (Coordinador).