NORMA CUBANA

NC

IEC 61508-2: 2012
(Publicada por la IEC en 2000)

SEGURIDAD FUNCIONAL DE LOS SISTEMAS ELÉCTRICOS/ELECTRÓNICOS/ELECTRÓNICOS PROGRAMABLES RELACIONADOS CON LA SEGURIDAD — PARTE 2: REQUISITOS PARA LOS SISTEMAS ELÉCTRICOS/ELECTRÓNICOS/ELECTRÓNICOS PROGRAMABLES RELACIONADOS CON LA SEGURIDAD (IEC 61508-2: 2000, IDT)

Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 2: *Requirements for electrical/electronic/programmable electronic safety-related systems*

ICS: 25.040.40

1. Edición Diciembre 2012

Oficina Nacional de Normalización (NC) Calle E No. 261 El Vedado, La Habana. Cuba. Teléfono: 830-0835 Fax: (537) 836-8048; Correo electrónico: nc@ncnorma.cu; Sitio Web: www.nc.cubaindustria.cu

Cuban National Bureau of Standards

Prefacio

La Oficina Nacional de Normalización (NC) es el Organismo Nacional de Normalización de la República de Cuba y representa al país ante las organizaciones internacionales y regionales de normalización.

La elaboración de las Normas Cubanas y otros documentos normativos relacionados se realiza generalmente a través de los Comités Técnicos de Normalización. Su aprobación es competencia de la Oficina Nacional de Normalización y se basa en las evidencias del consenso.

Esta Norma Cubana:

- Ha sido elaborada por el Comité Técnico de Normalización NC/CTN 116 de Automática, integrado por representantes de las siguientes entidades:

  - Empresa de Automatización Integral perteneciente al Ministerio de la Informática y las Comunicaciones
  - Ministerio de la Industria Básica
  - Universidad de Oriente
  - Universidad Central de Villa Clara, Marta Abreu
  - Instituto Superior Politécnico, José Antonio Echevarría
  - ALIMATIC del Ministerio de la Industria Alimentaria
  - Universidad de Ciencias Informáticas
  - Instituto de Cibernética, Matemática y Física
  - Ministerio de Ciencia, Tecnología y Medio Ambiente
  - Oficina Nacional de Normalización

- Es una adopción idéntica por el método de reimpresión de la versión oficial en español de la Norma Europea EN 61508-2: 2001 *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 2: Requirements for electrical/electronic/programable electronic safety-related systems* que a su vez adopta de forma idéntica a la Norma Internacional IEC 61508-1: 2000)

NORMA EUROPEA
EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

EN 61508-2

Diciembre 2001

ICS 25.040.40

Versión en español

Seguridad funcional de los sistemas eléctricos/electrónicos/ electrónicos programables relacionados con la seguridad Parte 2: Requisitos para los sistemas eléctricos/electrónicos/ electrónicos programables relacionados con la seguridad

(CEI 61508-2:2000)

Functional safety of electrical/electronic/ programmable electronic safety-related systems.
Part 2: Requirements for electrical/ electronic/programmable electronic safety-related systems.
(IEC 61508-2:2000).

Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité.
Partie 2: Prescriptions pour les systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité.
(CEI 61508-2:2000).

Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/ programmierbarer elektronischer Systeme.
Teil 2: Anforderungen an sicherheitsbezogene elektrische/ elektronische/programmierbare elektronische Systeme.
(IEC 61508-2:2000).

Esta norma europea ha sido aprobada por CENELEC el 2001-07-03. Los miembros de CENELEC están sometidos al Reglamento Interior de CEN/CENELEC que define las condiciones dentro de las cuales debe adoptarse, sin modificación, la norma europea como norma nacional.

Las correspondientes listas actualizadas y las referencias bibliográficas relativas a estas normas nacionales, pueden obtenerse en la Secretaría Central de CENELEC, o a través de sus miembros.

Esta norma europea existe en tres versiones oficiales (alemán, francés e inglés). Una versión en otra lengua realizada bajo la responsabilidad de un miembro de CENELEC en su idioma nacional, y notificada a la Secretaría Central, tiene el mismo rango que aquéllas.

Los miembros de CENELEC son los comités electrotécnicos nacionales de normalización de los países siguientes: Alemania, Austria, Bélgica, Dinamarca, España, Finlandia, Francia, Grecia, Irlanda, Islandia, Italia, Luxemburgo, Malta, Noruega, Países Bajos, Portugal, Reino Unido, República Checa, Suecia y Suiza.

CENELEC
COMITÉ EUROPEO DE NORMALIZACIÓN ELECTROTÉCNICA
European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung
SECRETARÍA CENTRAL: Rue de Stassart, 35 B-1050 Bruxelles

ANTECEDENTES

El texto de la Norma Internacional CEI 61508-2:2000, preparado por el Subcomité SC 65A, *Aspectos de sistemas*, del Comité Técnico TC 65, *Medida y control en procesos industriales*, de CEI, fue sometido al Procedimiento de Aceptación Única (UAP) y fue aprobado por CENELEC como Norma Europea EN 61508-2 el 2001-07-03 sin ninguna modificación.

Se fijaron las siguientes fechas:

– Fecha límite en la que la norma europea debe adoptarse a nivel nacional por publicación de una norma nacional idéntica o por ratificación	(dop)	2002-08-01
– Fecha límite en la que deben retirarse las normas nacionales divergentes con esta norma	(dow)	2004-08-01

Los anexos denominados “normativos” forman parte del cuerpo de la norma.

En esta norma los anexos A, B, C y ZA son normativos.

El anexo ZA ha sido añadido por CENELEC.

La Norma CEI 61508 es una publicación básica de seguridad que se aplica a la seguridad funcional de los sistemas eléctricos, electrónicos y electrónicos programables relacionados con la seguridad. El objeto y campo de aplicación establece:

"Esta norma internacional trata los aspectos a tener en consideración cuando se utilicen sistemas eléctricos/electrónicos/electrónicos programables (E/E/PE), para ejecutar funciones de seguridad. Uno de los principales objetivos de esta norma internacional es permitir la elaboración de normas internacionales específicas a cada sector de aplicación por los comités técnicos responsables de los sectores correspondientes. Esto permitirá tener en cuenta el conjunto de los factores pertinentes para cada aplicación, y de responder a las necesidades especificas de cada uno de estos sectores. Otro de los objetivos perseguidos por esta norma internacional es permitir el desarrollo de sistemas E/E/PE relacionados con la seguridad en ausencia eventual de normas internacionales para este sector de aplicación".

El Informe CENELEC R0BT-004, ratificado por el 103 BT (marzo 2000) acepta que algunas normas CEI, hoy publicadas o en preparación, sean implementaciones sectoriales de la Norma CEI 61508. Por ejemplo:

- CEI 61511 – *Seguridad funcional. Sistemas instrumentados de seguridad para el sector de industrias de transformación.*

- CEI 62061 – *Seguridad de las máquinas. Seguridad funcional de los sistemas de control eléctricos, electrónicos y electrónicos programables.*

- CEI 61513 – *Centrales nucleares. Instrumentación y control para los sistema importantes para la seguridad. Requisitos generales para los sistemas.*

El sector ferroviario ha desarrollado también un conjunto de normas europeas (EN 50126, EN 50128 y prEN 50129).

NOTA – Las Normas EN 50126 y EN 50128 están basadas en los proyectos iniciales de la Norma CEI 61508. El prEN 50129 está basado en principio, en la última versión de la Norma CEI 61508.

Esta lista no prejuzga otras implementaciones sectoriales de la Norma CEI 61508 que podrán estar actualmente en preparación o publicadas por CENELEC o CEI.

DECLARACIÓN

El texto de la Norma Internacional CEI 61508-2:2000 fue aprobado por CENELEC como norma europea sin ninguna modificación.

En la versión oficial, para la bibliografía, debe añadirse la siguiente nota para la norma indicada*:

CEI 61000-4	NOTA – Armonizada como Norma EN 61000-4, serie (sin ninguna modificación).
CEI 60870-5-1	NOTA – Armonizada como Norma EN 60870-5-1:1993 (sin ninguna modificación).

* Introducida en la norma indicándose con una línea vertical en el margen izquierdo del texto.

ÍNDICE

Página

INTRODUCCIÓN

Los sistemas eléctricos y electrónicos se han utilizado durante muchos años para realizar funciones de seguridad en la mayoría de los sectores de aplicación. Los sistemas basados en la informática (generalmente referidos a Sistemas Electrónicos Programables (PES)[1)] se utilizan en todos los sectores de aplicación para realizar funciones no relacionadas con la seguridad, pero cada día más se están utilizando para funciones de seguridad. Si se quiere explotar de forma eficaz y segura la tecnología de los sistemas informáticos, es imprescindible que el responsable de tomar decisiones haya sido orientado en los aspectos de seguridad en los cuales va a tomar las decisiones.

Esta norma internacional establece una aproximación genérica para todas las actividades relacionadas con el ciclo de vida de seguridad de los sistemas que incluyan componentes eléctricos y/o electrónicos y/o electrónicos programables (E/E/PES) que se utilizan para realizar las funciones de seguridad. Esta propuesta unificada ha sido adoptada con el fin de desarrollar una política técnica lógica y coherente relativa a todos los aparatos eléctricos relacionados con la seguridad. Uno de los principales objetivos perseguidos es el de facilitar la elaboración de normas de aplicación sectorial.

En la mayoría de los casos, la seguridad se obtiene gracias a un cierto número de sistemas de protección basados en distintas tecnologías (por ejemplo, mecánica, hidráulica, neumática, eléctrica, electrónica, electrónica programable). Por lo tanto, toda estrategia de seguridad debe tener en cuenta no solamente todos los elementos de un sistema de seguridad individual (por ejemplo, sensores, dispositivos de control e interruptores), sino que también debe tener en cuenta todos los sistemas relacionados con la seguridad como elementos individuales de un conjunto complejo. Es por ello que esta norma internacional, tratando esencialmente los sistemas, relacionados con la seguridad, eléctricos/electrónicos/ electrónicos programables E/E/PE, también puede proporcionar un sistema en el cual pueden considerarse los sistemas relacionados con la seguridad basados en otras tecnologías.

Existe gran variedad de aplicaciones de los E/E/PES. Estos cubren un gran número de grados de complejidad, y potenciales de peligros y riesgos en todos los sectores de aplicación. Para cada aplicación, las medidas de seguridad requeridas dependerán de los propios factores de la aplicación. Esta norma internacional, por ser genérica, debe permitir en lo sucesivo trasponer estas medidas en las normas internacionales de aplicación sectorial.

Esta norma internacional:

- concierne a todas las fases del ciclo de vida de la seguridad de los E/E/PES y del software (desde la concepción inicial, pasando por el diseño, la instalación, la explotación y el mantenimiento, hasta la finalización del servicio) donde los E/E/PES realizan funciones de seguridad;

- ha sido elaborada teniendo en cuenta la rápida evolución de la tecnología; el marco que comprende esta norma internacional es suficientemente sólido y extenso como para prever las evoluciones futuras;

- permite la elaboración de normas internacionales por sectores de aplicación concernientes a los E/E/PES relacionados con la seguridad. La elaboración de normas internacionales por sector de aplicación a partir de esta norma internacional debe permitir alcanzar un alto nivel de coherencia (por ejemplo, principios subyacentes, terminología, etc.) tanto en el seno de cada sector de aplicación, como de un sector a otro. Esto proporcionará una mejora en términos de seguridad y de beneficios económicos;

- proporciona un método para el desarrollo de los requisitos de seguridad necesarios para lograr la seguridad funcional requerida para los sistemas E/E/PE relacionados con la seguridad;

- utiliza los niveles de integridad de seguridad para especificar el nivel objetivo de integridad de seguridad para las funciones de seguridad que deben realizar los sistemas E/E/PE relacionados con la seguridad;

- adopta un planteamiento basado en el riesgo para determinar los requisitos de los niveles de integridad de seguridad;

1) PES del inglés: Programmable Electronic Systems.

- fija los objetivos cuantitativos para las medidas de fallo de los sistemas E/E/PE relacionados con la seguridad que tienen relación con los niveles de integridad de seguridad;

- fija un límite inferior para las medidas de fallo, en el caso de un modo de fallo peligroso, este límite podrá exigirse para un sistema E/E/PE relacionado con la seguridad único, en el caso de un sistema E/E/PE relacionado con la seguridad funcionando:

  - en un modo de baja demanda, el límite inferior está fijado a una probabilidad media de fallo de 10^{-5} con el fin de que las funciones por las cuales el sistema ha sido diseñado sean realizadas cuando sean requeridas;

  - en un modo de funcionamiento continuo o de alta demanda, el límite inferior está fijado a una probabilidad de fallo peligroso de 10^{-9} por hora;

  NOTA – Un sistema E/E/PE relacionado con la seguridad único no implica necesariamente una arquitectura en un solo canal.

- adopta una amplia gama de principios, técnicas y medidas para la realización de la seguridad funcional de los sistemas E/E/PE relacionados con la seguridad, pero no utiliza el concepto de "libre de fallo" (seguridad intrínseca) que tiene un sentido particular cuando los modos de fallo están bien definidos y el nivel de complejidad es relativamente bajo. Este concepto ha sido considerado como inadecuado debido a la inmensa gama de complejidad de los sistemas E/E/PE relacionados con la seguridad que entran en el objeto y campo de aplicación de esta norma.

Seguridad funcional de los sistemas eléctricos/electrónicos/ electrónicos programables relacionados con la seguridad Parte 2: Requisitos para los sistemas eléctricos/electrónicos/ electrónicos programables relacionados con la seguridad

1 OBJETO Y CAMPO DE APLICACIÓN

1.1 Esta parte de la Norma CEI 61508

a) sólo se puede utilizar cuando se asegure una perfecta comprensión con la Norma CEI 61508-1 que proporciona el marco global que permite realizar la seguridad funcional;

b) se aplica a todo sistema relacionado con la seguridad tal como se define en la Norma CEI 61508-1, que contiene al menos un componente eléctrico, electrónico o electrónico programable;

c) se aplica a todos los subsistemas y sus componentes en un sistema E/E/PE relacionado con la seguridad (incluyendo los sensores, accionadores y la interfaz del operario);

d) especifica la forma de refinar las informaciones desarrolladas de acuerdo con la Norma CEI 61508-1, relacionadas con los requisitos de seguridad globales y su aplicación a los sistemas E/E/PE relacionados con la seguridad, y especifica la forma en la que los requisitos de seguridad globales se refinan en requisitos de funciones de seguridad de los E/E/PES y en requisitos de integridad de seguridad de los E/E/PES;

e) especifica los requisitos para las actividades que deben aplicarse durante el diseño y la fabricación de los sistemas relacionados con la seguridad (lo que significa que debe establecer el modelo del ciclo de vida de la seguridad de los E/E/PES), a excepción del software (soporte lógico) que se trata en la Norma CEI 61508-3 (véanse las figuras 2 y 3), estos requisitos incluyen la aplicación de técnicas y de medidas que se clasifican en función del nivel de integridad de seguridad para evitar y controlar los fallos y averías;

f) especifica la información necesaria para la instalación, la puesta en servicio y la validación final de la seguridad de los sistemas E/E/PE relacionados con la seguridad;

g) no se aplica a la fase de explotación y de mantenimiento de los sistemas E/E/PE relacionados con la seguridad – que se tratan en la Norma CEI 61508-1 – sin embargo, la Norma CEI 61508-2 proporciona los requisitos de preparación de las informaciones y de los procedimientos necesarios al usuario para la explotación y el mantenimiento de los sistemas E/E/PE relacionados con la seguridad;

h) especifica los requisitos que debe cumplir la organización que realice una modificación de los sistemas E/E/PE relacionados con la seguridad.

NOTA 1 – Esta parte de la Norma CEI 61508 se destina principalmente a los suministradores y/o a los servicios técnicos internos de las empresas. Por esta razón incluye los requisitos aplicables para modificaciones.

NOTA 2 – La relación entre la Norma CEI 61508-2 y la Norma CEI 61508-3 se muestra en la figura 3.

1.2 Las partes 1, 2, 3 y 4 de esta norma son publicaciones básicas de seguridad, aunque este estado no sea aplicable en el contexto de los sistemas E/E/PE de baja complejidad relacionados con la seguridad (véase el apartado 3.4.4 de la parte 4). Como publicaciones básicas de seguridad, estas normas están previstas para utilizarse por los comités técnicos para la preparación de normas de acuerdo con los principios contenidos en la Guía CEI 104 y la Guía ISO/CEI 51. Las partes 1, 2, 3 y 4 también están destinadas a utilizarse como publicaciones independientes.

Una de las responsabilidades de un comité técnico es, en la medida de lo posible, utilizar las publicaciones básicas de seguridad para la preparación de sus publicaciones. En este contexto, los requisitos, los métodos de ensayo o las condiciones de ensayo de esta publicación básica de seguridad sólo se aplican si se indican específicamente, o se incluyen en las publicaciones preparadas por estos comités técnicos.

NOTA 1 – La seguridad funcional de un sistema E/E/PE relacionado con la seguridad no puede realizarse a no ser que se cumplan todos los requisitos pertinentes. En consecuencia, es importante que todos los requisitos pertinentes se consideren cuidadosamente y se referencien de forma apropiada.

NOTA 2 – En los Estados Unidos de América y en Canadá, en espera de la futura publicación de la Norma CEI 61551 (la versión de la Norma CEI 61508 para procesos), las normas nacionales existentes de seguridad de procesos basadas en la Norma CEI 61508 (por ejemplo, la Norma ANSI/ISA-S84.01) pueden aplicarse en el sector de procesos industriales en lugar de la Norma CEI 61508.

1.3 La figura 1 muestra la estructura general de las partes 1 a 7 de la Norma CEI 61508 e indica el papel que la Norma CEI 61508-2 juega en el logro de la seguridad funcional para los sistemas E/E/PE relacionados con la seguridad. El anexo A de la Norma CEI 61508-6 describe la aplicación de las Normas CEI 61508-2 y CEI 61508-3.

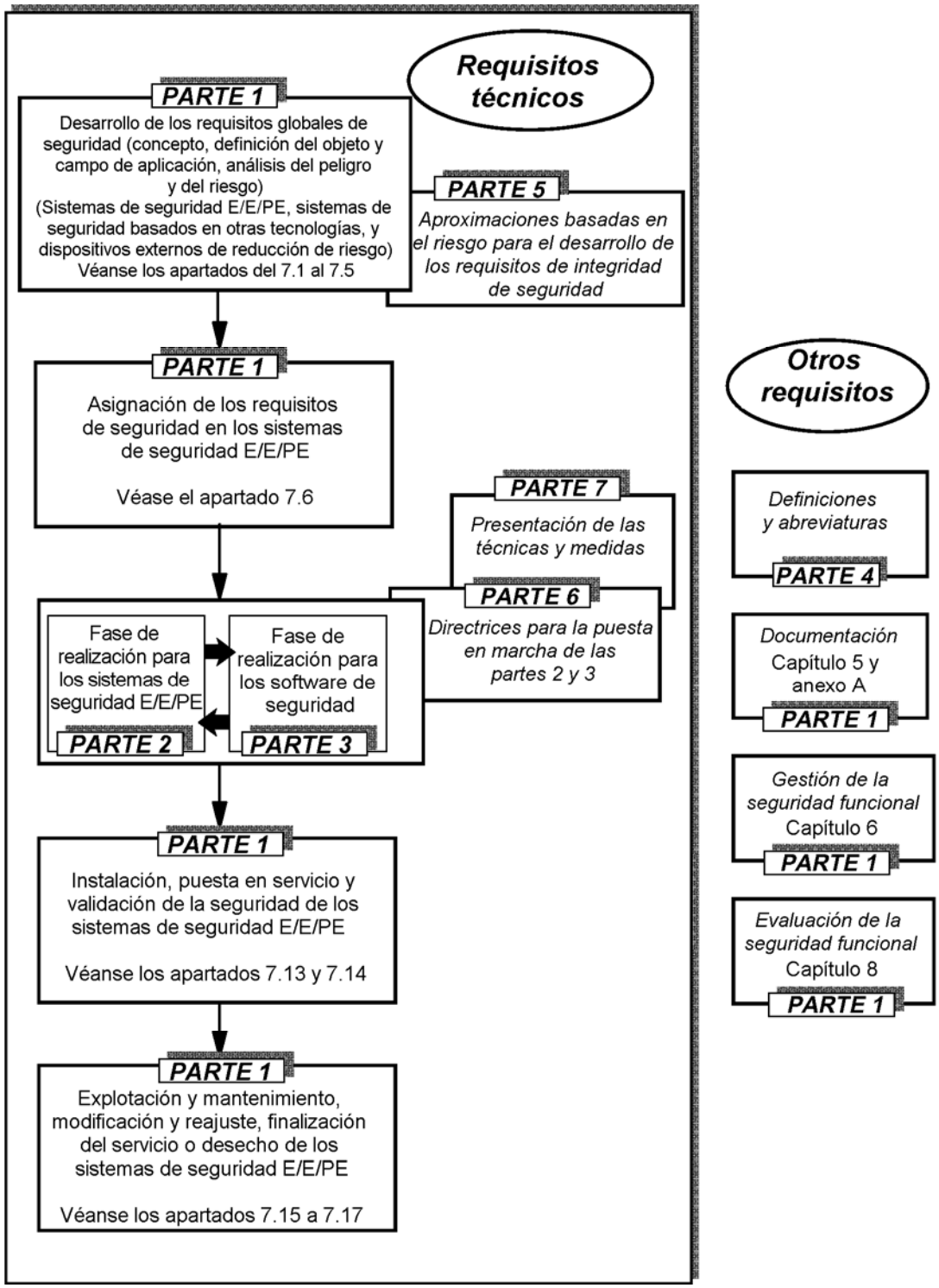


Fig. 1 – Estructura general de la Norma CEI 61508

5 DOCUMENTACIÓN

Los requisitos relacionados con la documentación se detallan en el capítulo 5 de la Norma CEI 61508-1.

6 GESTIÓN DE LA SEGURIDAD FUNCIONAL

Los requisitos para la gestión de la seguridad funcional se detallan en el capítulo 6 de la Norma CEI 61508-1.

7 REQUISITOS DEL CICLO DE VIDA DE LA SEGURIDAD DE LOS E/E/PES

7.1 Generalidades

7.1.1 Objetivos y requisitos: generalidades

7.1.1.1 Este apartado establece los objetivos y los requisitos para las fases del ciclo de vida de la seguridad de los E/E/PES.

NOTA – La Norma CEI 61508-1 proporciona los objetivos y los requisitos del ciclo de vida de la seguridad global, así como una introducción general a la estructura de la norma.

7.1.1.2 Para todas las fases del ciclo de vida de la seguridad de los E/E/PES, la tabla 1 indica:

– los objetivos a alcanzar;

– el objeto y campo de aplicación de la fase correspondiente;

– una referencia al apartado que contiene los requisitos;

– los datos requeridos para las fases;

– los resultados requeridos para cumplir con los requisitos del apartado correspondiente.

7.1.2 Objetivos

7.1.2.1 El primer objetivo de los requisitos de este apartado es estructurar de forma sistemática las fases del ciclo de vida de la seguridad de los E/E/PES que deben tenerse en cuenta para realizar la seguridad funcional exigida de los sistemas E/E/PE relacionados con la seguridad.

7.1.2.2 El segundo objetivo de los requisitos de este apartado es documentar todas las informaciones relativas a la seguridad funcional de los sistemas E/E/PE relacionados con la seguridad del conjunto del ciclo de vida de la seguridad de los E/E/PES.

7.1.3 Requisitos

7.1.3.1 El ciclo de vida de la seguridad de los E/E/PES que debe utilizarse para declarar la conformidad con esta norma se especifica en la figura 2. Si se utiliza otro ciclo de vida de la seguridad de los E/E/PES, debe especificarse durante la planificación de la seguridad funcional (véase el capítulo 6 de la Norma CEI 61508-1) y cumplir con el conjunto de los objetivos y requisitos de cada apartado de la Norma CEI 61508-2.

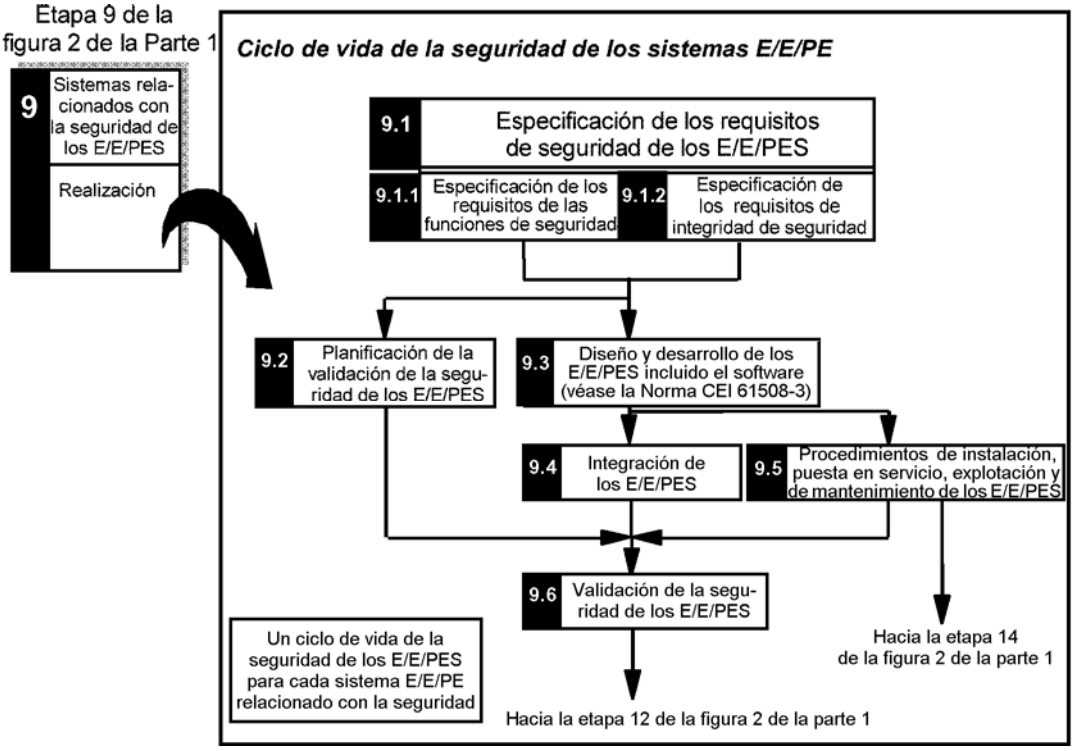
NOTA – Las relaciones entre la Norma CEI 61508-2 y la Norma CEI 61508-3, así como sus objetos y campos de aplicación respectivos se muestran en la figura 3.

7.1.3.2 Los procedimientos de gestión de la seguridad funcional (véase el capítulo 6 de la Norma CEI 61508-1) deben ejecutarse en paralelo con las fases del ciclo de vida de la seguridad de los E/E/PES.

7.1.3.3 Cada fase del ciclo de vida de la seguridad de los E/E/PES debe dividirse en actividades elementales, teniendo en cuenta el objeto y campo de aplicación, de los datos y de los resultados especificados para cada fase (véase la tabla 1).

7.1.3.4 Excepto cuando esté justificado, durante la planificación de la seguridad funcional, los resultados de cada fase del ciclo de vida de la seguridad de los E/E/PES deben documentarse (véase el capítulo 5 de la Norma CEI 61508-1).

7.1.3.5 Los resultados de cada fase del ciclo de vida de los E/E/PES deben cumplir con los objetivos y requisitos especificados para cada fase (véanse los apartados del 7.2 al 7.9).



NOTA – Véase también el punto b) del capítulo A.2 de la Norma CEI 61508-6.

Fig. 2 – Ciclo de vida de la seguridad de los E/E/PES (durante la fase de realización)

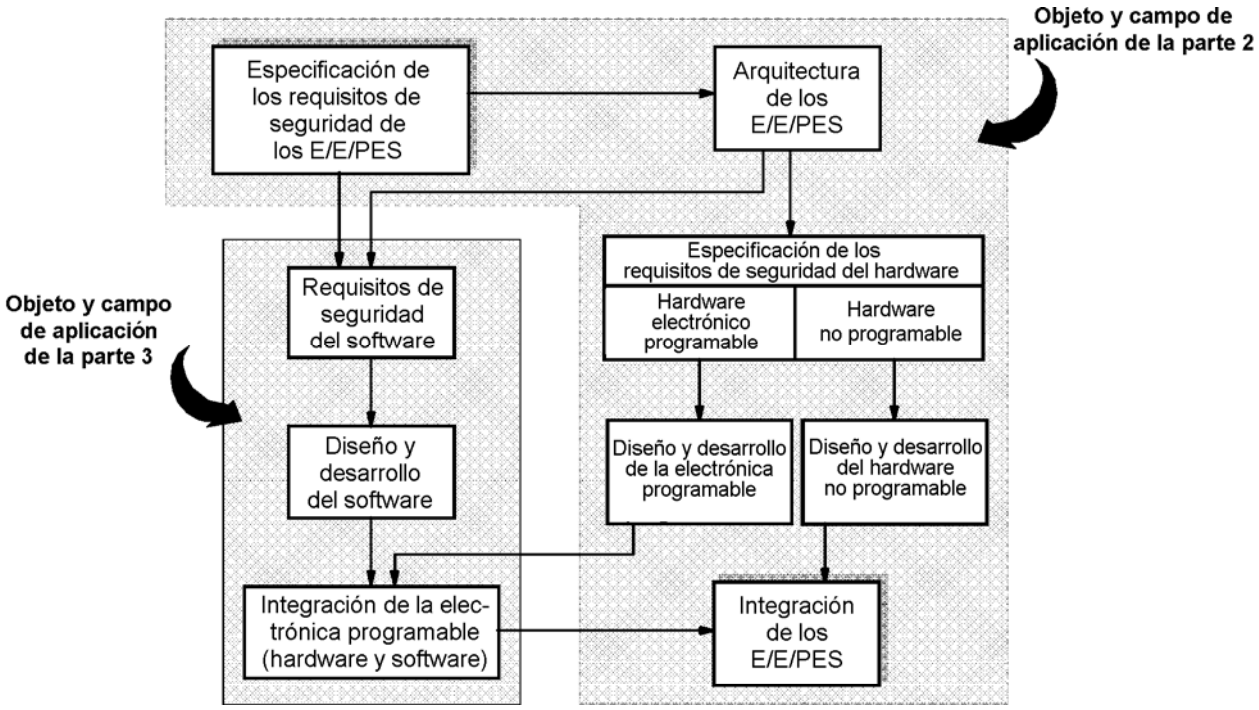


Fig. 3 – Relación, objeto y campo de aplicación de la Norma CEI 61508-2 y de la Norma CEI 61508-3

Tabla 1
Presentación del ciclo de vida de la seguridad de los E/E/PES

Fase o actividad del ciclo de vida de la seguridad		Objetivos	Campo de aplicación	Requisitos (apartado)	Entradas	Salidas
Número de etapa de la figura 2	Título					
9.1	Especificación de los requisitos de seguridad de los E/E/PES	Especificar los requisitos para cada sistema E/E/PE relacionado con la seguridad en términos de función de seguridad requeridos y de integridad de seguridad requerida para obtener la seguridad funcional requerida	Sistemas E/E/PE relacionados con la seguridad	7.2.2	Descripción de la atribución de los requisitos de seguridad (véase el apartado 7.6 de la Norma CEI 61508-1)	Requisitos de seguridad de los E/E/PES Requisitos de seguridad del software para la contribución a la especificación de los requisitos de seguridad del software
9.2	Planificación de la validación de la seguridad de los E/E/PES	Planificar la validación de la seguridad de los sistemas E/E/PE relacionados con la seguridad	Sistemas E/E/PE relacionados con la seguridad	7.3.2	Requisitos de seguridad de los E/E/PES	Plan de validación de la seguridad de los sistemas E/E/PE relacionados con la seguridad
9.3	Diseño y desarrollo de los E/E/PES	Diseñar los sistemas E/E/PE relacionados con la seguridad de forma que cumplan con los requisitos de las funciones de seguridad y de integridad de seguridad	Sistemas E/E/PE relacionados con la seguridad	7.4.2 a 7.4.9	Requisitos de seguridad de los E/E/PES	Diseño de los sistemas E/E/PE relacionados con la seguridad, de acuerdo con los requisitos de seguridad de los E/E/PES Plan de ensayos de integración de los E/E/PES Información sobre la arquitectura PES como contribución a la especificación de los requisitos de seguridad del software
9.4	Integración de los E/E/PES	Integrar y ensayar los sistemas E/E/PE relacionados con la seguridad	Sistemas E/E/PE relacionados con la seguridad	7.5.2	Diseño de los E/E/PES Plan de ensayos de la integración de los E/E/PES Hardware y software de electrónicas programables	Sistemas E/E/PE relacionados con la seguridad, plenamente funcionales y de acuerdo con el diseño de los E/E/PES Resultados de los ensayos de integración de los E/E/PES
9.5	Procedimientos de instalación, puesta en servicio y explotación y de mantenimiento de los E/E/PES	Desarrollar procedimientos que permitan asegurar que la seguridad funcional de los sistemas E/E/PE relacionados con la seguridad se mantienen durante la explotación y el mantenimiento	Sistemas E/E/PE relacionados con la seguridad EUC (Equipo sometido a control)	7.6.2	Requisitos de seguridad de los E/E/PES Diseño de los E/E/PES	Procedimientos de instalación, de puesta en servicio, de explotación y de mantenimiento de los E/E/PES para cada E/E/PES individual
9.6	Validación de la seguridad de los E/E/PES	Validar la conformidad, en todos los aspectos, de los sistemas E/E/PE relacionados con la seguridad, de los requisitos de seguridad en términos de funciones de seguridad requeridos y de la integridad de seguridad requerida	Sistemas E/E/PE relacionados con la seguridad	7.7.2	Requisitos de seguridad de los E/E/PES; Plan de validación de la seguridad de los sistemas E/E/PE relacionados con la seguridad	Sistemas E/E/PE relacionados con la seguridad completamente validados en términos de seguridad Resultados de la validación de la seguridad de los E/E/PES

(Continúa)

Tabla 1 *(Fin)*
Presentación del ciclo de vida de la seguridad de los E/E/PES

Fase o actividad del ciclo de vida de la seguridad		Objetivos	Campo de aplicación	Requisitos (apartado)	Entradas	Salidas
Número de etapa de la figura 2	Título					
–	Modificación de los E/E/PES	Realizar correcciones, mejoras o adaptaciones a los sistemas E/E/PES relacionados con la seguridad para asegurar que el nivel de integridad de seguridad exigido efectivamente se realiza y se mantiene	Sistemas E/E/PE relacionados con la seguridad	7.8.2	Requisitos de seguridad de los E/E/PES	Resultados de modificación de los E/E/PES
–	Verificación de los E/E/PES	Ensayar y evaluar los resultados de una fase dada para asegurar que son correctos y de acuerdo con los productos y normas dadas para esta fase	Sistemas E/E/PE relacionados con la seguridad	7.9.2	Como arriba – en función de la fase Para cada fase, plan de verificación de los sistemas E/E/PE relacionados con la seguridad	Como arriba – en función de la fase Para cada fase, plan de verificación de los sistemas E/E/PE relacionados con la seguridad
–	Evaluación de la seguridad funcional de los E/E/PES	Investigar y obtener una conclusión de la seguridad funcional de los sistemas E/E/PE relacionados con la seguridad	Sistemas E/E/PE relacionados con la seguridad	8	Plan de evaluación de la seguridad funcional de los E/E/PES	Resultados de la evaluación de la seguridad funcional de los E/E/PES

7.2 Especificación de los requisitos de seguridad de los E/E/PES

NOTA – Esta fase se representa en la etapa 9.1 de la figura 2.

7.2.1 Objetivo. El objetivo de los requisitos de este apartado es especificar los requisitos para cada sistema E/E/PE relacionado con la seguridad en términos de función de seguridad requeridos y de integridad de seguridad requerida, para obtener la seguridad funcional exigida.

NOTA – Por ejemplo, pueden exigirse unas funciones de seguridad para poner o mantener el EUC en un estado seguro.

7.2.2 Requisitos generales

7.2.2.1 La especificación de los requisitos de seguridad E/E/PES debe resultar de la atribución de los requisitos de seguridad como los descritos en el apartado 7.6 de la Norma CEI 61508-1 y de los requisitos especificados durante la planificación de la seguridad funcional (véase el capítulo 6 de la Norma CEI 61508-1). Estas informaciones se deben poner a disposición del responsable del desarrollo del E/E/PES.

NOTA – Conviene tomar precauciones particulares cuando unas funciones no relacionadas con la seguridad y unas funciones de seguridad se realizan en el mismo sistema E/E/PE relacionado con la seguridad. Mientras que la presencia simultánea de estos tipos de funciones se admita en esta norma, puede dar lugar a una mayor complejidad y hacer más difícil la ejecución de las actividades del ciclo de vida de la seguridad de los E/E/PES (por ejemplo, el diseño, la validación, la evaluación y el mantenimiento de la seguridad funcional).

7.2.2.2 Los requisitos de seguridad de los E/E/PES deben expresarse y estructurarse para que sean:

a) claros, precisos, sin ambigüedad, verificables, ensayables, mantenibles y viables; y

b) escritos de forma que puedan ser comprendidos por los que van a utilizar la información en cualquier etapa del ciclo de vida de la seguridad de los E/E/PES.

7.2.2.3 La especificación de los requisitos de seguridad de los E/E/PES debe contener los requisitos aplicables a las funciones de seguridad de los E/E/PES (véase al apartado 7.2.3.1) así como los requisitos aplicables a la integridad de seguridad de los E/E/PES (véase al apartado 7.2.3.2).

7.2.3 Requisitos de seguridad de los E/E/PES

7.2.3.1 La especificación de los requisitos de las funciones de seguridad de los E/E/PES debe contener:

a) una descripción de todas las funciones de seguridad necesarias para la realización de la seguridad funcional requerida y debe, para cada función de seguridad:

   - proporcionar unos requisitos globales suficientemente detallados para el diseño y el desarrollo de los sistemas E/E/PE relacionados con la seguridad,

   - describir la forma en la que los sistemas E/E/PE relacionados con a seguridad tienen la intención de realizar o de mantener un estado seguro para el EUC,

   - precisar la necesidad de un control continuo o no así como los periodos correspondientes, cuando se trata de obtener o de mantener un estado seguro del EUC, y

   - especificar la aplicabilidad de la función de seguridad a los sistemas E/E/PE relacionados con la seguridad funcionando en modo de baja demanda o de demanda elevada/continua;

b) prestaciones en términos de velocidad de tratamiento y de tiempo de respuesta;

c) interfaces entre el sistema E/E/PE relacionado con la seguridad y el operario, necesarios para realizar la seguridad funcional requerida;

d) toda la información ligada a la seguridad funcional puede tener influencia sobre el diseño del sistema E/E/PE relacionado con la seguridad;

e) todas las interfaces entre los sistemas E/E/PE relacionados con la seguridad y todos los otros sistemas (directamente asociados al interior, o al exterior del EUC);

f) todos los modos de explotación relevantes del EUC que incluyen:

   - la preparación para la utilización, incluyendo la inicialización y el reglaje,

   - el arranque, aprendizaje, funcionamiento en modo automático, manual, semiautomático o en régimen de operación,

   - el no funcionamiento en régimen de operación, reinicialización, parada y mantenimiento,

   - condiciones anormales razonablemente previsibles;

   NOTA 1 – Las condiciones anormales razonablemente previsibles son las condiciones anormales que el desarrollador o el usuario puede razonablemente prevenir.

   NOTA 2 – Se admite que se requieran unas funciones de seguridad suplementarias para unos modos de funcionamiento (por ejemplo, la inicialización, el ajuste o el mantenimiento) para permitir realizar estas operaciones con toda seguridad.

g) se deben detallar todos los modos de comportamiento del sistema relacionado con la seguridad - en particular el comportamiento en caso de fallo y la respuesta requerida (por ejemplo, alarma, parada automática, etc.) del sistema E/E/PE relacionado con la seguridad;

h) la importancia de todas las interacciones entre el hardware/software – cuando sea relevante, todas las limitaciones exigidas entre el hardware y el software debe identificarse y documentarse;

NOTA 3 – Cuando estas intervenciones no se conocen antes de terminar el diseño, sólo se pueden declarar las limitaciones de orden general.

i) las restricciones y condiciones de las limitaciones del sistema E/E/PE relacionado con la seguridad y los subsistemas asociados, por ejemplo las limitaciones temporales;

j) todos los requisitos especificados ligados a los procedimientos de arranque y rearranque de los sistemas E/E/PE relacionados con la seguridad.

7.2.3.2 La especificación de los requisitos de integridad de seguridad de los E/E/PES debe contener:

a) el nivel de integridad de seguridad para cada función de seguridad y cuando se requiera (véase la nota 2), la medida objetivo de fallo requerida para la función de seguridad;

NOTA 1 – El nivel de integridad de seguridad de una función de seguridad determina la medida objetivo de fallo de la función de seguridad de acuerdo con la Norma CEI 61508-1, tablas 2 y 3.

NOTA 2 – Es necesario especificar la medida objetivo de fallo de una función de seguridad cuando la reducción necesaria de riesgo para la función de seguridad se ha obtenido utilizando un método cuantitativo (véase la Norma CEI 61508-1, apartado 7.5.2.2).

b) el modo de funcionamiento en baja demanda o fuerte demanda/continua de cada función de seguridad;

c) los requisitos, limitaciones, funciones y dispositivos que permiten realizar el ensayo periódico del hardware E/E/PES;

d) todas las condiciones del entorno extremas a las que el sistema E/E/PE será expuesto durante su ciclo de vida de seguridad, incluyendo la fabricación, el almacenamiento, el transporte, los ensayos, la instalación, la puesta en servicio, la explotación y el mantenimiento;

e) los límites de inmunidad electromagnética (véase la Norma CEI 61000-1-1) que son necesarios para asegurar la compatibilidad electromagnética - conviene deducir los límites de inmunidad electromagnética teniendo en cuenta a la vez el entorno electromagnético (véase la Norma CEI 61000-2-5) y los niveles de integridad de seguridad requeridos.

NOTA 1 – Es importante notar que el nivel de integridad de seguridad es un factor determinante para los límites de inmunidad electromagnética, especialmente cuando el nivel de perturbación electromagnética en el entorno se somete a una repartición estática. En la práctica, a menudo es imposible especificar un nivel absoluto de perturbación; sólo se puede indicar un nivel que se espera que no se exceda en la práctica (se trata del nivel de compatibilidad electromagnética). Desafortunadamente, los problemas de orden práctico prueban que es muy difícil definir la probabilidad ligada a dicha previsión. En consecuencia, el límite de inmunidad no garantiza que el sistema E/E/PE relacionado con la seguridad no fallará debido a las perturbaciones electromagnéticas; proporciona únicamente un cierto nivel de confianza para que un fallo no ocurra. El nivel de confianza real depende del límite de inmunidad en relación a la repartición estadística de los niveles de perturbación en el entorno de explotación. Para unos niveles de integridad de seguridad superiores, es necesario tener un nivel de confianza más alto y, para esto, se recomienda que el margen para el que el límite de inmunidad exceda el límite de compatibilidad sea más importante para los niveles de integridad de seguridad superiores.

NOTA 2 – También pueden encontrarse directrices en las normas de CEM de familias de productos. Pero es importante reconocer que unos niveles de inmunidad más elevados que los especificados en estas normas pueden ser necesarios en unas localizaciones particulares o cuando el equipo es previsto para se utilizado en un entorno electromagnético más severo.

NOTA 3 – En la elaboración de la especificación de los requisitos de seguridad de los E/E/PES, conviene tener en cuenta la aplicación en la que el sistema E/E/PE relacionado con la seguridad se debe utilizar. Esto es notablemente importante para el mantenimiento, en donde se recomienda que el intervalo del ensayo periódico especificado no sea inferior al que se puede alcanzar razonablemente para la aplicación particular. Por ejemplo, el tiempo entre servicios que se puede obtener de forma realista para unos artículos de serie utilizados por el gran público, será probablemente superior al de una aplicación mejor controlada.

7.2.3.3 Para evitar los errores durante la especificación de los requisitos de seguridad de los E/E/PES, debe utilizarse un conjunto de técnicas y medidas apropiado de acuerdo con la tabla B.1.

7.3 Planificación de la validación de la seguridad de los E/E/PES

NOTA – Esta fase se representa por la etapa 9.2 de la figura 2. Se realizará normalmente en paralelo a las actividades de diseño y de desarrollo de los E/E/PES (véase al apartado 7.4).

7.3.1 Objetivo. El objetivo de los requisitos de este apartado es planificar la validación de la seguridad de los sistemas E/E/PE relacionados con la seguridad.

7.3.2 Requisitos

7.3.2.1 La planificación debe realizarse con el fin de especificar las etapas (tanto en términos de procedimiento como de técnica) que deben utilizarse para demostrar que los sistemas E/E/PE relacionados con la seguridad están de acuerdo con la especificación de los requisitos de seguridad de los E/E/PES (véase el apartado 7.2).

NOTA – Véase la Norma 61508-3 para el plan de validación del software.

7.3.2.2 La planificación de la validación de los sistemas E/E/PE relacionados con la seguridad debe tener en cuenta los siguientes elementos:

a) el conjunto de los requisitos definidos en la especificación de los requisitos de seguridad de los E/E/PES;

b) los procedimientos a aplicar para validar la puesta en marcha de cada función de seguridad así como los criterios de aceptación/rechazo para la realización de los ensayos;

c) los procedimientos a aplicar para validar la integridad de seguridad requerida para cada función de seguridad así como los criterios de aceptación/rechazo para la realización de los ensayos;

d) el entorno necesario para la realización de los ensayos, incluyendo el conjunto de herramientas y equipos calibrados necesarios;

e) los procedimientos de evaluación del ensayo (acompañados de las justificaciones correspondientes);

f) los procedimientos de ensayo y los criterios de prestación a aplicar para validar los niveles de inmunidad electromagnética especificados;

NOTA – La Norma CEI 61000-2-5 y la Norma CEI 61000-4 dan las directrices para la especificación de los niveles de ensayo de inmunidad.

g) estrategias de resolución de los fallos para la validación.

7.4 Diseño y desarrollo de los E/E/PES

NOTA – Esta fase se representa en la etapa 9.3 de la figura 2. Se realizará normalmente en paralelo con la planificación de la validación de la seguridad de los E/E/PES (véase el apartado 7.3).

7.4.1 Objetivo. El objetivo de los requisitos de este apartado es asegurar que el diseño y la puesta en marcha de los sistemas relacionados con la seguridad satisfacen los requisitos de las funciones de seguridad y de integridad de seguridad especificados (véase el apartado 7.2).

7.4.2 Requisitos generales

7.4.2.1 El diseño del sistema E/E/PE relacionado con la seguridad debe crearse de acuerdo con la especificación de los requisitos de seguridad de los E/E/PES (véase el apartado 7.2), teniendo en cuenta todos los requisitos del apartado 7.4.

7.4.2.2 El diseño del sistema E/E/PE relacionado con la seguridad (incluyendo la arquitectura del hardware y del software global, los sensores, los accionadores, la electrónica programable, el software integrado, el software de aplicación, etc.), véase la figura 4, debe satisfacer todos los requisitos de los puntos a) al c) siguientes:

a) los requisitos de integridad de seguridad del hardware que incluyen:

- las limitaciones de arquitectura relativas a la integridad de seguridad del hardware (véase el apartado 7.4.3.1), y
- los requisitos relativos a la probabilidad de fallos aleatorios peligrosos del hardware (véase el apartado 7.4.3.2);

b) los requisitos de integridad de seguridad de las anomalías sistemáticas, que incluyen:

- los requisitos para evitar los fallos (véase el apartado 7.4.4), y los requisitos para controlar las anomalías sistemáticas (véase el apartado 7.4.5), o
- la evidencia de que el equipo está "validado en uso" (véanse los apartados del 7.4.7.6 al 7.4.7.12);

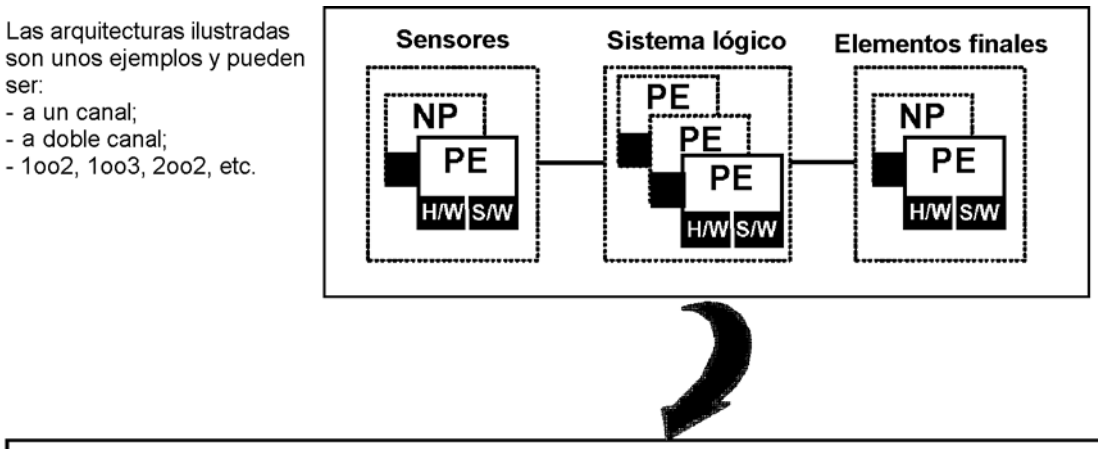
c) los requisitos relativos al comportamiento del sistema cuando se detecte una anomalía (véase el apartado 7.4.6).

NOTA 1 – Marco general de integridad de seguridad de los E/E/PES: el método general para elegir una aproximación de diseño que demuestre la obtención de un nivel de integridad de seguridad (a la vez para el hardware y la integridad de seguridad de las anomalías sistemáticas), en los sistemas E/E/PE relacionados con la seguridad, es el siguiente:

- determinar el nivel de integridad de seguridad (SIL)[1)] necesario de las funciones de seguridad (véanse las Normas CEI 61508-1 y CEI 61508-5);
- poner: integridad de seguridad del hardware = integridad de seguridad de las anomalías sistemáticas = SIL (véase el apartado 7.4.3.2.1);
- para lo que es la integridad de seguridad del hardware, determinar la arquitectura que cumple las limitaciones de la arquitectura (véase el apartado 7.4.3.1) y demostrar que las probabilidades de fallo de las funciones de seguridad, debidas a los fallos aleatorios del hardware, cumplen las medidas objetivo de fallo (véase el apartado 7.4.3.2);
- para lo que es la integridad de seguridad de las anomalías sistemáticas, elegir las características de diseño que controlan (toleran) las anomalías sistemáticas en explotación real (véase el apartado 7.4.5) o confirmar que los requisitos de "validación en uso" se cumplen (véanse los apartados del 7.4.7.6 al 7.4.7.12); y
- para lo que es la integridad de seguridad de las anomalías sistemáticas, elegir las técnicas y medidas que eviten (impidan la introducción de) anomalías sistemáticas durante el diseño y el desarrollo (véase el apartado 7.4.4) o confirmar que los requisitos de "validación en uso" se cumplen (véanse los apartados del 7.4.7.6 al 7.4.7.12).

NOTA 2 – La Norma CEI 61508-3 contiene unos requisitos relacionados con la arquitectura del software (véase el apartado 7.4.2.2), unos requisitos que permiten producir una especificación de ensayo de integración de la electrónica programable y del software (véase el apartado 7.5), y unos requisitos para integrar la electrónica programable y el software de acuerdo con esta especificación (véase el apartado 7.5). En todos los casos, es necesaria una cercana cooperación entre el desarrollador del sistema E/E/PE relacionado con la seguridad y del desarrollador del software.

1) Del inglés: "Safety Integrity Level".



Arquitectura de la electrónica programable		
Arquitectura del hardware de PE	**Arquitectura del software de PE (la arquitectura del software incluye el software integrado y el software de aplicación)**	
	Software integrado de PE	Software de aplicación de PE
Características generales y específicas de la aplicación en el hardware de PE Ejemplos: - ensayos de diagnóstico; - procesos redundantes; - tarjetas E/S duales.	Ejemplos: - conductores de comunicaciones - tratamiento de anomalías; - software supervisor.	Ejemplos: - funciones de entrada/salida; - funciones derivadas (tales como verificación del sensor si no proporciona el servicio del software integrado.

Leyenda

PE	**electrónica programable**
NP	**dispositivos no programables**
H/W	**hardware**
S/W	**software**
MooN	**M entre N (por ejemplo 1oo2 es 1 entre 2)**

Fig. 4 – Relación entre la arquitectura del hardware y del software de la electrónica programable

7.4.2.3 Cuando un sistema E/E/PE relacionado con la seguridad debe poner en marcha unas funciones de seguridad y unas funciones no relacionadas con la seguridad, cualquier hardware y software deben tratarse como unos elementos relacionados con la seguridad, excepto si se puede demostrar que la puesta en servicio de las funciones de seguridad y las funciones no relacionadas con la seguridad son suficientemente independientes (lo que significa que el fallo de cualquier función no relacionada con la seguridad no provoca un fallo peligroso de las funciones relacionadas con la seguridad). Se recomienda, en la medida de lo posible, separar las funciones relacionadas con la seguridad de las funciones no relacionadas con las seguridad.

NOTA 1 – Se establece una independencia suficiente de la puesta en servicio demostrando que la probabilidad de un fallo dependiente entre partes no relacionadas con la seguridad y partes relacionadas con la seguridad es suficientemente baja en relación con el nivel de integridad de seguridad más elevado asociado a las funciones de seguridad implicadas.

NOTA 2 – Conviene prestar particular atención si unas funciones que no son de seguridad se ponen en servicio en el mismo sistema E/E/PE relacionado con la seguridad. Aunque esté autorizado por esta norma, puede llevar a una mayor complejidad y la dificultad para conducir las actividades ligadas al ciclo de vida de los E/E/PES puede aumentar (por ejemplo, el diseño, la validación, la evaluación de la seguridad funcional y el mantenimiento).

7.4.2.4 Los requisitos para el hardware y el software deben determinarse por el nivel de integridad de seguridad de la función de seguridad que tenga el nivel de integridad de seguridad más alto, excepto si se puede demostrar que la puesta en servicio de las funciones de seguridad de diferentes niveles de integridad de seguridad es suficientemente independiente.

NOTA 1 – Se establece una independencia suficiente de la puesta en servicio demostrando que la probabilidad de un fallo dependiente entre las partes utilizando unas funciones de seguridad de niveles de integridad diferentes es suficientemente baja en relación al nivel de integridad de seguridad más alto asociado a las funciones de seguridad implicadas.

NOTA 2 – Cuando varias funciones de seguridad se realizan en un sistema E/E/PE relacionado con la seguridad, es necesario tener en cuenta la posibilidad de una anomalía única que puede provocar el fallo de varias funciones de seguridad. En tal caso, puede ser apropiado determinar los requisitos relativos al hardware y al software sobre la base del nivel de integridad de seguridad más alto que el asociado a una cualquiera de las funciones de seguridad, según el riesgo correspondiente a tal fallo.

7.4.2.5 Cuando la independencia entre las funciones de seguridad es necesaria (véanse los apartados 7.4.2.3 y 7.4.2.4), entonces deben documentarse durante el diseño los aspectos siguientes:

a) el método para lograr la independencia;

b) la justificación de este método.

7.4.2.6 Los requisitos relativos al software relacionado con la seguridad (véase la Norma CEI 61508-3) se deben poner a disposición del desarrollador del sistema E/E/PE relacionado con la seguridad.

7.4.2.7 El desarrollador del sistema E/E/PE relacionado con la seguridad debe revisar los requisitos del software y del hardware relacionados con la seguridad para asegurar que se especifican de forma apropiada. El desarrollador de los E/E/PES debe tener en cuenta los elementos siguientes:

a) funciones de seguridad;

b) requisitos de integridad de seguridad del sistema E/E/PE relacionado con la seguridad;

c) interfaces entre equipos y operador.

7.4.2.8 La documentación de diseño del sistema E/E/PE relacionado con la seguridad debe especificar las técnicas y las medidas necesarias durante las fases del ciclo de vida de la seguridad de los E/E/PES para obtener el nivel de integridad de seguridad.

7.4.2.9 La documentación de diseño del sistema E/E/PE relacionado con la seguridad debe justificar unas técnicas y medidas elegidas para constituir un conjunto integrado de acuerdo con el nivel de integridad de seguridad requerido.

NOTA – La adopción de una aproximación global utilizando una aprobación de tipo independiente de los sistemas E/E/PE relacionados con la seguridad (incluyendo los sensores, accionadores, etc.) para el hardware y el software, los ensayos de diagnóstico y las herramientas de programación y utilizando, en la medida de lo posible, unos lenguajes apropiados para el software, permite potencialmente reducir la complejidad técnica de la aplicación de los E/E/PES.

7.4.2.10 Durante las actividades de diseño y desarrollo, la importancia de todas las interacciones entre el hardware y el software (cuando sea apropiado) debe identificarse, evaluarse y documentarse.

7.4.2.11 El diseño debe basarse en una descomposición en subsistemas, teniendo cada subsistema un diseño y un conjunto de ensayos de integración especificados (véase el apartado 7.4.7).

NOTA 1 – Se puede considerar que un subsistema incluye un solo componente o un grupo cualquiera de componentes. Un sistema E/E/PE relacionado con la seguridad completo se constituye de un cierto número de subsistemas identificables y distintos que, cuando están juntos, realizan la función de seguridad considerada. Un subsistema puede estar constituido por varios canales. Véase el apartado 7.4.7.3.

NOTA 2 – Cada vez que sea posible, conviene utilizar unos subsistemas existentes y verificados para la realización. Esta posición sólo es válida si es posible conectar, casi al 100%, la funcionalidad, la capacidad y las características del subsistema existente con los nuevos requisitos, o bien si el subsistema verificado se estructura de tal forma que el usuario sea capaz de elegir solamente las funciones, las capacidades y las características necesarias para la aplicación específica. Unas funcionalidades, unas capacidades o unas características excesivas puede ir en detrimento de la seguridad del sistema, cuando el subsistema existente es de una complejidad demasiado grande, o presenta unas características no utilizadas, o si no es posible obtener la protección necesaria contra las funciones no deseadas.

7.4.2.12 Cuando un subsistema tiene salidas múltiples, es necesario determinar si varias combinaciones de los estados de salida, teniendo por origen eventual un fallo del sistema E/E/PE relacionado con la seguridad, pueden provocar un evento peligroso (determinado por el análisis de peligro y de riesgo, véase la Norma CEI 61508-1, apartado 7.4.2.10). Cuando esto ha sido establecido, es necesario considerar que el impedimento de esta combinación de estados de salidas es una función de seguridad explotada en modo de demanda alta/continua (véanse los apartados 7.4.6.3 y 7.4.3.2.5).

7.4.2.13 La devaluación (véase la Norma CEI 61508-7, apartado A.2.8) se debe utilizar tanto como sea posible para todos los componentes. Cualquier justificación para utilizar un componente cualquiera en sus límites debe documentarse (véase la Norma CEI 61508-1, capítulo 5).

NOTA – Cuando la devaluación es apropiada, conviene utilizar un factor de devaluación de al menos 0,67.

7.4.3 Requisitos de la integridad de seguridad del hardware

NOTA – El capítulo A.2 de la Norma CEI 61508-6 proporciona una vista general de las etapas necesarias durante la realización de la integridad de seguridad del hardware requerida y muestra como este capítulo guarda relación con otros requisitos de esta norma.

7.4.3.1 Limitaciones de la arquitectura sobre la integridad de seguridad del hardware

7.4.3.1.1 En el contexto de la integridad de seguridad del hardware, el nivel de integridad de seguridad más alto que se puede exigir para una función de seguridad dada está limitado por la tolerancia a las anomalías del hardware y la proporción de fallos en la seguridad (véase el anexo C) de los subsistemas que realizan la función de seguridad. Las tablas 2 y 3 especifican el nivel de integridad de seguridad más alta que se puede exigir para una función de seguridad que utiliza un subsistema, teniendo en cuenta la tolerancia a las anomalías del hardware y la proporción de fallos en seguridad (véase el anexo C) de este subsistema. Los requisitos de las tablas 2 y 3 deben aplicarse a cada subsistema que realice una función de seguridad y, en consecuencia, a cada parte del sistema E/E/PE relacionado con la seguridad; los apartados del 7.4.3.1.2 al 7.4.3.1.4 especifican cada una de las tablas 2 y 3 que se aplican a un subsistema particular. Los apartados del 7.4.3.1.5 y 7.4.3.1.6 especifican la forma en la que se deduce el nivel de integridad de seguridad más alto que puede ser exigido para una función de seguridad dada. Con respecto a estos requisitos:

a) una tolerancia a las anomalías del hardware N significa que N+1 anomalías pueden causar la pérdida de la función de seguridad. Durante la determinación de la tolerancia a las anomalías del hardware, ninguna otra medida puede controlar el efecto de las anomalías, los diagnósticos por ejemplo, no deben tenerse en cuenta; y

b) cuando una anomalía directamente da lugar a la aparición de una o varias anomalías subsecuentes, estas se consideran como una anomalía única;

c) durante la determinación de la tolerancia a la anomalía del hardware, ciertas anomalías pueden excluirse previendo que su probabilidad de ocurrencia sea muy baja en relación a los requisitos de integridad de seguridad del subsistema. Estas exclusiones de anomalías se deben justificar y documentar (véase la nota 3);

d) la proporción de fallos en seguridad de un subsistema se define por la relación del nivel medio de fallos en seguridad más los fallos peligrosos detectados al nivel de fallo medio total del subsistema (véase el anexo C).

NOTA 1 – Las limitaciones de la arquitectura se han incluido para obtener una arquitectura suficientemente robusta, teniendo en cuenta el nivel de complejidad del subsistema. El nivel de integridad de seguridad del hardware para el sistema E/E/PE relacionado con la seguridad, obtenido por aplicación de estos requisitos, es el máximo que se permite exigir aunque, en ciertos casos, un nivel de integridad superior teóricamente se podría calcular si se ha adoptado una aproximación únicamente matemática para el sistema E/E/PE relacionado con la seguridad.

NOTA 2 – La arquitectura y el subsistema obtenido para satisfacer los requisitos de tolerancia a las anomalías del hardware es el que se utiliza en las condiciones de funcionamiento normal. Se admite flexibilizar los requisitos de tolerancia de las anomalías cuando el sistema E/E/PE relacionado con la seguridad se está reparando en línea. Sin embargo, los parámetros claves relativos a cualquier flexibilidad eventual deben haber sido, previamente, evaluados (por ejemplo comparando el tiempo medio de restablecimiento a la probabilidad de una demanda).

NOTA 3 – Esto es necesario ya que si un componente tiene claramente una muy baja probabilidad de fallo a causa de propiedades inherentes en su diseño y en su construcción (por ejemplo la fuga de un accionador mecánico), normalmente no se considera como deseable de restringir (sobre la base de la tolerancia a las anomalías del hardware) la integridad de seguridad de una función de seguridad que utiliza este componente.

7.4.3.1.2 Un subsistema (véase la nota 1 del apartado 7.4.2.11) puede considerarse como del tipo A si, para los componentes necesarios en la realización de la función de seguridad:

a) los modos de fallo de todos los componentes que lo constituyen están bien definidos; y

b) el comportamiento del subsistema en unas condiciones de anomalías puede determinarse completamente; y

c) existe unos datos de fallo, obtenidos a partir de la experiencia sobre el terreno, suficientemente fiables como para apoyar los niveles de fallo exigidos relativos a unos fallos peligrosos detectados o no detectados (véanse los apartados 7.4.7.3 y 7.4.7.4).

7.4.3.1.3 Un subsistema (véase la nota 1 del apartado 7.4.2.11) se puede considerar como del tipo B si, para los componentes necesarios en la realización de la función de seguridad:

a) el modo de fallo de al menos uno de los componentes que lo constituyen no está bien definido; y

b) el comportamiento del subsistema en unas condiciones de anomalía no se puede determinar completamente; y

c) no existe, para el subsistema, ningún dato de fallo, obtenido a partir de la experiencia sobre el terreno suficientemente fiable como para apoyar los niveles de fallo exigidos relativos a unos fallos peligrosos detectados o no detectados (véanse los apartados 7.4.7.3 y 7.4.7.4).

NOTA – Esto significa que si al menos uno de los componentes del subsistema propiamente dicho satisface las condiciones aplicables a un subsistema de tipo B, en este caso, el subsistema debe ser del tipo B antes que del tipo A. Véase también el apartado 7.4.2.11, nota 1.

7.4.3.1.4 Las limitaciones de la arquitectura de la tabla 2 o de la tabla 3 deben aplicarse a cada subsistema que realice una función de seguridad de tal forma que:

a) los requisitos de tolerancia a las anomalías del hardware deben lograrse para el conjunto del sistema E/E/PE relacionado con la seguridad;

b) la tabla 2 se aplica a cada subsistema de tipo A que forma parte de los sistemas E/E/PE relacionados con la seguridad;

NOTA 1 – Si el sistema E/E/PE relacionado con la seguridad contiene únicamente subsistemas de tipo A, entonces los requisitos de la tabla 2 se aplicarán al conjunto del sistema E/E/PE relacionado con la seguridad.

c) la tabla 3 se aplica a cada subsistema de tipo B que forma parte de los sistemas E/E/PE relacionados con la seguridad;

NOTA 2 – Si el sistema E/E/PE relacionado con la seguridad contiene únicamente subsistemas de tipo B, los requisitos de la tabla 3 se aplicarán al conjunto del sistema relacionado con la seguridad.

d) las tablas 2 y 3 se aplicarán a los sistemas E/E/PE relacionados con la seguridad incluyendo a la vez los subsistemas de tipo A y de tipo B, dado que los requisitos de la tabla 2 deben aplicarse a los subsistemas de tipo A y los requisitos de la tabla 3 deben aplicarse a los subsistemas de tipo B.

Tabla 2
Integridad de seguridad del hardware: limitaciones de la arquitectura sobre los subsistemas relacionados con la seguridad de tipo A

Proporción de fallos en seguridad	Tolerancia a las anomalías del hardware (véase la nota 2)		
	0	1	2
< 60%	SIL1	SIL2	SIL3
60% – < 90%	SIL2	SIL3	SIL4
90% – < 99%	SIL3	SIL4	SIL4
≥ 99%	SIL3	SIL4	SIL4

NOTA 1 – Véanse los apartados del 7.4.3.1.1 al 7.4.3.1.4 para más detalles en cuanto a la interpretación de esta tabla.

NOTA 2 – Una tolerancia a las anomalías del equipo N significa que N + 1 anomalías puede causar la pérdida de la función de seguridad.

NOTA 3 – Véase el anexo C para los detalles relacionados con el cálculo de la proporción de los fallos en seguridad.

Tabla 3
Integridad de seguridad del hardware: limitaciones de la arquitectura sobre los subsistemas relacionados con la seguridad de tipo B

Proporción de fallos en seguridad	Tolerancia a las anomalías del hardware (véase la nota 2)		
	0	1	2
< 60%	No permitido	SIL1	SIL2
60% – < 90%	SIL1	SIL2	SIL3
90% – < 99%	SIL2	SIL3	SIL4
≥ 99%	SIL3	SIL4	SIL4

NOTA 1 – Véanse los apartados del 7.4.3.1.1 al 7.4.3.1.4 para más detalles en cuanto a la interpretación de esta tabla.

NOTA 2 – Una tolerancia a las anomalías del equipo N significa que N + 1 anomalías puede causar la pérdida de la función de seguridad.

NOTA 3 – Véase el anexo C para los detalles relacionados con el cálculo de la proporción de los fallos en seguridad.

7.4.3.1.5 En los sistemas E/E/PE relacionados con la seguridad en los que la función de seguridad se pone en marcha a través de un solo canal (como se muestra en la figura 5), el nivel de integridad de seguridad máximo del hardware que se puede exigir por la función de seguridad considerada, debe determinarse por el subsistema que satisface los requisitos de nivel de integridad de seguridad del hardware más bajo (determinado teniendo en cuenta las tablas 2 y 3).

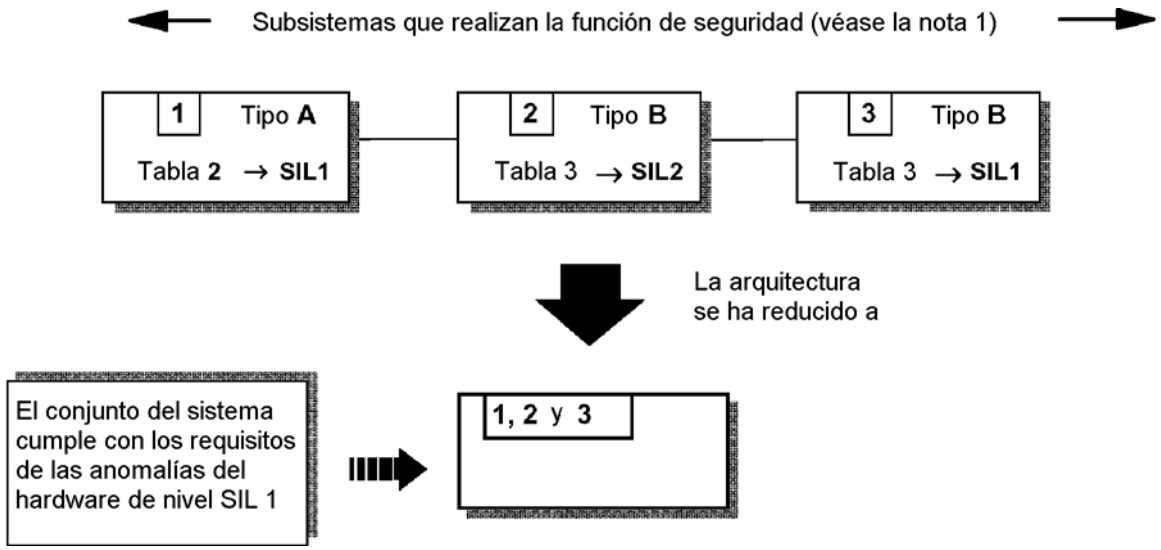
EJEMPLO: Suponiendo una arquitectura en la que una función de seguridad particular se realiza por un solo canal de los subsistemas, 1, 2 y 3 como muestra la figura 5 y los subsistemas satisfacen los requisitos de las tablas 2 y 3 de la manera siguiente:

– subsistema 1 cumple con los requisitos de tolerancia de las anomalías del hardware de un nivel SIL 1, para una proporción de fallos en seguridad especificada;

– subsistema 2 cumple con los requisitos de tolerancia de las anomalías del hardware de un nivel SIL 2, para una proporción de fallos en seguridad especificada;

– subsistema 3 cumple con los requisitos de tolerancia de las anomalías del hardware de un nivel SIL 3, para una proporción de fallos en seguridad especificada.

Para esta arquitectura particular, cada uno de los subsistemas 1 y 3 sólo es capaz de satisfacer los requisitos de tolerancia de las anomalías del hardware de nivel SIL1, mientras que el subsistema 2 es capaz de satisfacer los requisitos de tolerancia de las anomalías del hardware de nivel SIL2. Consecuentemente, los dos subsistemas 1 y 3 limitan el nivel de integridad de seguridad del hardware que se puede exigir, en términos de tolerancia a las anomalías del hardware, para la función de seguridad considerada, al nivel SIL1.



NOTA 1 – Los subsistemas que realizan la función de seguridad se extenderán sobre el conjunto del subsistema E/E/PE en términos de alcance, desde los sensores hasta los accionadores.

NOTA 2 – Para más detalles en cuanto a la interpretación de esta figura, véase el ejemplo del apartado 7.4.3.1.5.

Fig. 5 – Ejemplo de limitación de la integridad de seguridad del hardware para una función de seguridad de un solo canal

7.4.3.1.6 En los sistemas E/E/PE relacionados con la seguridad en los que una función de seguridad se pone en marcha a través de varios canales de subsistemas (como muestra la figura 6), el nivel de integridad de seguridad máxima del hardware que se puede exigir para la función de seguridad considerada, se debe determinar por:

a) la evaluación de cada subsistema en relación a los requisitos de la tabla 2 o 3 (como se especifica desde el apartado 7.4.3.1.2 al 7.4.3.1.4); y

b) agrupando los subsistemas por combinaciones; y

c) analizando estas combinaciones para determinar el nivel de integridad de seguridad global del hardware.

EJEMPLO: Se admite realizar el reagrupamiento y el análisis de las combinaciones de diversas formas. Para mostrar un método posible, se supone una arquitectura en la que una función de seguridad particular se realiza o bien por una combinación de subsistemas 1, 2 y 3, o bien por una combinación de subsistemas 4, 5 y 3, como se muestra en la figura 6. En este caso, la combinación de los subsistemas 1 y 2 y la combinación de los subsistemas 4 y 5 tienen la misma funcionalidad en términos de funciones de seguridad y contribuyen independientemente a proporcionar unos datos al subsistema 3. En este ejemplo, la combinación de subsistemas paralelos se basa en el hecho que cada subsistema realiza la función de seguridad requerida que le concierne independientemente del otro subsistema (paralelo). La función de seguridad se realizará:

– en caso de una anomalía, o bien en el subsistema 1, o bien en el subsistema 2 (ya que la combinación de los subsistemas 4 y 5 es capaz de asegurar la función de seguridad); o

– en caso de una anomalía o bien en el subsistema 4, o bien en el subsistema 5 (ya que la combinación de los subsistemas 1 y 2 es capaz de asegurar la función de seguridad).

Cada subsistema está de acuerdo con los requisitos de las tablas 2 y 3 de la forma siguiente:

– el subsistema 1 está de acuerdo con los requisitos de tolerancia a las anomalías del hardware de un nivel SIL3, para una proporción de fallos en seguridad especificada;

– el subsistema 2 está de acuerdo con los requisitos de tolerancia a las anomalías del hardware de un nivel SIL2, para una proporción de fallos en seguridad especificada;

– el subsistema 3 está de acuerdo con los requisitos de tolerancia a las anomalías del hardware de un nivel SIL2, para una proporción de fallos en seguridad especificada;

– el subsistema 4 está de acuerdo con los requisitos de tolerancia a las anomalías del hardware de un nivel SIL2, para una proporción de fallos en seguridad especificada;

– el subsistema 5 está de acuerdo con los requisitos de tolerancia a las anomalías del hardware de un nivel SIL1, para una proporción de fallos en seguridad especificada.

La determinación del nivel de integridad de seguridad máxima del hardware que se puede exigir, para el sistema E/E/PE relacionado con la seguridad completo, ejecutando la función de seguridad considerada, se detalla en las siguientes etapas:

a) Combinando los subsistemas 1 y 2: la tolerancia a las anomalías del hardware y la proporción de fallos en seguridad realizadas por combinación de los subsistemas 1 y 2 (cada uno estando separado de acuerdo con los requisitos de los niveles SIL1 y SIL2 respectivamente) cumpliendo con los requisitos del nivel SIL2 (determinado por el subsistema 2).

b) Combinando los subsistemas 4 y 5: la tolerancia a las anomalías del hardware y la proporción de fallos en seguridad realizadas por combinación de los subsistemas 4 y 5 (cada uno estando separado de acuerdo con los requisitos de los niveles SIL2 y SIL1 respectivamente) cumpliendo con los requisitos del nivel SIL1 (determinado por el subsistema 5).

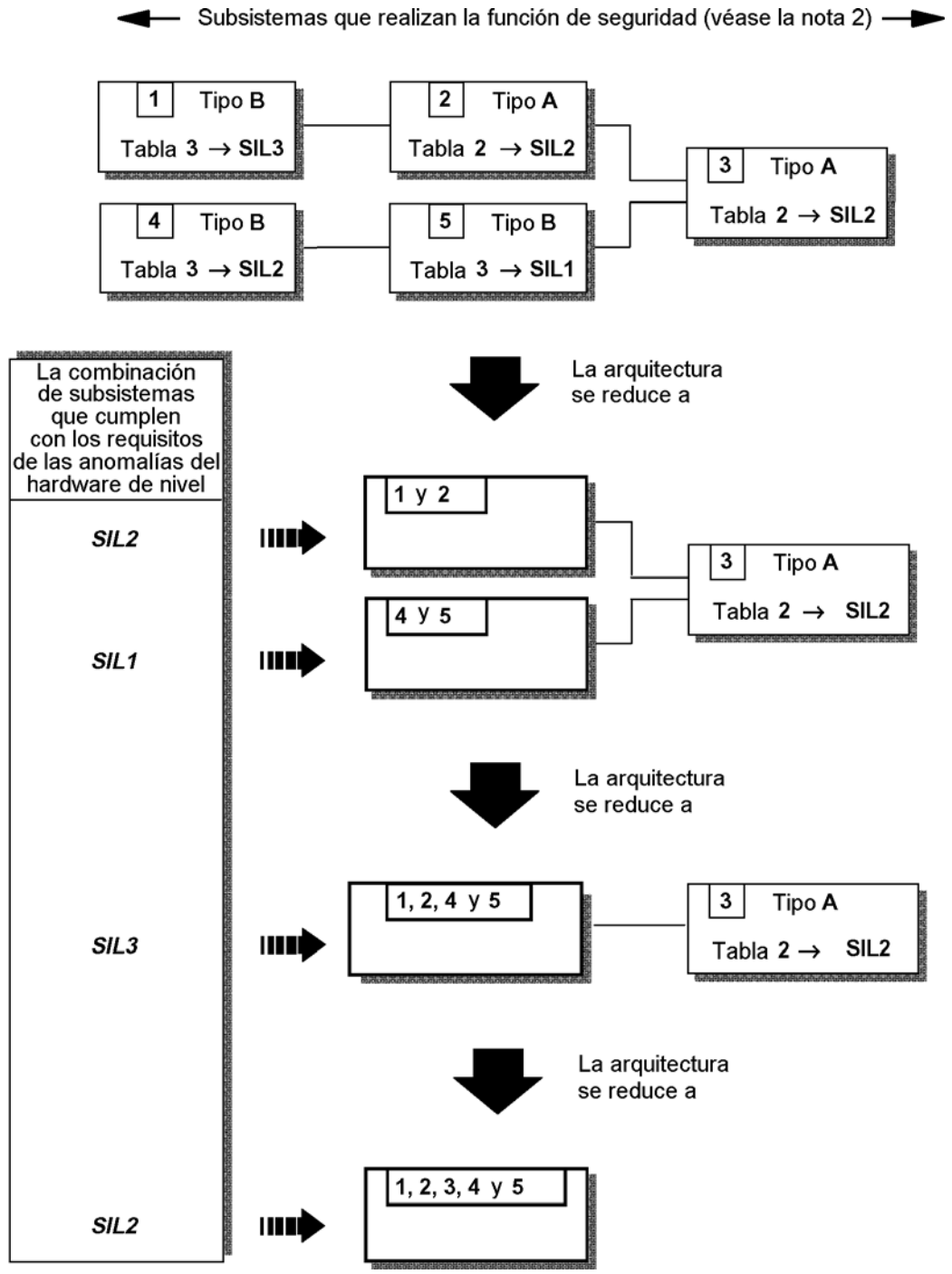
c) Combinando los subsistemas 1 y 2 con la combinación de los subsistemas 4 y 5: el nivel de integridad de seguridad del hardware, con respecto a la tolerancia a las anomalías del hardware, de la combinación de los subsistemas 1, 2, 4 y 5 se determina de la forma siguiente:

   – decidiendo la combinación de los subsistemas (es decir la combinación de los subsistemas 1 y 2 o la combinación de los subsistemas 4 y 5) que ha realizado el nivel de integridad de seguridad del hardware reivindicable más alto (en términos de cumplimiento con las tolerancias a las anomalías del hardware); y

   – analizando el efecto de otra combinación de subsistemas sobre la tolerancia a las anomalías del hardware por la combinación de subsistemas 1, 2, 4 y 5.

   En este ejemplo, la combinación de los subsistemas 1 y 2 tiene una reivindicación admisible máxima de nivel SIL2 (véase el apartado a) anterior) mientras que la combinación de los subsistemas 4 y 5 tiene una reivindicación máxima de nivel SIL1 (véase el apartado b) anterior). Sin embargo, en caso de una anomalía en la combinación de los subsistemas 1 y 2, la función de seguridad se podría asegurar por la combinación de los subsistemas 4 y 5. Para tener en cuenta este efecto, la tolerancia a las anomalías del hardware realizado por la combinación de los subsistemas 1 y 2 aumenta en 1. Aumentando 1 la tolerancia a las anomalías del hardware, aumenta también 1 el nivel de integridad de seguridad del hardware (véanse las tablas 2 y 3). En consecuencia, con respecto a la tolerancia a las anomalías del hardware y a la proporción de fallos en seguridad, la combinación de los subsistemas 1, 2, 4 y 5 tiene un nivel de integridad de seguridad del hardware reivindicable máximo SIL3 [es decir, el nivel de integridad de seguridad del hardware realizado por la combinación de los subsistemas 1 y 2 (que era SIL2) más 1].

d) El sistema E/E/PE relacionado con la seguridad completo: el nivel de integridad de seguridad del hardware, con respecto a la tolerancia a las anomalías del hardware, que se puede exigir para el sistema E/E/PE relacionado con la seguridad completo que pone en marcha la función de seguridad considerada, se determina analizando la combinación de los subsistemas 1, 2, 4 y 5 [que satisfacen los requisitos de tolerancia a las anomalías de nivel SIL3 (véase el apartado c)] así como el subsistema 3 (que satisface los requisitos de tolerancia a las anomalías de nivel SIL2). Es decir, el subsistema que satisface los requisitos de nivel de integridad de seguridad más bajo del hardware, en este caso, el subsistema 3, que determina el nivel de integridad de seguridad máximo del hardware para el conjunto del sistema E/E/PE relacionado con la seguridad. En consecuencia, en este ejemplo, el nivel de integridad de seguridad máxima del hardware, con respecto a la tolerancia a las anomalías del hardware, que se ha obtenido para el sistema relacionado con la seguridad poniendo en marcha la función de seguridad, es el nivel SIL2.



NOTA 1 – Los subsistemas 1 y 2 así como los subsistemas 3 y 4 tienen la misma funcionalidad en términos de realización de la función de seguridad y contribuyen independientemente a proporcionar datos al subsistema 3.

NOTA 2 – Los subsistemas que realizan la función de seguridad se extenderán al conjunto del sistema E/E/PE en términos de cobertura, de los sensores a los accionadores.

NOTA 3 – Para más detalles en cuanto a la interpretación de esta figura, véase el ejemplo en el apartado 7.4.3.1.6.

Fig. 6 – Ejemplo de limitación de la integridad de seguridad del hardware para una función de seguridad de varios canales

7.4.3.2 Requisitos relacionados con la estimación de la probabilidad de fallo de las funciones de seguridad debida a los fallos aleatorios del hardware

7.4.3.2.1 La probabilidad de fallo de cada función de seguridad, debida a los fallos aleatorios del hardware, calculada de acuerdo con los apartados 7.4.3.2.2 y 7.4.3.2.3 debe ser inferior o igual a la medida objetivo de fallo tal como especifica la especificación de los requisitos de seguridad (véase el apartado 7.2.3.2).

NOTA 1 – En el caso de una función de seguridad en modo de baja demanda, la medida objetivo de la fallo se expresa en términos de probabilidad media de fallo en ejecución, durante la demanda, la función por la cual se diseña, determinada por el nivel de integridad de seguridad de la función de seguridad (véase la Norma CEI 61508-1, tabla 2), excepto si un requisito, en la especificación de los requisitos de integridad de seguridad de los E/E/PES (véase el apartado 7.2.3.2), imponiendo a la función de seguridad cumplir una medida objetivo de fallo que un SIL especifica. Por ejemplo, cuando una medida objetivo de fallo de $1{,}5 \times 10^{-6}$ (probabilidad de fallo durante una demanda) se especifica con el fin de tener la reducción necesaria de riesgo, es necesario que la probabilidad de fallo de la función de seguridad, debida a los fallos aleatorios del hardware, sea inferior o igual a $1{,}5 \times 10^{-6}$ fallos peligrosos por hora.

NOTA 2 – En el caso de una función de seguridad en modo de alta demanda, la medida objetivo de la fallo se expresa en términos de probabilidad media de fallo en ejecución, durante la demanda, la función por la cual se diseña, determinada por el nivel de integridad de seguridad de la función de seguridad (véase la Norma CEI 61508-1, tabla 3), excepto si un requisito, en la especificación de los requisitos de integridad de seguridad de los E/E/PES (véase el apartado 7.2.3.2), imponiendo a la función de seguridad cumplir una medida objetivo de fallo que un SIL especifica. Por ejemplo, cuando una medida objetivo de fallo de $1{,}5 \times 10^{-6}$ (probabilidad de fallo durante una demanda) se especifica con el fin de tener la reducción necesaria de riesgo, es necesario que la probabilidad de fallo de la función de seguridad, debida a los fallos aleatorios del hardware, sea inferior o igual a $1{,}5 \times 10^{-6}$ fallos peligrosos por hora.

NOTA 3 – Con el fin de demostrar que esto se ha realizado, es necesario efectuar una predicción de fiabilidad para la función de seguridad correspondiente, utilizando la técnica apropiada (véase el apartado 7.4.3.2.2), y comparar el resultado a la medida objetivo de fallo en el requisito de integridad de seguridad, para una función de seguridad considerada (véase la Norma CEI 61508-1, tablas 2 y 3).

7.4.3.2.2 La probabilidad de fallo de cada función de seguridad, debida a los fallos aleatorios del hardware, se debe estimar teniendo en cuenta:

a) la arquitectura del sistema E/E/PE relacionado con la seguridad, ya que se relaciona con cada una de las funciones de seguridad considerada;

NOTA 1 – Esto implica decidir cuales son los modos de fallo de los subsistemas que están en configuración en serie (es decir, que todo fallo provoca el fallo de la función de seguridad correspondiente) y que son los modos de fallo que están en configuración paralela (es decir, que los fallos simultáneos son necesarios para provocar la fallo de la función de seguridad).

b) el nivel de fallo estimado de cada subsistema, en todos los modos susceptibles de provocar un fallo peligroso del sistema E/E/PE relacionado con la seguridad, los fallos se detectan por unos ensayos de diagnóstico (véanse los apartados 7.4.7.3 y 7.4.7.4);

c) el nivel de fallo estimado de cada subsistema, en todos los modos susceptibles de provocar un fallo peligroso del sistema E/E/PE relacionado con la seguridad, los fallos no se detectan por unos ensayos de diagnóstico (véanse los apartados 7.4.7.3 y 7.4.7.4);

d) la susceptibilidad a los fallos de causa común del sistema E/E/PE relacionado con la seguridad (véanse las notas 2 y 11);

NOTA 2 – Por ejemplo, véase el anexo D de la Norma CEI 61508-6.

e) la cobertura de diagnóstico de los ensayos periódicos de diagnóstico (determinada de acuerdo con el anexo C), y el intervalo correspondiente de los ensayos de diagnóstico;

NOTA 3 – El intervalo de los ensayos de diagnóstico y el tiempo de reparación que resulta constituyen, en conjunto, el tiempo medio hasta el restablecimiento que se tiene en cuenta en el modelo de fiabilidad. Del mismo modo, en el caso de un sistema E/E/PE relacionado con la seguridad explotado en modo de alta demanda/continua para el que cualquier fallo peligroso de un canal entraña un fallo peligroso del sistema E/E/PE relacionado con la seguridad, el intervalo de los ensayos de diagnóstico se tiene en cuenta directamente (es decir, se añade al tiempo de restablecimiento) en el modelo de fiabilidad, si no es de un orden de magnitud inferior al nivel de demanda medio (véase el apartado 7.4.3.2.5).

NOTA 4 – Determinando el intervalo de los ensayos de diagnóstico, los intervalos entre cada una de los ensayos que contribuyen a la cobertura de diagnóstico se tienen en cuenta.

f) los intervalos de tiempo a los que los ensayos periódicos se realizan para revelar los fallos peligrosos que no se detectan por los ensayos de diagnóstico;

g) los tiempos de reparación corresponden a los fallos detectados;

NOTA 5 – El tiempo de reparación constituye una parte del tiempo medio de restablecimiento (véase el VEI 191-13-08), que también debe incluir el tiempo pasado en la detección del fallo y todo periodo de tiempo durante el cual la reparación no es posible (véase la Norma CEI 61508-6, anexo B que proporciona un ejemplo de la forma siguiente en el que el tiempo medio de restablecimiento se puede utilizar para calcular la probabilidad de un fallo). En las situaciones en las que la reparación sólo se puede realizar en un periodo de tiempo especificado, por ejemplo cuando el EUC está parado y en estado seguro, es particularmente importante que el periodo de tiempo durante el cual ninguna reparación es posible se tenga en cuenta, especialmente cuando es relativamente largo.

h) la probabilidad de un fallo no detectada de un proceso cualquiera de comunicación de datos (véase la nota 11 y el apartado 7.4.8.1).

NOTA 6 – La Norma CEI 61508-6, anexo B, describe una aproximación simplificada que se puede utilizar para estimar la probabilidad de un fallo peligroso de una función de seguridad debido a un fallo aleatoria del hardware, con el fin de determinar que una arquitectura cumple la medida objetivo de fallo requerido.

NOTA 7 – La Norma CEI 61508-6, anexo A, capítulo A.2 proporciona una vista del conjunto de etapas necesario durante la realización de la integridad de seguridad del hardware requerido, y presenta la forma siguiente en la que este apartado está en relación con otros requisitos de esta norma.

NOTA 8 – Es necesario cuantificar separadamente, para cada función, la fiabilidad del sistema E/E/PE relacionado con la seguridad ya que diferentes modos de fallo de los componentes se aplican y la arquitectura de los sistemas E/E/PE relacionados con la seguridad (en términos de redundancia) puede también variar.

NOTA 9 – Un cierto número de métodos de modelización están disponibles y el analista debe determinar el más apropiado, en función de los casos. Los métodos disponibles son:

- análisis causa-consecuencia (véase el apartado B.6.6.2 de la Norma CEI 61508-7);
- análisis por árbol de fallos (véase el apartado B.6.6.5 de la Norma CEI 61508-7);
- modelos de Markov (véase el apartado C.6.4 de la Norma CEI 61508-7);
- diagramas de fiabilidad (véase el apartado C.6.5 de la Norma CEI 61508-7).

NOTA 10 – El tiempo medio de restablecimiento (véase VEI 191-13-08) tenido en cuenta en el modelo de fiabilidad necesita tener en cuenta el intervalo de los ensayos de diagnóstico, el tiempo de reparación y todos los otros retrasos previsibles en el restablecimiento.

NOTA 11 – Los fallos de causa común y las debidas a los procesos de comunicación de los datos pueden resultar de otros efectos que los fallos de los componentes del hardware (por ejemplo, perturbación electromagnética, errores de decodificación, etc.). De todos modos, estos fallos se consideran, para las necesidades de esta norma, como unas fallos aleatorios del hardware.

7.4.3.2.3 El intervalo de los ensayos de diagnóstico, para cada subsistema que tiene una tolerancia a las anomalías del hardware superior a cero, debe ser tal que el sistema E/E/PE relacionado con la seguridad pueda cumplir el requisito de probabilidad de fallo aleatorio del hardware (véase el apartado 7.4.3.2.1).

7.4.3.2.4 El intervalo de los ensayos de diagnóstico de cada subsistema que tiene una tolerancia a las anomalías del hardware nulo, la función de seguridad es completamente dependiente (véase la nota 1), y que realiza solamente las funciones de seguridad explotadas en modo de baja demanda, debe ser tal que el sistema E/E/PE relacionado con la seguridad pueda cumplir el requisito de probabilidad de fallo aleatorio del hardware (véase el apartado 7.4.3.2.1).

NOTA 1 – Se considera que una función de seguridad depende completamente de un subsistema si un fallo del subsistema provoca un fallo de la función de seguridad del sistema E/E/PE relacionado con la seguridad considerado, y que la función de seguridad no se ha asignado a otro sistema relacionado con la seguridad (véase el apartado 7.6 de la Norma CEI 61508-1).

NOTA 2 – Cuando es posible un cierto número de combinaciones de estados de salida de un subsistema provoque directamente un evento peligroso (determinado por el análisis de peligros y de riesgos, véase el apartado 7.4.2.10 de la Norma CEI 61508-1) y cuando la combinación de los estados de salida en presencia de una anomalía en el subsistema no se puede determinar (por ejemplo en el caso de subsistemas de tipo B), entonces es necesario considerar que la detección de anomalías peligrosas en el subsistema es una función de seguridad explotada en modo de demanda alta/continua y son aplicables los requisitos de los apartados 7.4.6.3 y 7.4.3.2.5.

7.4.3.2.5 El intervalo de ensayos de diagnóstico de cada subsistema que tiene una tolerancia a las anomalías del hardware nula, en el cual la función de seguridad es completamente dependiente (véase la nota 1) y que realiza una función de seguridad explotada en modo de demanda alta/continua (véase la nota 2), debe ser tal que la suma del intervalo de los ensayos de diagnóstico y del tiempo necesario de ejecución de la acción especificada (reacción a anomalías) pueda realizar o mantener un estado seguro [véase el punto g) del apartado 7.2.3.1] es inferior al tiempo de seguridad del proceso. El tiempo de seguridad del proceso se define como el periodo de tiempo entre la aparición de un fallo en el EUC o en el sistema de control del EUC (este fallo puede dar lugar a un evento peligroso) y la aparición del evento peligroso cuando la función de seguridad no se ha puesto en marcha.

NOTA 1 – Se considera que una función de seguridad depende completamente de un subsistema si el fallo del subsistema provoca el fallo de la función de seguridad en el sistema E/E/PE relacionado con la seguridad considerado, y que la función de seguridad no ha sido asignada a otro sistema relacionado con la seguridad (véase el apartado 7.6 de la Norma CEI 61508-1).

NOTA 2 – En el caso de un subsistema que realiza una función de seguridad particular para la que el informe del nivel de los ensayos de diagnóstico al nivel de demanda sobrepase 100, el subsistema se puede tratar como si realiza una función de seguridad en modo de baja demanda (véase el apartado 7.4.3.2.4), con tal que la función de seguridad no impida la combinación de estados de salida que conducen a un evento peligroso (véase la nota 3).

NOTA 3 – Si la función de seguridad consiste en impedir una combinación particular de estados de salida pudiendo ser el origen de un evento peligroso, siempre es necesario considerar que tal función de seguridad se explota en modo de demanda elevada/continua (véase el apartado 7.4.2.12).

7.4.3.2.6 Si, para un diseño particular, la medida objetivo de fallo del requisito de integridad de seguridad de la función de seguridad considerada no se cumple, entonces:

– determinar los componentes, subsistemas y/o parámetros críticos;

– evaluar el efecto de las posibles medidas de mejora sobre los componentes, subsistemas y/o parámetros críticos (por ejemplo, componentes más débiles, defensas suplementarias contra los fallos de modo común, cobertura de diagnóstico aumentada, redundancia aumentada, intervalo de ensayos periódicas reducido, etc.);

– elegir y llevar a cabo las mejoras aplicables;

– repetir las etapas necesarias para determinar la nueva probabilidad de fallo del hardware.

7.4.4 Requisitos para evitar los fallos

NOTA – Los apartados del 7.4.4.1 al 7.4.4.6 no son aplicables en el caso de un subsistema que cumple los requisitos que permiten considerarlo como “válido en utilización” (véase del apartado 7.4.7.6 al 7.4.7.12).

7.4.4.1 Un conjunto conveniente de técnicas y medidas debe diseñarse y utilizarse para evitar la introducción de anomalías durante el diseño y el desarrollo de los E/E/PES del sistema E/E/PE relacionado con la seguridad (véase la tabla B.2).

7.4.4.2 De acuerdo con el nivel de integridad de seguridad exigido, el método de diseño elegido incluye unas disposiciones que facilitan:

a) la transparencia, la modularidad y las otras características que permiten controlar la complejidad;

b) una expresión clara y precisa de:

   – la funcionalidad,

   – las interfaces de los subsistemas,

   – la secuencia y de las informaciones temporales,

   – la simultaneidad y de la sincronización de ejecución;

c) un documento claro y preciso así como la comunicación de informaciones;

d) la verificación y la validación.

7.4.4.3 Los requisitos de mantenimiento destinados a asegurar el mantenimiento de la integridad de seguridad de los sistemas E/E/PE relacionados con la seguridad al nivel requerido, se deben formalizar durante la etapa de diseño.

7.4.4.4 Cuando sea aplicable, deben utilizarse las herramientas de ensayos automáticos y de las herramientas de desarrollo integradas.

7.4.4.5 Durante el diseño, los ensayos de integración de los E/E/PES deben planificarse. La documentación del programa de ensayos debe incluir:

a) los tipos de ensayos a realizar así como los procedimientos a seguir;

b) el entorno, las herramientas, la configuración y los programas de ensayo;

c) los criterios de aceptación/rechazo de los ensayos.

7.4.4.6 Durante el diseño, es necesario separar las actividades que pueden realizarse en los locales del desarrollador y las que necesitan un acceso al sitio del usuario.

7.4.5 Requisitos para el control de las anomalías sistemáticas

NOTA – Los apartados del 7.4.5.1 al 7.4.5.3 no son aplicables en el caso en el que un subsistema que cumple los requisitos que permiten considerarlo como "válido en utilización" (véase del apartado 7.4.7.6 al 7.4.7.12).

7.4.5.1 Con el fin de controlar las anomalías sistemáticas, el diseño de los E/E/PES debe tener unas características de diseño tales que los sistemas E/E/PE relacionados con la seguridad sean tolerantes a:

a) anomalías de diseño residuales del hardware, excepto si la eventualidad de las anomalías de diseño del hardware se puede excluir (véase la tabla A.16);

b) limitaciones del entorno, incluyendo las perturbaciones electromagnéticas (véase la tabla A.17);

c) errores imputables al operario del EUC (véase la tabla A.18);

d) anomalías de diseño residuales del software (véase el apartado 7.4.3 de la Norma CEI 61508-3 así como la tabla correspondiente);

e) errores y otros efectos que provienen de un proceso de comunicación de datos (véase el apartado 7.4.8).

7.4.5.2 La mantenibilidad y la probabilidad deben tenerse en cuenta durante las actividades de diseño y desarrollo para facilitar la puesta en marcha de estas propiedades en los sistemas E/E/PE finales relacionados con la seguridad.

7.4.5.3 El diseño de los sistemas relacionados con la seguridad deben tener en cuenta las aptitudes y los limites humanos y debe convenir a las acciones atribuidas a los operarios y al personal encargado del mantenimiento. El diseño de todas las interfaces debe seguir las buenas prácticas en términos de factor humano y debe adaptarse al nivel probable de formación y de conocimiento de los operarios como, por ejemplo, en el caso de sistemas E/E/PE relacionados con la seguridad de serie destinados al gran público, en donde el operario es un miembro del público.

NOTA 1 – Se recomienda que el objetivo del diseño sea prevenir o eliminar, en la medida de lo posible, los errores humanos críticos previsibles imputables a los operarios o al personal de mantenimiento o que la acción necesite una confirmación secundaria antes de la finalización.

NOTA 2 – Se admite que ciertos errores debidos a los operarios o al personal de mantenimiento no sean recuperables por los sistemas E/E/PE relacionados con la seguridad, por ejemplo, si no son detectables o recuperables de forma realista si no es por inspección directa, tales como ciertos fallos mecánicos del EUC.

7.4.6 Requisitos de comportamiento del sistema, durante la detención de una anomalía

7.4.6.1 La detección de una anomalía peligrosa (por los ensayos de diagnóstico, los ensayos periódicos o cualquier otro medio) en un subsistema que tiene una tolerancia a las anomalías del hardware superior a cero debe lanzar:

a) o bien una acción especificada para alcanzar o mantener un estado seguro (véase la nota), o

b) o bien el aislamiento de la parte del subsistema que presenta la anomalía con el fin de permitir la continuidad de la seguridad de la explotación del EUC, mientras que la parte que presenta la anomalía se repara. Si la reparación no se completa durante el tiempo medio hasta el restablecimiento (MTTR) tomado como hipótesis en el cálculo de la probabilidad de fallo aleatorio del hardware (véase el apartado 7.4.3.2.2), debe tener lugar una acción especificada con el fin de alcanzar o mantener un estado seguro (véase la nota).

NOTA – La acción especificada (reacción a anomalías) requerida para alcanzar o mantener un estado seguro debe especificarse en los requisitos de seguridad de los E/E/PES (véase el apartado 7.2.3.1). Puede consistir, por ejemplo, en la parada de seguridad del EUC, o de la parte del EUC en la que se basa, en lo relativo a la reducción de riesgo, el subsistema que presenta una anomalía.

7.4.6.2 La detección de una anomalía peligrosa (por los ensayos de diagnóstico, los ensayos periódicos o cualquier otro medio) en un subsistema que tiene una tolerancia a las anomalías del hardware nula, y el cual es completamente dependiente de una función de seguridad (véase la nota 1), debe en el caso en el que este subsistema es utilizado únicamente por una (unas) función (es) de seguridad en explotación en modo de baja demanda, lanzar:

a) o bien una acción especificada para alcanzar o mantener un estado seguro;

b) o bien la reparación del subsistema que presenta una anomalía, en el intervalo de tiempo medio hasta el restablecimiento tomando como hipótesis el cálculo de la probabilidad de fallo aleatorio del hardware (véase el apartado 7.4.3.2.2). Durante este intervalo, la seguridad del EUC debe estar asegurada por las medidas y limitaciones suplementarias. La reducción de riesgo proporcionada por estas medidas y limitaciones debe ser al menos igual a la reducción de riesgo proporcionada por el sistema E/E/PE relacionado con la seguridad en ausencia de cualquier anomalía. Las medidas y limitaciones suplementarias se deben especificar en los procedimientos de explotación y de mantenimiento de los E/E/PES (véase el apartado 7.6). Si la reparación no se realiza en el intervalo de tiempo medio hasta el restablecimiento (MTTR), entonces debe realizarse una acción especificada para alcanzar o mantener un estado seguro (véase la nota 2).

NOTA 1 – Se considera que una función de seguridad depende completamente de un subsistema si un fallo del subsistema provoca un fallo de la función de seguridad en el sistema E/E/PE relacionado con la seguridad considerado, y que la función de seguridad no ha sido asignada a otro sistema relacionado con la seguridad (véase el apartado 7.6 de la Norma CEI 61508-1).

NOTA 2 – La acción especificada (reacción a anomalías) requerida para alcanzar o mantener un estado seguro debe especificarse en los requisitos de seguridad de los E/E/PES (véase el apartado 7.2.3.1). Puede consistir, por ejemplo, en la parada de seguridad del EUC, o de la parte del EUC en la que se basa, en lo relativo a la reducción de riesgo, el subsistema que presenta una anomalía.

7.4.6.3 La detección de una anomalía peligrosa (por los ensayos de diagnóstico, los ensayos periódicos o cualquier otro medio) en un subsistema que tiene una tolerancia a las anomalías del hardware nula, y el cual es completamente dependiente de una función de seguridad (véase la nota 1), debe en el caso en el que un subsistema que realiza una(s) función(es) de seguridad en explotación en modo de alta demanda o continua (véanse las notas 2 y 3), lanzar una acción específica para alcanzar o mantener un estado seguro (véase la nota 3).

NOTA 1 – Se considera que una función de seguridad depende completamente de un subsistema si un fallo del subsistema provoca un fallo de la función de seguridad en el sistema E/E/PE relacionado con la seguridad considerado, y que la función de seguridad no ha sido asignada a otro sistema relacionado con la seguridad (véase el apartado 7.6 de la Norma CEI 61508-1).

NOTA 2 – Cuando haya la posibilidad que una cierta combinación de estados de salida de un subsistema provoque directamente un evento peligroso (como el determinado por el análisis de peligros y riesgos, véase el apartado 7.4.2.12) y cuando la combinación de los estados de salida en presencia de una anomalía en un subsistema no se pueda determinar (por ejemplo en el caso de subsistemas de tipo B), entonces es necesario considerar que la detección de anomalías peligrosas en el subsistema es una función de seguridad explotada en modo de alta demanda o continua y son aplicables los requisitos de los apartados 7.4.6.3 y 7.4.3.2.5).

NOTA 3 – La acción especificada (reacción a anomalías) requerida para alcanzar o mantener un estado seguro debe especificarse en los requisitos de seguridad de los E/E/PES (véase el apartado 7.2.3.1). Puede consistir, por ejemplo, en la parada de seguridad del EUC, o de la parte del EUC en la que se basa, en lo relativo a la reducción de riesgo, el subsistema que presenta una anomalía.

7.4.7 Requisitos de realización de los E/E/PES

7.4.7.1 Los sistemas E/E/PE relacionados con la seguridad deben realizarse de acuerdo con el diseño de los E/E/PES.

7.4.7.2 Todos los subsistemas que son utilizados por una función de seguridad al menos deben estar identificados y documentados como los subsistemas relacionados con la seguridad.

7.4.7.3 Las informaciones siguientes deben estar disponibles para cada subsistema relacionado con la seguridad (véase también el apartado 7.4.7.4):

a) especificación funcional de las funciones e interfaces del subsistema que pueden ser utilizados por las funciones de seguridad;

b) nivel de fallo estimado (debido a los fallos aleatorios del hardware) en todos los modos susceptibles de provocar un fallo peligroso del sistema E/E/PE relacionado con la seguridad que se detectan por los ensayos de diagnóstico (véase el apartado 7.4.7.4);

c) nivel de fallo estimado (debido a los fallos aleatorios del hardware) en todos los modos susceptibles de provocar un fallo peligroso del sistema E/E/PE relacionado con la seguridad que no se detectan por los ensayos de diagnóstico (véase el apartado 7.4.7.4);

d) las limitaciones relativas al entorno del subsistema conviene observarlas con el fin de mantener la validez de los niveles de fallo estimados debidos a los fallos aleatorios del hardware;

e) las limitaciones relativas al tiempo de vida del subsistema que conviene no sobrepasar con el fin de mantener la validez de los niveles de fallo estimados debidos a los fallos aleatorios del hardware;

f) los ensayos periódicos y/o los requisitos de mantenimiento;

g) la cobertura de diagnóstico deducida de acuerdo con el anexo C (cuando sea requerida, véase la nota 1);

h) el intervalo de los ensayos de diagnóstico (cuando sea requerido véase la nota 1);

NOTA 1 – Los puntos g) y h) anteriores se refieren a los ensayos de diagnóstico que son internos al subsistema. Las informaciones correspondientes se requieren únicamente en el modelo de fiabilidad del sistema E/E/PE relacionado con la seguridad, los ensayos de diagnóstico se anuncian como estando ejecutados en el subsistema considerado (véase el apartado 7.4.3.2.2).

i) las informaciones suplementarias (por ejemplo, los tiempos de reparación) que son necesarias para deducir el tiempo de restablecimiento (MTTR) a continuación de la detección de una anomalía por los diagnósticos;

NOTA 2 – Los puntos del b) al i) son necesarios para permitir la estimación de la probabilidad de fallo en demanda, o de la probabilidad de fallo por hora, de la función de seguridad (véase el apartado 7.4.3.2.2).

NOTA 3 – Los puntos b), c), g) h) e i) se requieren sólo como parámetros separadores para los subsistemas tales como sensores y accionadores que se pueden combinar en las arquitecturas redundantes con el fin de mejorar la integridad de seguridad del hardware. Para los elementos cuyas unidades lógicas no serán combinadas en las arquitecturas redundantes relacionadas con la seguridad, se acepta que el rendimiento se especifique en términos de probabilidad de fallo en demanda, o probabilidad de fallo por hora, teniendo en cuenta los puntos b), c), g), h) e i). Para dichos elementos también es necesario establecer el intervalo de ensayos periódicos para los fallos no detectados por los ensayos de diagnóstico.

j) las informaciones necesarias para deducir la proporción de fallo en seguridad (SFF) del subsistema como el aplicado al sistema E/E/PE relacionado con la seguridad, determinado de acuerdo con el anexo C;

k) la tolerancia a las anomalías del hardware, para el subsistema;

NOTA 4 – Los puntos j) y k) son necesarios para determinar el nivel más alto de integridad de seguridad que puede predecirse por una función de seguridad, teniendo en cuenta las limitaciones de la arquitectura (véase le apartado 7.4.3.1).

l) las aplicaciones relativas a la aplicación del subsistema que convienen observar con el fin de evitar fallos sistemáticos;

m) el nivel de integridad más alto que se puede predecir para una función de seguridad que utiliza el subsistema, sobre la base de:

- medidas y técnicas utilizadas para impedir la introducción de anomalías sistemáticas durante el diseño y la realización del hardware y del software del subsistema (véanse los apartados 7.4.4.1 y 7.4 de la Norma CEI 61508-3),

- las características de diseño que hacen el subsistema tolerante a las anomalías sistemáticas (véase el apartado 7.4.5.1);

NOTA 5 – Esto no se requiere en el caso de los subsistemas que se consideran como validados en uso (véase el apartado 7.4.7.5).

n) las informaciones necesarias para identificar las configuraciones del hardware y del software con el fin de permitir la gestión de la configuración del sistema E/E/PE relacionado con la seguridad, de acuerdo con el apartado 6.2.1 de la Norma CEI 61508-1;

o) la evidencia documental de que el subsistema ha sido validado.

7.4.7.4 Los niveles de fallo estimados, debidos a los fallos aleatorios del hardware, para los subsistemas [véanse los puntos b) y c) del apartado 7.4.7.3] pueden determinarse

a) o bien por un análisis de los modos de fallos y de los efectos del diseño utilizando unos niveles de fallo de los componentes que provienen de un origen industrial reconocido;

NOTA 1 – Conviene que todos los datos utilizados relativos a los fallos tengan un nivel de confianza del al menos un 70%. La determinación estadística del nivel de confianza se define en la Publicación IEEE 352. Un término equivalente , nivel de significación, se utiliza en la Norma CEI 61164.

NOTA 2 – Si los datos relativos a la localización de los fallos específicos del hardware están disponibles, es preferible utilizarlas. Si este no es el caso, pueden utilizarse unos datos genéricos.

NOTA 3 – Aunque se tome como hipótesis un nivel de fallo constante para la mayor parte de las estimaciones estadísticas, esto se aplica solamente si el tiempo de vida útil de los componentes no se ha sobrepasado. Más allá de su tiempo de vida útil (es decir, cuando la probabilidad de fallo aumenta en función del tiempo), los resultados de la mayoría de los métodos de cálculo probabilístico son menos significantes. Esto es porque conviene que cualquier estimación probabilística incluya una especificación del tiempo de vida útil de los componentes. El tiempo de vida útil depende fuertemente del propio componente, y de sus condiciones de utilización - la temperatura en particular (por ejemplo los condensadores electrolíticos pueden ser muy sensibles). La experiencia a permitido mostrar que el tiempo de vida útil a menudo se sitúa entre 8 y 12 años. De todos modos, puede ser significativamente menor si los componentes se utilizan en condiciones próximas a sus límites de especificación. Los componentes que tengan unos tiempos de vida útil más largos tienen tendencia a ser considerablemente más caros.

b) o bien por experiencia de un uso anterior del subsistema en un entorno similar (véase el apartado 7.4.7.9).

7.4.7.5 En el caso de un subsistema considerado como validado en uso (véase el apartado 7.4.7.6), no se describen las informaciones relativas a las técnicas y medidas para la prevención y el control de las anomalías sistemáticas [véase el punto m) del apartado 7.4.7.3].

7.4.7.6 Un subsistema desarrollado anteriormente debe considerarse como validado en uso cuando tiene una funcionalidad claramente restringida y cuando existe una evidencia documentada apropiada, basada en el uso anterior de una configuración específica del subsistema (durante el cual todos los tiempos de fallo se han registrado formalmente, véase el apartado 7.4.7.10) que tiene en cuenta todos los análisis o ensayos suplementarios, como se requiere (véase el apartado 7.4.7.8). La evidencia documental debe mostrar que la probabilidad de fallo del subsistema (debido a un fallo aleatorio del hardware y a las anomalías sistemáticas), en el sistema E/E/PE relacionado con la seguridad, es suficientemente baja para que el (los) nivel (es) de integridad de seguridad requerido(s), para la (las) función(es) de seguridad que utiliza(n) el subsistema, sea(n) alcanzado(s).

7.4.7.7 La evidencia documental requerida en el apartado 7.4.7.6 debe demostrar que las condiciones de uso anteriores (véase la nota) del subsistema especificado son las mismas, o suficientemente próximas, que las que se encuentra el subsistema en el sistema E/E/PE relacionado con la seguridad, con el fin de determinar que la probabilidad de cualquier anomalía sistemática no revelado es suficientemente bajo para que el (los) nivel(es) de integridad de seguridad requerido(s), para la función de seguridad que utiliza en subsistema, sea(n) alcanzado(s).

NOTA – Las condiciones de uso (perfil de explotación) incluyen todos los factores que pueden influenciar la probabilidad de anomalías sistemáticas en el hardware y el software del subsistema. Por ejemplo, el entorno, los modos de utilización, las funciones completas, la configuración, las interfaces con otros sistemas, el sistema de explotación, el compilador, los factores humanos.

7.4.7.8 Cuando existe una diferencia entre las condiciones de uso anteriores y las del subsistema en el sistema E/E/PE relacionado con la seguridad, se debe identificar y realizar una demostración explícita, sobre la base de una combinación de métodos analíticos apropiados y de ensayos, con el fin de determinar que la probabilidad de una anomalía sistemática no revelado es suficientemente bajo para que el(los) nivel(es) de integridad de seguridad de la(s) funciones de seguridad que utiliza(n) este subsistema sea(n) alcanzado(s).

7.4.7.9 La evidencia documental requerida en el apartado 7.4.7.6 debe establecer que la extensión de la utilización anterior (en términos de horas de explotación) de la configuración especificada del subsistema es suficiente para soportar los niveles de fallo predecidos sobre una base estadística. Como mínimo, es necesario un tiempo de explotación suficiente para establecer que los datos relativos a los niveles de fallo predecidos tienen un límite inferior de confianza, unilateralmente, al 70% (véase el anexo D de la Norma CEI 61508-7, y la Publicación IEEE 352). No debe tenerse en cuenta, para un subsistema individual, un tiempo inferior a un año, en el tiempo de explotación total, por el análisis estadístico (véase la nota).

NOTA – El tiempo necesario, en términos de horas de explotación, requerido para obtener los niveles de fallo predecidos puede resultar de la explotación de un cierto número de subsistemas idénticos, si los fallos de todos los subsistemas han sido efectivamente detectadas y registradas (véase el apartado 7.4.7.10). Si, por ejemplo, 100 subsistemas están libres de fallos durante 10 000 h, el tiempo de explotación total libres de fallos se considera igual a 1 000 000 h. En este caso, cada subsistema ha sido utilizado durante un año y el conjunto de horas transcurridas en explotación se tiene en cuenta en el tiempo de explotación total.

7.4.7.10 Sólo los usos anteriores para los cuales todos los fallos del subsistema han sido efectivamente detectadas y registradas (por ejemplo, cuando los datos relativos a los fallos se han recogido de acuerdo con las recomendaciones de la Norma CEI 60300-3-2) deben tenerse en cuenta para determinar si se cumplen los requisitos anteriores (apartados del 7.4.7.6 al 7.4.7.9).

7.4.7.11 Deben tenerse en cuenta los factores siguientes para determinar si se cumplen los requisitos anteriores (apartados del 7.4.7.6 al 7.4.7.9), tanto en términos de cobertura como en grado de detalle de la información disponible (véase también el apartado 4.1 de la Norma CEI 61508-1):

a) la complejidad del subsistema;

b) la contribución del subsistema a la reducción de riesgo;

c) las consecuencias asociadas a un fallo del subsistema;

d) el aspecto innovador del diseño.

7.4.7.12 Conviene que la aplicación de un subsistema relacionado con la seguridad validado en uso, en el sistema E/E/PE relacionado con la seguridad se restrinja a las funciones e interfaces del subsistema que cumple los requisitos apropiados (véanse los apartados del 7.4.7.6 al 7.4.7.10).

NOTA – Las medidas de los apartados del 7.4.7.4 al 7.4.7.12 también son aplicables para los subsistemas que contienen software. En este caso, es necesario asegurar que el subsistema sólo ejecuta, en su aplicación de seguridad, la función para la cual se da la previsión del nivel de integridad de seguridad. Véase también el apartado 7.4.2.11 de la Norma CEI 61508-3.

7.4.8 Requisitos relativos a las comunicaciones de datos

7.4.8.1 Cuando una forma cualquiera de comunicación de datos se utiliza en la realización de una función de seguridad, la probabilidad de fallo de la función de seguridad debido al proceso de comunicación debe estimarse teniendo en cuenta los errores de transmisión, las repeticiones, las supresiones, las inserciones, las modificaciones de la secuencia, la corrupción, el retraso y la ocultación (véase también el apartado 7.4.8.2). Esta probabilidad debe tenerse en cuenta durante la estimación de la probabilidad de fallos peligrosos de la función de seguridad, debido a un fallo aleatorio del hardware (véase el apartado 7.4.3.2.2).

NOTA – El término ocultación significa que el contenido exacto de un mensaje no se identifica correctamente. Por ejemplo, un mensaje que proviene de un componente que no es de seguridad se identifica incorrectamente como un mensaje que proviene de un componente de seguridad.

7.4.8.2 En particular, los siguientes parámetros deben tenerse en cuenta para estimar la probabilidad de fallo de la función de seguridad debido al proceso de comunicación:

a) el nivel de error residual (véase VEI 371-08-05);

b) el nivel de pérdida de información (véase VEI 371-08-09);

c) los límites y la variabilidad de la velocidad de transferencia de la información (relación binaria);

d) los límites, y la variabilidad, del tiempo de retardo debido a la propagación de la información.

NOTA 1 – Puede demostrarse que la probabilidad de un fallo peligroso (por hora) es igual al cociente de la probabilidad de error residual por la longitud del mensaje (en bits) multiplicado por la velocidad de transmisión en el bus de los mensajes relacionados con la seguridad así como por un factor de 3600.

NOTA 2 – Las informaciones complementarias figuran en la Norma CEI 60870-5-1 y en las Normas EN 50159-1 y EN 50159-2.

7.5 Integración de los E/E/PES

NOTA – Esta fase se representa en la etapa 9.4 de la figura 2.

7.5.1 Objetivo. El objetivo de los requisitos de este apartado es integrar y someter los sistemas E/E/PE relacionados con la seguridad a los ensayos de integración.

7.5.2 Requisitos

7.5.2.1 Los sistemas E/E/PE relacionados con la seguridad deben integrarse de acuerdo con el diseño E/E/PES especificado y deben someterse a los ensayos de acuerdo con los ensayos de integración de los E/E/PES especificados (véase el apartado 7.4.2.11).

7.5.2.2 En el marco de la integración de todos los módulos en los sistemas E/E/PE relacionados con la seguridad, los sistemas E/E/PE relacionados con la seguridad deben someterse a los ensayos como se especifica (véase el apartado 7.4). Estos ensayos deben demostrar que todos los módulos interaccionan de forma correcta para cumplir sus funciones previstas y que se diseñan de forma que no realicen funciones no previstas.

NOTA 1 – Esto no implica someter a los ensayos a todas las combinaciones de entrada. Puede ser suficiente someter a los ensayos a todas las clases de equivalencia (véase el apartado B.5.2 de la Norma CEI 61508-7). Se admite que el número de casos de ensayo se pueda reducir a un nivel aceptable por un análisis estático (véase el apartado B.6.4 de la Norma CEI 61508-7), un análisis dinámico (véase el apartado B.6.5 de la Norma CEI 61508-7) o un análisis de los fallos (véase el apartado B.6.6 de la Norma CEI 61508-7). Cuando el desarrollo se realiza de acuerdo con las reglas que dan lugar a un diseño estructurado (véase el apartado B.3.2 de la Norma CEI 61508-7) o según los métodos semiformales (véase el apartado B.2.3 de la Norma CEI 61508-7) los requisitos son más fáciles que cuando este no es el caso.

NOTA 2 – Cuando el desarrollo se realiza según los métodos formales (véase el apartado B.2.2 de la Norma CEI 61508-7) o utilizando los ensayos o declaraciones formales (véanse los apartados C.5.13 y C.3.3 de la Norma CEI 61508-7), se admite que el campo de aplicación de estos ensayos sea reducido.

NOTA 3 – También se admite utilizar los ensayos estáticos (véase el apartado B.5.3 de la Norma CEI 61508-7).

7.5.2.3 La integración del software relacionado con la seguridad en el PES se debe realizar de acuerdo con el apartado 7.5 de la Norma CEI 61508-3.

7.5.2.4 La documentación apropiada de los ensayos de integración de los sistemas E/E/PE relacionados con la seguridad debe producirse, indicando los resultados de los ensayos y precisando la conformidad a los objetivos y criterios especificados durante la fase de diseño y desarrollo. En caso de fallo, deben documentarse las razones del fallo y las acciones correctivas.

7.5.2.5 Durante los ensayos de integración, todas las modificaciones o cambios realizados sobre los sistemas E/E/PE relacionados con la seguridad deben hacerse con el objeto de un análisis de impacto que debe identificar todos los componentes afectados así como las actividades de reverificación necesarias.

7.5.2.6 Los ensayos de integración de los E/E/PES deben documentar las siguientes informaciones:

a) la versión de la especificación de ensayo utilizado;

b) los criterios de aceptación de los ensayos de integración;

c) la versión de los sistemas E/E/PE relacionados con la seguridad sometidos a los ensayos;

d) las herramientas y los equipos utilizados así como los datos de calibración;

e) los resultados de cada ensayo;

f) toda divergencia entre los resultados previstos y reales;

g) el análisis realizado así como las decisiones tenidas en cuenta en la consecución del ensayo o la emisión de una demanda de modificación, en el caso en el que se observaran discrepancias.

7.5.2.7 Durante la integración de los E/E/PES, con el fin de evitar anomalías, debe utilizarse un conjunto de técnicas y medidas, de acuerdo con la tabla B.3.

7.6 Procedimientos de explotación y de mantenimiento de los E/E/PES

NOTA – Esta fase se representa en la etapa 9.5 de la figura 2.

7.6.1 Objetivo. El objetivo de los requisitos de este apartado es desarrollar unos procedimientos que permitan asegurar que la seguridad funcional requerida de los sistemas E/E/PE relacionados con la seguridad se mantiene durante la explotación y el mantenimiento.

7.6.2 Requisitos

7.6.2.1 Deben prepararse los procedimientos de explotación y de mantenimiento de los E/E/PES y debe especificarse la siguiente información:

a) las acciones periódicas que es necesario ejecutar con el fin de mantener la seguridad funcional de los sistemas E/E/PE relacionados con la seguridad “tal y como ha sido diseñado”, incluyendo el reemplazamiento sistemático de los componentes de vida predefinida, por ejemplo los ventiladores de refrigeración de las baterías, etc.;

b) las acciones y limitaciones que son necesarias (por ejemplo, durante la instalación, el arranque, el funcionamiento normal, los ensayos individuales en serie, las perturbaciones previsibles, las anomalías o fallos así como la parada) para prevenir un estado de no seguridad y/o reducir las consecuencias de un evento peligroso;

c) la documentación que es necesaria mantener en caso de fallo del sistema así como los niveles de fallo de demandas sobre los sistemas E/E/PE relacionados con la seguridad;

d) la documentación que es necesaria mantener, mostrando que los resultados de las auditorías y ensayos realizados sobre los sistemas relacionados con la seguridad;

e) los procedimientos de mantenimiento a seguir cuando ocurren anomalías o fallos en los sistemas E/E/PE relacionados con la seguridad, incluyendo

- procedimientos de diagnóstico de anomalías y reparación,
- procedimientos de revalidación,
- requisitos relativos a los informes de mantenimiento;

f) los procedimientos de informes de ejecución del mantenimiento deben estar especificados. En particular:

- procedimientos de los informes de los fallos,
- procedimientos de análisis de los fallos;

g) las herramientas necesarias en el mantenimiento y en la revalidación así como en los procedimientos de las herramientas y los equipos.

NOTA 1 – Puede ser beneficioso, por razones de seguridad y económicas, integrar los procedimientos de explotación y mantenimiento de los E/E/PES a los procedimientos globales de explotación y mantenimiento del EUC.

NOTA 2 – Conviene que los procedimientos de explotación y de mantenimiento de los E/E/PES incluyan los procedimientos de modificación del software (véase la Norma CEI 61508-3, apartado 7.8).

7.6.2.2 Los procedimientos de explotación y de mantenimiento del sistema E/E/PE relacionado con la seguridad debe estar continuamente mejorado sobre la base de datos tales que (1) los resultados de las auditorías de seguridad funcional y (2) los ensayos realizados sobre los sistemas E/E/PE relacionados con la seguridad.

7.6.2.3 Las acciones de mantenimiento periódico requerido para mantener la seguridad funcional requerida (como la diseñada) de los sistemas E/E/PE relacionados con la seguridad deben determinarse por un método sistemático. Este método debe determinar los fallos no revelados de todos los componentes relacionados con la seguridad (desde los sensores hasta los elementos finales) que podrían conllevar una reducción de la integridad de seguridad obtenida. Los métodos apropiados incluyen:

- examen de árboles de fallo;
- análisis de los modos de fallo y de sus efectos;
- mantenimiento basado en la fiabilidad.

NOTA 1 – Tener en cuenta el factor humano es un elemento clave para la determinación de las acciones requeridas y de la(s) interfaz(ces) apropiada(s) con los sistemas E/E/PE relacionados con la seguridad.

NOTA 2 – Se realizarán ensayos periódicos según la frecuencia necesaria para realizar la medida objetivo de fallos.

NOTA 3 – La frecuencia de los ensayos periódicos, del intervalo entre ensayos de diagnóstico y la duración de la reparación depende de varios factores (véase el anexo B de la Norma CEI 61508-6) tales como:

- la medida objetivo de fallos asociados al nivel de integridad de seguridad;
- la arquitectura;
- la cobertura del diagnóstico de los ensayos de diagnóstico;
- la tasa de demanda media.

NOTA 4 – La frecuencia de los ensayos periódicos y el intervalo entre los ensayos de diagnóstico son susceptibles de influir de forma importante en la realización de la integridad de seguridad del hardware. Uno de los principios justificantes del análisis de fiabilidad del hardware (véase el apartado 7.4.3.2.2) es asegurar que las frecuencias de los dos tipos de ensayos convienen a la integridad de seguridad objetivo del hardware.

7.6.2.4 Se debe evaluar el impacto eventual de los procedimientos de explotación y de mantenimiento de los E/E/PES sobre el EUC.

7.6.2.5 Para evitar anomalías y fallos durante los procedimientos de explotación y de mantenimiento de los E/E/PES, debe utilizarse un conjunto apropiado de técnicas y de medidas, de acuerdo con la tabla B.4.

7.7 Validación de la seguridad de los E/E/PES

NOTA – Esta fase se representa en la etapa 9.6 de la figura 2.

7.7.1 Objetivo. El objetivo de los requisitos de este apartado es validar la conformidad, en todos los aspectos, de los sistemas E/E/PE relacionados con la seguridad a los requisitos de seguridad, en términos de funciones de seguridad y de integridad de seguridad requeridos (véase el apartado 7.2).

7.7.2 Requisitos

7.7.2.1 La validación de la seguridad de los E/E/PES debe realizarse de acuerdo con un plan preestablecido (véase también el apartado 7.7. de la Norma CEI 61508-3).

NOTA 1 – Sobre el ciclo de vida de la seguridad de los E/E/PES, la actividad de validación de la seguridad de los E/E/PES se ilustra antes de la instalación; sin embargo, en ciertos casos, la validación de la seguridad de los E/E/PES sólo puede realizarse después de la instalación (por ejemplo, cuando el desarrollo del software aplicado no ha finalizado hasta después de la aplicación).

NOTA 2 – La validación de un sistema electrónico programable relacionado con la seguridad comprende la validación del hardware y del software. Los requisitos de validación se dan en la Norma CEI 61508-3.

7.7.2.2 Todos los equipos de medida de ensayo utilizados para la validación deben calibrarse en función de un patrón ligado a una norma nacional si está disponible o según un procedimiento bien adaptado. Debe verificarse el funcionamiento correcto de todos los equipos de ensayo.

7.7.2.3 Cada función de seguridad especificada en los requisitos de seguridad de los E/E/PES (véase el apartado 7.2) así como los procedimientos de explotación y mantenimiento de los E/E/PE deben validarae por ensayo y/o análisis.

7.7.2.4 La documentación relativa a los ensayos de validación de seguridad de los E/E/PES debe elaborarse e indicarse para cada función de seguridad.

a) la versión del plan de validación de seguridad de los E/E/PES utilizados;

b) la función de seguridad sometida a ensayo (o a análisis), así como la referencia específica al requisito especificado durante la planificación de la validación de seguridad de los E/E/PES;

c) las herramientas y equipos utilizados así como los datos de calibración;

d) los resultados de cada ensayo;

e) las divergencias entre los resultados previstos y los resultados reales.

NOTA – No es necesario realizar una documentación separada para cada función de seguridad; sin embargo, las informaciones requeridas en los puntos del a) al e) deben aplicarse a cada función de seguridad y cuando para una función de seguridad dada, estas informaciones son diferentes, deben indicarse.

7.7.2.5 En caso de divergencia (es decir, cuando los resultados reales se diferencian de los resultados previstos más allá de las tolerancias), los resultados de los ensayos de validación de la seguridad de los E/E/PES se debe documentar indicando:

a) el análisis realizado; y

b) las decisiones tenidas en cuenta en la consecución del ensayo o la emisión de una demanda de modificación y vuelta a una etapa anterior del ensayo de validación.

7.7.2.6 El suministrador o el desarrollador debe tener disponibles los resultados de los ensayos de validación de la seguridad de los E/E/PES para el desarrollador del EUC y del sistema de control del EUC de forma que le permita satisfacer los requisitos para la validación de la seguridad global de la Norma CEI 61508-1.

7.7.2.7 Para evitar anomalías durante la validación de la seguridad de los E/E/PES, debe utilizarse un conjunto apropiado de técnicas y de medidas, de acuerdo con la tabla B.5.

7.8 Modificación de los E/E/PES

7.8.1 Objetivo. El objetivo de los requisitos de este apartado es asegurar que la integridad de seguridad requerida se mantiene después de las correcciones, mejoras o adaptaciones aportadas a los sistemas E/E/PE relacionados con la seguridad.

7.8.2 Requisitos

7.8.2.1 Para cada actividad de modificación de los E/E/PES, debe establecerse y mantenerse una documentación adecuada. La documentación debe incluir:

a) la especificación detallada de la modificación o del cambio;

b) un análisis de impacto de la actividad de modificación sobre el sistema en su conjunto, incluyendo el hardware, el software (véase la Norma CEI 61508-3), la interacción humana, el entorno así como las interacciones eventuales;

c) todas las aprobaciones relativas a las modificaciones;

d) el avance de las modificaciones;

e) los ensayos elementales de los componentes, incluyendo los datos de revalidación;

f) el histórico de la gestión de la configuración de los E/E/PES;

g) las diferencias en relación a la explotación y a las condiciones normales;

h) las modificaciones que son necesarias aportar a los procedimientos del sistema;

i) las modificaciones que son necesarias aportar a la documentación.

7.8.2.2 Los fabricantes o los proveedores de sistemas que anuncian su conformidad con todo o parte de esta norma deben mantener un sistema que permita iniciar las modificaciones como resultado de una detección de defectos en el hardware o en el software, e informar a los usuarios de la necesidad de modificar en el caso de un defecto que afecta a la seguridad.

7.8.2.3 Las modificaciones deben realizarse utilizando al menos el mismo nivel de experiencia, de herramientas automáticas (véase el apartado 7.4.4.2 de la Norma CEI 61508-3), de planificación y de gestión que el desarrollo inicial de los sistemas E/E/PE relacionados con la seguridad.

7.8.2.4 Después de la modificación, los sistemas E/E/PE relacionados con la seguridad deben verificarse y revalidarse.

NOTA – Véase también el apartado 7.16.2.6 de la Norma CEI 61508-1.

7.9 Verificación de los E/E/PES

7.9.1 Objetivo. El objetivo de los requisitos de este apartado es probar y evaluar los resultados de una fase para asegurarse del carácter correcto y de la coherencia de los resultados en relación a los productos y normas proporcionadas como entradas en esta fase.

NOTA – Para mayor comodidad, todas las actividades de verificación se han reagrupado en el apartado 7.9, pero de hecho se realizan a lo largo de varias fases.

7.9.2 Requisitos

7.9.2.1 La verificación de los sistemas E/E/PE relacionados con la seguridad debe planificarse y documentarse en paralelo con el desarrollo (véase el apartado 7.4), para cada fase del ciclo de vida global de la seguridad de los E/E/PES.

7.9.2.2 La planificación de la verificación de los E/E/PES debe referirse a todos los criterios, técnicas y herramientas a utilizar durante la verificación para esta fase.

7.9.2.3 La planificación de la verificación de los E/E/PES debe especificar las actividades tomadas para asegurarse del carácter correcto y de la coherencia de los sistemas en relación a los productos y normas proporcionadas como entradas para esta fase.

7.9.2.4 La planificación de la verificación de los E/E/PES debe tener en cuenta los siguientes elementos:

a) elección de las estrategias y técnicas de verificación;

b) elección y utilización de los equipos de ensayo;

c) elección y la documentación de las actividades de verificación;

d) evaluación de los resultados de verificación obtenidos directamente a partir de los equipos de verificación y a partir de los ensayos.

7.9.2.5 Durante cada fase de diseño y desarrollo, debe demostrarse que se cumplen los requisitos funcionales y los requisitos de integridad de seguridad.

7.9.2.6 El resultado de cada actividad de verificación debe documentarse e indicarse o bien que el sistema E/E/PE relacionado con la seguridad ha pasado de forma satisfactoria la verificación, o la razón del rechazo. Los elementos siguientes deben tenerse en cuenta:

a) elementos que no están conformes a uno o varios requisitos pertinentes del ciclo de vida de la seguridad E/E/PES (véase el apartado 7.2);

b) elementos que no están conformes a una o varias normas de diseño aplicables (véase el apartado 7.4);

c) elementos que no están conformes a uno o varios requisitos de gestión de seguridad aplicables (véase el capítulo 6).

7.9.2.7 Para la verificación de los requisitos de seguridad de los E/E/PES, después del establecimiento de los requisitos de seguridad E/E/PES (véase el apartado 7.2) y antes de la siguiente fase (diseño y desarrollo), la verificación debe:

a) determinar la adecuación de los requisitos de seguridad para satisfacer los requisitos establecidos en la atribución de los requisitos de seguridad de los E/E/PES (véase la Norma CEI 61508-1) para la seguridad, la funcionalidad y otros requisitos especificados durante la planificación de la seguridad, y

b) verificar las incompatibilidades entre:

- los requisitos de seguridad (véase el apartado 7.2),
- la asignación de los requisitos de seguridad (CEI 61508-1),
- los ensayos de los E/E/PES (véase el apartado 7.4), y
- la documentación del usuario y de toda otra documentación relativa al sistema.

7.9.2.8 Para la verificación del diseño y del desarrollo de los E/E/PES, después de completar el diseño y el desarrollo de los E/E/PES (véase el apartado 7.4) y antes de la fase siguiente (integración), la verificación debe

a) asegurarse que los ensayos de los E/E/PES (véase el apartado 7.4) son adecuados al diseño y al desarrollo de los E/E/PES (véase el apartado 7.4);

b) asegurar la coherencia y la completitud (hasta el nivel de módulo incluso) del diseño y del desarrollo de los E/E/PES (véase el apartado 7.4) en relación a los requisitos de seguridad de los E/E/PES (véase el apartado 7.2); y

c) verificar las incompatibilidades entre

- los requisitos de seguridad de los E/E/PES (véase el apartado 7.2),
- el diseño y el desarrollo de los E/E/PES (véase el apartado 7.4),y
- los ensayos de los E/E/PES (véase el apartado 7.4).

NOTA 1 – La tabla B.5 recomienda unas técnicas de validación de la seguridad, de análisis de los fallos y de las técnicas de ensayo que también se aplican en la verificación.

NOTA 2 – La tabla A.1, que da las anomalías y los fallos que deben detectarse, se tiene en cuenta para verificar que la cobertura del diagnóstico se ha realizado.

7.9.2.9 Para la verificación de la integración de los E/E/PES, la integración de los sistemas E/E/EPE relacionados con la seguridad debe verificarse para asegurarse de la conformidad con los requisitos del apartado 7.5.

7.9.2.10 Los casos de ensayos así como sus resultados deben documentarse.

8 EVALUACIÓN DE LA SEGURIDAD FUNCIONAL

Los requisitos relacionados con la evaluación de la seguridad funcional son como se detallan en el capítulo 8 de la Norma CEI 61508-1.

ANEXO A (Normativo)

TÉCNICAS Y MEDIDAS APLICABLES A LOS SISTEMAS E/E/PE RELACIONADOS CON LA SEGURIDAD: CONTROL DE LOS FALLOS EN EXPLOTACIÓN

A.1 Generalidades

Este anexo se debe utilizar junto al apartado 7.4 y limita la cobertura de diagnóstico máximo que se admite anunciar para las técnicas y medidas pertinentes. Para cada nivel de integridad de seguridad, el anexo recomienda unas técnicas y medidas para controlar los fallos aleatorios, sistemáticos, ambientales y de operación del hardware. El anexo B de la Norma CEI 61508-6 y el anexo A de la Norma CEI 61508-7 proporciona más información en cuanto a las arquitecturas y medidas correspondientes.

No es posible enumerar cada causa física particular de un fallo en un hardware complejo por dos razones principales:

- la relación causa/efecto entre fallos y anomalías a menudo es difícil de determinar;
- la caracterización de los fallos pasa de aleatorios a sistemáticos en función de la complejidad del hardware y del software utilizados.

En función del momento de su aparición, los fallos de los sistemas E/E/PE relacionados con la seguridad se pueden clasificar en diferentes categorías:

- fallos debidos a anomalías que aparecen **antes o durante la instalación del sistema** (por ejemplo, las anomalías del software incluyen las anomalías de especificación y de programa, las anomalías del hardware incluyen las anomalías de fabricación y la selección de componentes incorrecta); y
- los fallos debidos a anomalías o errores humanos que aparecen **después de la instalación del sistema** (por ejemplo, los fallos aleatorios del hardware o los fallos debidos a una utilización incorrecta).

Para evitar o controlar estos fallos, una vez que han aparecido, en general es necesario un gran número de medidas. La estructura de los requisitos proporcionada en los anexos A y B resulta de la división de las medidas en medidas para **evitar los fallos** durante las diferentes fases del ciclo de vida de la seguridad de los E/E/PES (anexo B) y las utilizadas para **controlar los fallos** durante la explotación (este anexo A). Las medidas que permiten controlar los fallos son características integradas de los sistemas E/E/PE relacionados con la seguridad.

La cobertura del diagnóstico y la proporción de los fallos en seguridad se determinan sobre la base de la tabla A.1 de acuerdo con los procedimientos detallados en el anexo C. Las tablas de la A.2 a la A.15 apoyan los requisitos de la tabla A.1 recomendando técnicas y medidas de ensayo de diagnóstico así como los niveles máximos de cobertura de diagnóstico que se pueden realizar utilizando estas técnicas y medidas. Estas tablas no reemplazan ninguno de los requisitos del anexo C. Las tablas de la A.2 a la A.15 no son exhaustivas. Otras técnicas y medidas pueden ser utilizadas, proporcionando evidencias que permitan apoyar que la cobertura de diagnóstico anunciada se produce. Si se anuncia una cobertura de diagnóstico alta, entonces, como mínimo, conviene que al menos se utilice una técnica que permita una cobertura de diagnóstico alta, a partir de cada una de estas tablas.

De la misma forma, las tablas de la A.16 a la A.18 recomiendan unas técnicas y medidas para cada nivel de integridad de seguridad para controlar los fallos sistemáticos. La tabla A.16 recomienda unas medidas globales para controlar los fallos sistemáticos (véase también la Norma CEI 61508-3), la tabla A.17 recomienda unas medidas para controlar los fallos ambientales y la tabla A.18 recomienda unas medidas para controlar los fallos de operación. La mayor parte de estas medidas de control se pueden clasificar en función de la tabla A.19.

Todas las técnicas y medidas desarrolladas en estas tablas se describen en el anexo A de la Norma CEI 61508-7. Las técnicas y medidas del software requeridas para cada nivel de integridad de seguridad se dan en la Norma CEI 61508-3. Las directrices que permiten determinar la arquitectura de un sistema E/E/PE relacionado con la seguridad se dan en el anexo B de la Norma CEI 61508-6.

El seguimiento de las directrices de este anexo no garantiza por sí mismo la integridad de seguridad. Es importante tener en cuenta los siguientes elementos:

– la coherencia de las técnicas y medidas elegidas así como la forma en la que se complementan; y

– las técnicas y medidas que se adaptan mejor a los problemas específicos encontrados durante el desarrollo de cada sistema particular E/E/PE relacionado con la seguridad.

A.2 Integridad de seguridad del hardware

La tabla A.1 proporciona los requisitos para los fallos o anomalías que se deben detectar por las técnicas y medidas de control de los fallos del hardware con el fin de realizar la cobertura de diagnóstico pertinente (véase también el anexo C). Las tablas de la A.2 a la A.15 apoyan los requisitos de la tabla A.1 recomendando técnicas y medidas de ensayo de diagnóstico así como los niveles máximos de cobertura de diagnóstico que se pueden realizar utilizando estas técnicas y medidas. Se admite que estos ensayos se apliquen de forma permanente o periódica. Las tablas no reemplazan ninguno de los requisitos del apartado 7.4. Las tablas de la A.2 a la A.15 no son exhaustivas. Otras técnicas y medidas pueden ser utilizadas, proporcionando evidencias que permitan apoyar que la cobertura de diagnóstico se produce.

NOTA 1 – La presentación general de las técnicas y medidas examinadas en estas tablas se proporciona en el anexo A de la Norma CEI 61508-7. El apartado aplicable se referencia en la segunda columna de las tablas de la A.2 a la A.15.

NOTA 2 – Los calificativos bajo, medio y alto de la cobertura de diagnóstico se cuantifica al 60%, 90% y 99% respectivamente.

Tabla A.1
Anomalías o fallos a detectar en explotación o a analizar para deducir la proporción de fallos en seguridad

Componentes	Véanse la(s) tabla(s)	Requisitos para la cobertura del diagnóstico o la proporción de fallos en seguridad anunciadas		
		Baja (60%)	Media (90%)	Alta (99%)
Dispositivos electromecánicos	A.2	Anomalías de activación o desactivación Contactos soldados	Anomalías de activación o desactivación Contactos individuales soldados	Anomalías de activación o desactivación Contactos individuales soldados No conducción positiva de los contactos (este fallo no se tiene en cuenta para los relés construidos y ensayados de acuerdo con la Norma EN 50205, o equivalente) No abertura positiva (este fallo no se tiene en cuenta para los interruptores de posición construidos y ensayados de acuerdo con la Norma EN 60947-5-1 o equivalente)
Hardware discreto E/S numérica E/S analógica Alimentación	A.3, A.7, A.9, A.11	 Bloqueo Bloqueo Bloqueo	 Modelo de anomalía en c.c. Modelo de anomalía en c.c. por variación y oscilación Modelo de anomalía en c.c. por variación y oscilación	 Modelo de anomalía en c.c. por variación y oscilación Modelo de anomalía en c.c. por variación y oscilación Modelo de anomalía en c.c. por variación y oscilación
Bus Generalidades Unidad de gestión de memoria Acceso directo a memoria Arbitraje del bus (véase la nota 1)	A.3 A.7 A.8	 Bloqueo de las direcciones Bloqueo de los datos o las direcciones Ningún acceso o acceso continuo Bloqueo de las señales de arbitraje	 Interrupción Decodificación de la dirección errónea Modelo de anomalía en c.c. para los datos y las direcciones Tiempo de acceso erróneo Ningún arbitraje o arbitraje continuo	 Interrupción Decodificación de la dirección errónea Todas las anomalías que afectan a los datos en memoria Datos o direcciones erróneas Tiempo de acceso erróneo Ningún arbitraje, arbitraje continuo o arbitraje erróneo
CPU Registro, RAM interna Codificación y ejecución incluyendo el registro del puntero Cálculo de la dirección Programa contador, puntero de pila	A.4,.A.10	 Bloqueo de los datos y las direcciones Codificación errónea o no ejecución Bloqueo Bloqueo	 Modelo de anomalía en c.c. para los datos y direcciones Codificación errónea o ejecución errónea Modelo de anomalía en c.c. Modelo de anomalía en c.c.	 Modelo de anomalía en c.c. para los datos y direcciones Cruce dinámico para las celdas de memoria Ningún direccionamiento, direccionamiento erróneo o múltiple Ninguna hipótesis de fallo definida Ninguna hipótesis de fallo definida Modelo de anomalía en c.c.

(Continúa)

Tabla A.1 *(Fin)*
Anomalías o fallos a detectar en explotación o a analizar para deducir la proporción de fallos en seguridad

Componentes	Véanse la(s) tabla(s)	Requisitos para la cobertura del diagnóstico o la proporción de fallos en seguridad anunciadas		
		Baja (60%)	**Media (90%)**	**Alta (99%)**
Gestión de las interrupciones	A.4	Ninguna interrupción o interrupción en continuo	Ninguna interrupción o interrupción continua Cruce de las interrupciones	Ninguna interrupción o interrupción continua Cruce de las interrupciones
Memoria invariable	A.5	Bloqueo de los datos y direcciones	Modelo de anomalía en c.c. para los datos y las direcciones	Todas las anomalías que afectan a los datos en memoria
Memoria variable	A.6	Bloqueo de los datos y direcciones	Modelo de anomalía en c.c. para los datos y las direcciones Modificación de los datos provocado por los errores del software para los DRAM integrados de 1 Mbits y mayores	Modelo de anomalía en c.c. para los datos y las direcciones Cruce dinámico de las celdas de memoria Ningún direccionamiento, direccionamiento erróneo o múltiple Modificación de los datos provocado por los errores del software para los DRAM integrados de 1 Mbits y mayores
Reloj (quartz)	A.12	Sub- o sobre- armónico	Sub- o sobre- armónico	Sub- o sobre- armónico
Comunicaciones y memoria de masa	A.13	Datos o direcciones erróneas Ninguna transmisión	Todas las anomalías que afectan a los datos en memoria Datos o direcciones erróneas Tiempo de transmisión erróneo Secuencia de transmisión errónea	Todas las anomalías que afectan a los datos en memoria Datos o direcciones erróneas Tiempo de transmisión erróneo Secuencia de transmisión errónea
Sensores	A.14	Bloqueo	Modelo de anomalía en c.c. Variación y oscilación	Modelo de anomalía en c.c. Variación y oscilación
Elementos finales	A.15	Bloqueo	Modelo de anomalía en c.c. Variación y oscilación	Modelo de anomalía en c.c. Variación y oscilación

NOTA 1 – El arbitraje del bus es el mecanismo que permite decidir el dispositivo que controla el bus.

NOTA 2 – "Bloqueo" es una categoría de anomalía que puede describirse con "0" o "1" o "activo" continuos en las patillas de un componente.

NOTA 3 – "Modelo de anomalía en c.c." (c.c. = corriente continua) indica los modos de anomalías siguientes: de bloqueo, de bloqueo abierto, salidas abiertas o de alta impedancia así como los cortocircuitos entre las líneas de señales.

Tabla A.2
Subsistemas eléctricos

Técnica/medida de diagnóstico	Véase la Norma CEI 61508-7 (apartados)	Cobertura del diagnóstico máxima considerada realizable	Notas
Detección de los fallos por supervisión en línea	A.1.1	Baja (modo de baja demanda) Media (modo de alta demanda o modo continuo)	Depende de la cobertura del diagnóstico de la detección de fallo
Supervisión de los contactos de relés	A.1.2	Alta	
Comparador	A.1.3	Alta	Elevado si los modos de fallo tienen una orientación de seguridad dominante
Dispositivo de toma de decisión mayoritario	A.1.4	Alta	Depende de la calidad del voto mayoritario
Principio de corriente en reposo	A.1.5	Baja	Únicamente para los sistemas E/E/PE relacionados con la seguridad para los que no es necesario un control continuo para realizar o mantener un estado de seguridad del EUC
NOTA 1 – Esta tabla no reemplaza ninguno de los requisitos del anexo C. NOTA 2 – Los requisitos del anexo C son apropiados para la determinación de la cobertura del diagnóstico. NOTA 3 – Para las notas generales relativas a esta tabla, véase el texto que precede a la tabla A.1.			

Tabla A.3
Subsistemas electrónicos

Técnica/medida de diagnóstico	Véase la Norma CEI 61508-7 (apartados)	Cobertura del diagnóstico máxima considerada realizable	Notas
Detección de los fallos por supervisión en línea	A.1.1	Baja (modo de baja demanda) Media (modo de alta demanda o modo continuo)	Depende de la cobertura del diagnóstico de la detección de fallo
Comparador	A.1.3	Alta	Alta si los modos de fallo tienen una orientación de seguridad predominante
Dispositivo de toma de decisión mayoritario	A.1.4	Alta	Depende de la calidad del voto mayoritario
Ensayos mediante el hardware redundante	A.2.1	Media	Depende de la cobertura del diagnóstico de la detección de fallo
Principios dinámicos	A.2.2	Media	Depende de la cobertura del diagnóstico de la detección de fallo
Puerto de acceso de ensayo normalizado y arquitectura de barrido del conjunto de las uniones	A.2.3	Alta	Depende de la cobertura del diagnóstico de la detección de fallo
Supervisado redundante	A.2.5	Alta	Depende del grado de redundancia y de la supervisión
Hardware con verificación automática	A.2.6	Alta	Depende de la cobertura del diagnóstico de los ensayos
Supervisión de la señal analógica	A.2.7	Baja	
NOTA 1 – Esta tabla no reemplaza ninguno de los requisitos del anexo C. NOTA 2 – Los requisitos del anexo C son apropiados para la determinación de la cobertura del diagnóstico. NOTA 3 – Para las notas generales relativas a esta tabla, véase el texto que precede a la tabla A.1.			

Tabla A.4
Unidades de tratamiento

Técnica/medida de diagnóstico	Véase la Norma CEI 61508-7 (apartados)	Cobertura del diagnóstico máxima considerada realizable	Notas
Comparador	A.1.3	Alta	Depende de la calidad de la comparación
Dispositivo de toma de decisión mayoritario	A.1.4	Alta	Depende de la calidad del voto mayoritario
Auto ensayo mediante el software: número limitado de configuraciones (un canal)	A.3.1	Baja	
Auto ensayo mediante el software: bit deslizante (un canal)	A.3.2	Media	
Auto ensayo soportado por el hardware (un canal)	A.3.3	Media	
Tratamiento codificado (un canal)	A.3.4	Alta	
Comparación recíproca por el software	A.3.5	Alta	Depende de la calidad de la comparación
NOTA 1 – Esta tabla no reemplaza ninguno de los requisitos del anexo C.			
NOTA 2 – Los requisitos del anexo C son apropiados para la determinación de la cobertura del diagnóstico.			
NOTA 3 – Para las notas generales relativas a esta tabla, véase el texto que precede a la tabla A.1.			

Tabla A.5
Rangos de memoria invariables

Técnica/medida de diagnóstico	Véase la Norma CEI 61508-7 (apartados)	Cobertura del diagnóstico máxima considerada realizable	Notas
Redundancia multibits mediante palabra reseñada	A.4.1	Media	
Suma de control modificada	A.4.2	Baja	
Firma de una sola palabra (8 bits)	A.4.3	Media	La eficacia de la firma depende de la longitud de la firma, en comparación con la longitud del bloque de información a proteger
Firma de una palabra doble (16 bits)	A.4.4	Alta	La eficacia de la firma depende de la longitud de la firma, en comparación con la longitud del bloque de información a proteger
Réplica de bloque	A.4.5	Alta	
NOTA 1 – Esta tabla no reemplaza ninguno de los requisitos del anexo C.			
NOTA 2 – Los requisitos del anexo C son apropiados para la determinación de la cobertura del diagnóstico.			
NOTA 3 – Para las notas generales relativas a esta tabla, véase el texto que precede a la tabla A.1.			

Tabla A.6
Rangos de memoria variables

Técnica/medida de diagnóstico	Véase la Norma CEI 61508-7 (apartados)	Cobertura del diagnóstico máxima considerada realizable	Notas
Ensayo RAM "damero" o "march"	A.5.1	Baja	
Ensayo RAM "walk-path"	A.5.2	Media	
Ensayo RAM "galpat" o "galpat" transparente	A.5.3	Alta	
Ensayo RAM "Abraham"	A.5.4	Alta	
Bit de paridad de la RAM	A.5.5	Baja	
Supervisión de la RAM con un código de Hamming modificado o detección del fallo de los datos de un código de detección de error (EDC)	A.5.6	Alta	
Doble RAM con ensayo de comparación mediante hardware o software y de lectura/escritura	A.5.7	Alta	

NOTA 1 – Esta tabla no reemplaza ninguno de los requisitos del anexo C.

NOTA 2 – Los requisitos del anexo C son apropiados para la determinación de la cobertura del diagnóstico.

NOTA 3 – Para las notas generales relativas a esta tabla, véase el texto que precede a la tabla A.1.

NOTA 4 – Para una RAM cuyos accesos a lectura/escritura son sólo esporádicos (por ejemplo, durante la configuración), las medidas de los apartados del A.4.1 al A.4.4 son eficaces si se realizan después de cada acceso de lectura/escritura.

Tabla A.7
Unidades de E/S e interfaz (comunicación externa)

Técnica/medida de diagnóstico	Véase la Norma CEI 61508-7 (apartados)	Cobertura del diagnóstico máxima considerada realizable	Notas
Detección de fallos por supervisión en línea	A.1.1	Baja (modo de baja demanda) Media (modo de alta demanda o modo continuo)	Depende de la cobertura del diagnóstico de la detección de fallos
Patrón de ensayo	A.6.1	Alta	
Protección por código	A.6.2	Alta	
Salida paralela multicanal	A.6.3	Alta	Únicamente si el flujo de los datos cambia durante el intervalo del ensayo de diagnóstico
Salidas supervisadas	A.6.4	Alta	Únicamente si el flujo de los datos cambia durante el intervalo del ensayo de diagnóstico
Comparación/voto mayoritario sobre las entradas (1oo2, 2oo3 o redundancia mejorada)	A.6.5	Alta	Únicamente si el flujo de los datos cambia durante el intervalo del ensayo de diagnóstico

NOTA 1 – Esta tabla no reemplaza ninguno de los requisitos del anexo C.

NOTA 2 – Los requisitos del anexo C son apropiados para la determinación de la cobertura del diagnóstico.

NOTA 3 – Para las notas generales relativas a esta tabla, véase el texto que precede a la tabla A.1.

Tabla A.8
Ruta de datos (comunicación interna)

Técnica/medida de diagnóstico	Véase la Norma CEI 61508-7 (apartados)	Cobertura del diagnóstico máxima considerada realizable	Notas
Redundancia del hardware sobre un bit	A.7.1	Baja	
Redundancia del hardware sobre varios bits	A.7.2	Media	
Redundancia del hardware completa	A.7.3	Alta	
Inspección utilizando los patrones de ensayo	A.7.4	Alta	
Redundancia de transmisión	A.7.5	Alta	Efectivo únicamente contra las anomalías transitorias
Redundancia de informaciones	A.7.6	Alta	
NOTA 1 – Esta tabla no reemplaza ninguno de los requisitos del anexo C.			
NOTA 2 – Los requisitos del anexo C son apropiados para la determinación de la cobertura del diagnóstico.			
NOTA 3 – Para las notas generales relativas a esta tabla, véase el texto que precede a la tabla A.1.			

Tabla A.9
Alimentación

Técnica/medida de diagnóstico	Véase la Norma CEI 61508-7 (apartados)	Cobertura del diagnóstico máxima considerada realizable	Notas
Protección contra las sobretensiones con parada de seguridad o conmutación sobre la segunda unidad de alimentación	A.8.1	Baja	Se recomienda utilizar siempre como suplemento otras técnicas definidas en esta tabla
Supervisión de la tensión (secundaria) con parada de seguridad o comunicación sobre la segunda unidad de alimentación	A.8.2	Alta	
Puesta fuera de tensión con parada de seguridad o comunicación sobre la segunda unidad de alimentación	A.8.3	Alta	Se recomienda utilizar siempre como suplemento otras técnicas definidas en esta tabla
Principio de corriente en reposo	A.1.5	Baja	Útil solamente contra las puestas fuera de tensión
NOTA 1 – Esta tabla no reemplaza ninguno de los requisitos del anexo C.			
NOTA 2 – Los requisitos del anexo C son apropiados para la determinación de la cobertura del diagnóstico.			
NOTA 3 – Para las notas generales relativas a esta tabla, véase el texto que precede a la tabla A.1.			

Tabla A.10
Secuencia del programa (perro guardián)

Técnica/medida de diagnóstico	Véase la Norma CEI 61508-7 (apartados)	Cobertura del diagnóstico máxima considerada realizable	Notas
"Perro guardián" con base de tiempo separada sin ventana temporal	A.9.1	Baja	
"Perro guardián" con base de tiempo separada y ventana temporal	A.9.2	Media	
Supervisión lógica de la secuencia del programa	A.9.3	Media	Depende de la calidad de la supervisión
Combinación de supervisión temporal y lógica de las secuencias del programa	A.9.4	Alta	
Supervisión temporal con control en línea	A.9.5	Media	
NOTA 1 – Esta tabla no reemplaza ninguno de los requisitos del anexo C.			
NOTA 2 – Los requisitos del anexo C son apropiados para la determinación de la cobertura del diagnóstico.			
NOTA 3 – Para las notas generales relativas a esta tabla, véase el texto que precede a la tabla A.1.			

Tabla A.11
Sistemas de ventilación y de calentamiento (si es necesario)

Técnica/medida de diagnóstico	Véase la Norma CEI 61508-7 (apartados)	Cobertura del diagnóstico máxima considerada realizable	Notas
Sensor de temperatura	A.10.1	Media	
Control de los ventiladores	A.10.2	Media	
Accionamiento de la parada de seguridad por medio de un fusible térmico	A.10.3	Alta	
Mensaje escalonado de los sensores térmicos y alarma condicional	A.10.4	Alta	
Conexión de refrigeración por aire forzado e indicación del estado	A.10.5	Alta	
NOTA 1 – Esta tabla no reemplaza ninguno de los requisitos del anexo C.			
NOTA 2 – Los requisitos del anexo C son apropiados para la determinación de la cobertura del diagnóstico.			
NOTA 3 – Para las notas generales relativas a esta tabla, véase el texto que precede a la tabla A.1.			

Tabla A.12
Reloj

Técnica/medida de diagnóstico	Véase la Norma CEI 61508-7 (apartados)	Cobertura del diagnóstico máxima considerada realizable	Notas
"Perro guardián" con base de tiempo separada sin ventana temporal	A.9.1	Baja	
"Perro guardián" con base de tiempo separada y ventana temporal	A.9.2	Alta	Depende de la restricción de tiempo para la ventana temporal
Supervisión lógica de la secuencia del programa	A.9.3	Media	Sólo efectiva contra los fallos de reloj si los eventos temporales externos influencian el flujo del programa lógico
Supervisión temporal y lógica	A.9.4	Alta	
Supervisión temporal con control en línea	A.9.5	Media	
NOTA 1 – Esta tabla no reemplaza ninguno de los requisitos del anexo C.			
NOTA 2 – Los requisitos del anexo C son apropiados para la determinación de la cobertura del diagnóstico.			
NOTA 3 – Para las notas generales relativas a esta tabla, véase el texto que precede a la tabla A.1.			

Tabla A.13
Comunicación y memoria de masa

Técnica/medida de diagnóstico	Véase la Norma CEI 61508-7 (capítulo y apartados)	Cobertura del diagnóstico máxima considerada realizable	Notas
Intercambio de información entre el sistema E/E/PE relacionado con la seguridad y el procedimiento	A.6	Véase la tabla A.7	Véase unidades E/S e interfaz
Intercambio de información entre sistemas E/E/PE relacionados con la seguridad	A.7	Véase la tabla A.8	Véase ruta de los datos/bus
Separación entre las líneas de alimentación eléctricas y las líneas de información	A.11.1	Alta	Se recomienda utilizar siempre como suplemento otras técnicas definidas en esta tabla
Separación espacial de las líneas múltiples	A.11.2	Alta	
Aumento de la inmunidad a las interferencias	A.11.3	Alta	
Transmisión de señales complementaria	A.11.4	Alta	
NOTA 1 – Esta tabla no reemplaza ninguno de los requisitos del anexo C.			
NOTA 2 – Los requisitos del anexo C son apropiados para la determinación de la cobertura del diagnóstico.			
NOTA 3 – Para las notas generales relativas a esta tabla, véase el texto que precede a la tabla A.1.			

Tabla A.14
Sensores

Técnica/medida de diagnóstico	Véase la Norma CEI 61508-7 (apartados)	Cobertura del diagnóstico máxima considerada realizable	Notas
Detección de los fallos por supervisión en línea	A.1.1	Baja (modo de baja demanda) Media (modo de alta demanda o modo continuo)	Depende de la cobertura del diagnóstico de la detección de fallos
Principio de corriente en reposo	A.1.5	Baja	Únicamente para los sistemas E/E/PE relacionados con la seguridad para los que no es necesario un control continuo para realizar o mantener un estado de seguridad del EUC
Supervisión de la señal analógica	A.2.7	Baja	
Patrón de ensayo	A.6.1	Alta	
Comparación/voto mayoritario sobre las entradas (1oo2, 2oo3 o redundancia mejorada)	A.6.5	Alta	Únicamente si el flujo de datos cambia durante el intervalo de ensayo de diagnóstico
Sensor de referencia	A.12.1	Alta	Depende de la cobertura del diagnóstico de la detección de fallos
Conmutador a acción directa	A.12.2	Alta	
NOTA 1 – Esta tabla no reemplaza ninguno de los requisitos del anexo C. NOTA 2 – Los requisitos del anexo C son apropiados para la determinación de la cobertura del diagnóstico. NOTA 3 – Para las notas generales relativas a esta tabla, véase el texto que precede a la tabla A.1.			

Tabla A.15
Elementos finales (accionadores)

Técnica/medida de diagnóstico	Véase la Norma CEI 61508-7 (apartados)	Cobertura del diagnóstico máxima considerada realizable	Notas
Detección de los fallos por supervisión en línea	A.1.1	Baja (modo de baja demanda) Media (modo de alta demanda o modo continuo)	Depende de la cobertura del diagnóstico de la detección de fallos
Supervisión de los contactos de relés	A.1.2	Alta	
Principio de corriente en reposo	A.1.5	Baja	Únicamente para los sistemas E/E/PE relacionados con la seguridad para los que no es necesario un control continuo para realizar o mantener un estado de seguridad del EUC
Patrón de ensayo	A.6.1	Alta	
Supervisión	A.13.1	Alta	Depende de la cobertura del diagnóstico de la detección de fallos
Supervisión cruzada de varios accionadores	A.13.2	Alta	
NOTA 1 – Esta tabla no reemplaza ninguno de los requisitos del anexo C. NOTA 2 – Los requisitos del anexo C son apropiados para la determinación de la cobertura del diagnóstico. NOTA 3 – Para las notas generales relativas a esta tabla, véase el texto que precede a la tabla A.1.			

A.3 Integridad de seguridad sistemática

Las tablas A.16 a A.18 proporcionan recomendaciones relativas a las técnicas y medidas destinadas a:

- controlar los fallos debidos al diseño del hardware y del software (véase la tabla A.16);
- controlar los fallos debidos a las limitaciones o influencias del entorno (véase la tabla A.17); y
- controlar los fallos observados durante la explotación (véase la tabla A.18).

Las tablas A.16 a A.18 proporcionan recomendaciones por nivel de integridad de seguridad indicando, en primer lugar, la importancia de la técnica o medida y, en segundo lugar, la eficacia requerida si se utiliza esta técnica o medida. La importancia se describe de la manera siguiente:

- HR: la técnica o medida es altamente recomendada para ese nivel de integridad de seguridad. Si esta técnica o medida no se utiliza, los motivos subyacentes deben describirse de forma detallada;
- R: la técnica o medida es recomendada para ese nivel de integridad de seguridad. Se exige al menos una de las técnicas del grupo sombreado;
- –: la técnica o medida no aporta ninguna recomendación a favor o en contra de su utilización;
- NR: la técnica o medida no es recomendada en absoluto para ese nivel de integridad de seguridad. Si se utiliza esta técnica o medida, los motivos subyacentes deben describirse de forma detallada.

La eficacia requerida se describe de la forma siguiente:

- Obligatoria: la técnica o medida se requiere para todos los niveles de integridad de seguridad y debe utilizarse tan eficazmente como sea posible (es decir, aportando una alta eficacia).
- Baja: si se utiliza, la técnica o medida debe aplicarse en la medida necesaria para proporcionar al menos una baja eficacia contra los fallos sistemáticos.
- Media: si se utiliza, la técnica o medida debe aplicarse en la medida necesaria para proporcionar al menos una eficacia media contra los fallos sistemáticos.
- Alta: si se utiliza, la técnica o medida debe aplicarse en la medida necesaria para proporcionar al menos una eficacia alta contra los fallos sistemáticos.

La tabla A.19 proporciona instrucciones relativas al nivel de eficacia para la mayor parte de las técnicas y medidas.

Si una medida no es obligatoria, en principio, puede reemplazarse por otras medidas (o bien tomadas separadamente, o bien en combinación); esto se rige por el sombreado de la zona correspondiente como se explica en la tabla.

Todas las técnicas y medidas proporcionadas aquí son características integradas de los sistemas E/E/PE relacionados con la seguridad que pueden ayudar al control de los fallos en línea. Los procedimientos así como las técnicas de organización y medida son necesarias durante el ciclo de vida de la seguridad de los E/E/PES para evitar la introducción de anomalías, y de las técnicas de validación de ensayos, del comportamiento de los sistemas E/E/PE relacionados con la seguridad contra influencias externas previsibles son necesarios para demostrar que las características de los elementos integrados son idóneos a la aplicación específica (véase el anexo B).

El anexo D de la Norma CEI 61508-6 proporciona informaciones sobre los fallos de causa común.

NOTA – La mayor parte de las medidas de las tablas de la A.16 a la A.18 pueden utilizarse con una eficacia variable, como se indica en la tabla A.19, que proporciona ejemplos de eficacia baja y alta. El esfuerzo necesario para una eficacia media se sitúa entre el especificado para una eficacia baja y el especificado para una eficacia alta.

Tabla A.16
Técnicas y medidas para controlar los fallos sistemáticos debidos al diseño del hardware y del software

	Técnica/medida	Véase la Norma CEI 61508-7 (capítulos o apartados)	SIL1	SIL2	SIL3	SIL4
	Supervisión de la secuencia del programa	A.9	HR baja	HR baja	HR media	HR alta
	Detección de los fallos por supervisión en línea (véase la nota 4)	A.1.1	R baja	R baja	R media	R alta
	Ensayos por el hardware redundante	A.2.1	R baja	R baja	R media	R alta
	Puerto de acceso de ensayo normalizado y arquitectura de barrido del conjunto de las uniones	A.2.3	R baja	R baja	R media	R alta
	Protección por código	A.6.2	R baja	R baja	R media	R alta
	Diversidad del hardware	B.1.4	– baja	– baja	R media	R alta
	Detección de anomalías y diagnóstico	C.3.1	Véase la tabla A.2 de la Norma CEI 61508-3			
	Códigos de corrección y detección del error	C.3.2				
	Programación por asertos del fallo	C.3.3				
	Dispositivos externos de seguridad	C.3.4				
	Programación diversa	C.3.5				
	Bloque de recuperación	C.3.6				
	Recuperación hacia atrás	C.3.7				
	Recuperación hacia adelante	C.3.8				
	Mecanismos de recuperación de las anomalías por relanzamiento	C.3.9				
	Memorización de los casos de ejecución	C.3.10				
	Degradación “elegante”	C.3.11				
	Inteligencia artificial – corrección de las anomalías	C.3.12				
	Reconfiguración dinámica	C.3.13				

Se debe exigir al menos una de las técnicas del grupo sombreado.

NOTA 1 – Para el significado de las entradas en cada nivel de integridad de seguridad, véase el texto inmediatamente anterior a esta tabla.

NOTA 2 – En esta tabla, las medidas que no hacen referencia a la tabla A.2 de la Norma CEI 61508-3 pueden utilizarse para hacer variar la eficacia de acuerdo con la tabla A.19 que proporciona unos ejemplos de eficacia baja y alta. El esfuerzo requerido para una eficacia media se encuentra entre el requerido para una eficacia baja y una eficacia alta.

NOTA 3 – La presentación general de las técnicas y medidas examinadas en esta tabla se proporciona en los anexos A, B y C de la parte 7. El apartado aplicable se referencia en la segunda columna.

NOTA 4 – Para los sistemas E/E/PE relacionados con la seguridad utilizados en un modo de funcionamiento de baja demanda (por ejemplo, sistemas de parada de urgencia), la cobertura del diagnóstico realizada a partir de la detección de los fallos por supervisión en línea es generalmente baja o inexistente.

Tabla A.17
Técnicas y medidas para controlar los fallos sistemáticos debidos a las limitaciones o influencias del entorno

	Técnica/medida	Véase la Norma CEI 61508-7 (capítulos o apartados)	SIL1	SIL2	SIL3	SIL4
	Medidas contra las caídas de tensión, las variaciones de tensión, las subidas de tensión, las bajadas de tensión	A.8	HR obligatoria	HR obligatoria	HR obligatoria	HR obligatoria
	Separación entre las líneas de alimentación eléctricas y las líneas de datos (véase la nota 4)	A.11.1	HR obligatoria	HR obligatoria	HR obligatoria	HR obligatoria
	Aumento de la inmunidad a las interferencias	A.11.3	HR obligatoria	HR obligatoria	HR obligatoria	HR obligatoria
	Medidas contra el entorno físico (por ejemplo temperatura, humedad, agua, vibraciones, polvo, sustancias corrosivas)	A.14	HR obligatoria	HR obligatoria	HR obligatoria	HR obligatoria
	Supervisión de la secuencia de instrucciones	A.9	HR baja	HR baja	HR media	HR alta
	Medidas contra el sobrecalentamiento	A.10	HR baja	HR baja	HR media	HR alta
	Separación espacial de las líneas múltiples	A.11.2	HR baja	HR baja	HR media	HR alta
	Detección de los fallos por supervisión en línea (véase la nota 5)	A.1.1	R baja	R baja	R media	R alta
	Ensayos por el hardware redundante	A.2.1	R baja	R baja	R media	R alta
	Protección por código	A.6.2	R baja	R baja	R media	R alta
	Transmisión de señales complementarias	A.11.4	R baja	R baja	R media	R alta
	Diversidad del hardware (véase la nota 6)	B.1.4	– baja	– baja	– media	R alta
	Arquitectura del software	Apartado 7.4.3 de la Norma CEI 61508-3	Véase la tabla A.2 de la Norma CEI 61508-3			

Se debe exigir al menos una de las técnicas del grupo sombreado.

NOTA 1 – Para el significado de las entradas en cada nivel de integridad de seguridad, véase el texto inmediatamente anterior a la tabla A.16.

NOTA 2 – En esta tabla, la mayor parte de las medidas pueden utilizarse para hacer variar la eficacia de acuerdo con la tabla A.19 que proporciona ejemplos de eficacia baja y alta.

NOTA 3 – La presentación general de las técnicas y medidas examinadas en esta tabla se proporciona en los anexos A y B de la Norma CEI 61508-7. El apartado aplicable se referencia en la segunda columna.

NOTA 4 – La separación entre las líneas de alimentación eléctrica y las líneas de datos no es necesaria en el caso de transporte óptico de las informaciones ni para las líneas de alimentación eléctrica de baja potencia que se diseñan para alimentar los componentes de los E/E/PES y transportar la información desde o hacia estos componentes.

NOTA 5 – Para los sistemas E/E/PE relacionados con la seguridad utilizados en un modo de funcionamiento de baja demanda (por ejemplo, sistemas de parada de urgencia), la cobertura del diagnóstico realizada a partir de la detección de los fallos por supervisión en línea es generalmente baja o inexistente.

NOTA 6 – La diversidad del hardware no se requiere si se ha demostrado, por validación y por una larga experiencia operacional, que el hardware está suficientemente exento de anomalías de diseño y protegido contra los fallos de causa común para satisfacer las medidas objetivo de los fallos.

Tabla A.18
Técnicas y medidas para controlar los fallos sistemáticos en explotación

	Técnica/medida	Véase la Norma CEI 61508-7 (apartados)	SIL1	SIL2	SIL3	SIL4
	Protección contra las modificaciones	B.4.8	HR obligatoria	HR obligatoria	HR obligatoria	HR obligatoria
	Detección de los fallos por supervisión en línea (véase la nota 4)	A.1.1	R baja	R baja	R media	R alta
	Acuse de recepción de las entradas	B.4.9	R baja	R baja	R media	R alta
	Programación por aserto de los fallos	C.3.3	Véase la tabla A.2 de la Norma CEI 61508-3			

Se debe exigir al menos una de las técnicas del grupo sombreado.

NOTA 1 – Para el significado de las entradas en cada nivel de integridad de seguridad, véase el texto inmediatamente anterior a la tabla A.16.

NOTA 2 – En esta tabla, la mayor parte de las medidas pueden utilizarse para hacer variar la eficacia de acuerdo con la tabla A.19 que proporciona ejemplos de eficacia baja y alta.

NOTA 3 – La presentación general de las técnicas y medidas examinadas en esta tabla se proporciona en los anexos A, B y C de la Norma CEI 61508-7. El apartado aplicable se referencia en la segunda columna.

NOTA 4 – Para los sistemas E/E/PE relacionados con la seguridad utilizados en un modo de funcionamiento de baja demanda (por ejemplo, sistemas de parada de urgencia), la cobertura del diagnóstico realizada a partir de la detección de los fallos por supervisión en línea es generalmente baja o inexistente.

Tabla A.19
Eficacia de las técnicas y medidas para controlar los fallos sistemáticos

Técnica /medida	Véase la Norma CEI 61508-7 (apartados)	Baja eficacia	Alta eficacia
Detección de los fallos por supervisión en línea (véase la nota)	A.1.1	De las señales de arranque del EUC y su sistema de control se utilizan para verificar el funcionamiento correcto de los sistemas E/E/PE relacionados con la seguridad (únicamente comportamiento temporal con un límite de tiempo superior)	Los sistemas E/E/PE relacionados con la seguridad se reinician por unas señales temporales y lógicas que provienen del EUC y de su sistema de control (ventana temporal para la función de "perro guardián" temporal)
Ensayos por el hardware redundante (véase la nota)	A.2.1	Del hardware suplementario se utiliza para ensayar las señales de arranque de los sistemas E/E/PE relacionados con la seguridad (únicamente comportamiento temporal con un límite de tiempo superior); este hardware conmuta un elemento final secundario	El hardware suplementario se reinicia por unas señales temporales y lógicas que provienen de los sistemas E/E/PE relacionados con la seguridad (ventana temporal para la función de "perro guardián" temporal); dispositivo de voto mayoritario entre varios canales
Puerto de acceso del ensayo normalizado y arquitectura del barrido del conjunto de las uniones	A.2.3	Ensayos de la lógica de semiconductores utilizado durante el ensayo periódico mediante ensayos definidos de barrido del conjunto de las uniones	Ensayo de diagnóstico de la lógica de semiconductores, de acuerdo con la especificación funcional de los sistemas E/E/PE relacionados con la seguridad; todas las funciones de los circuitos integrados son controlados
Protección por código	A.6.2	Detección de los fallos por redundancia temporal de la transmisión de las señales	Detección de los fallos por redundancia temporal y redundancia de las informaciones de transmisión de señales
Supervisión de la secuencia de instrucciones	A.9	Supervisión temporal o lógica se la secuencia de instrucciones	Supervisión temporal y lógica de la secuencia de instrucciones en numerosos puntos de control del programa
Medidas contra los sobrecalentamientos	A.10	Sensor de temperatura, detección del sobrecalentamiento	Accionamiento de la parada de seguridad por medio de un fusible térmico
Aumento de la inmunidad a las interferencias (véase la nota)	A.11.3	Filtro antirruido al nivel de la alimentación y al nivel de las entradas y salidas críticas; blindaje si fuera necesario	Filtros contra las perturbaciones electromagnéticas normalmente inesperadas; blindaje
Medidas contra el entorno físico	A.14	Práctica generalmente aceptada para la aplicación considerada	Técnicas referenciadas en las normas para una aplicación particular
Diversidad del hardware	B.1.4	Dos o más elementos que realizan la misma función pero diferentes de diseño	Dos o más elementos que realizan funciones diferentes
Acuse de recepción de las entradas	B.4.9	Control por retorno de las acciones de entrada hacia el operario	Reglas de verificación estrictas para la entrada de datos por el operario, con rechazo de las entradas incorrectas

NOTA – En el caso de las técnicas referenciadas A.1.1, A.2.1, A.11.3 y A.14, se supone, para una alta eficacia de la técnica o de la medida, que las aproximaciones de baja eficacia también se utilizan.

ANEXO B (Normativo)

TÉCNICAS Y MEDIDAS APLICABLES A LOS SISTEMAS E/E/PE RELACIONADOS CON LA SEGURIDAD: PREVENCIÓN DE LOS FALLOS SISTEMÁTICOS DURANTE LAS DIFERENTES FASES DEL CICLO DE VIDA

Las tablas B.1 a B.5 de este anexo recomiendan, para cada nivel de integridad de seguridad, unas técnicas y unas medidas destinadas a evitar los fallos en los sistemas E/E/PE relacionados con la seguridad. El anexo B de la Norma CEI 61508-7 proporciona información suplementaria relativa a las técnicas y medidas aplicables. Los requisitos relativos a las medidas de control de los fallos se dan en el anexo A y se describen en el anexo A de la Norma CEI 61508-7.

No es posible enumerar cada causa física particular de los fallos sistemáticos, que aparecen durante el ciclo de vida de la seguridad o cada remedio aplicable, por dos razones principales:

- el efecto de un fallo sistemático depende de la fase del ciclo de vida durante el cual se ha introducido; y

- la eficacia de toda medida única que permite evitar los fallos sistemáticos depende de la aplicación.

Por lo tanto es imposible realizar un análisis cuantitativo de la prevención de los fallos sistemáticos.

Los fallos de los sistemas E/E/PE relacionados con la seguridad pueden clasificarse en función de la fase del ciclo de vida durante la cual una anomalía causal se introduce de la forma siguiente:

- fallos debidos a anomalías que aparecen **antes o durante la instalación del sistema** (por ejemplo, las anomalías del software que incluyen las anomalías de especificación y de programa, las anomalías del hardware que incluyen las anomalías de fabricación y una selección de componentes incorrecta); y

- fallos debidos a anomalías que aparecen **después de la instalación del sistema** (por ejemplo, fallos aleatorios del hardware o fallos debidos a una instalación incorrecta).

Para evitar o controlar estos fallos, una vez que han aparecido, son necesarias, en general, un gran número de medidas. La estructura de los requisitos proporcionada en los anexos A y B resulta de la división de las medidas en **medidas para evitar los fallos** durante las diferentes fases del ciclo de vida de la seguridad de los E/E/PES (este anexo) y las utilizadas para **controlar los fallos** durante la explotación (anexo A). Las medidas destinadas a controlar los fallos son características integradas de los sistemas E/E/PE relacionados con la seguridad mientras que las medidas destinadas a evitar los fallos son puestas en marcha durante el ciclo de vida de la seguridad.

Las tablas B.1 a B.5 proporcionan recomendaciones para un nivel de integridad de seguridad que indica, en primer lugar, la importancia de la técnica o de la medida y, en segundo lugar, la eficacia requerida si se utiliza esta técnica o medida. La importancia se describe de la manera siguiente:

- HR: la técnica o medida es altamente recomendada para ese nivel de integridad de seguridad. Si esta técnica o medida no se utiliza, los motivos subyacentes deben describirse de forma detallada;

- R: la técnica o medida es recomendada para ese nivel de integridad de seguridad. Se exige al menos una de las técnicas del grupo sombreado;

- –: la técnica o medida no aporta ninguna recomendación a favor o en contra de su utilización;

- NR: la técnica o medida no es recomendada en absoluto para ese nivel de integridad de seguridad. Si se utiliza esta técnica o medida, los motivos subyacentes deben describirse de forma detallada.

La eficacia requerida se describe de la forma siguiente:

– Obligatoria: la técnica o medida se requiere para todos los niveles de integridad de seguridad y debe utilizarse tan eficazmente como sea posible (es decir, aportando una alta eficacia).

– Baja: si se utiliza, la técnica o medida debe aplicarse en la medida necesaria para proporcionar al menos una baja eficacia contra los fallos sistemáticos.

– Media: si se utiliza, la técnica o medida debe aplicarse en la medida necesaria para proporcionar al menos una eficacia media contra los fallos sistemáticos.

– Alta: la técnica o medida debe aplicarse en la medida necesaria para proporcionar al menos una eficacia alta contra los fallos sistemáticos.

NOTA – La mayor parte de las medidas de las tablas B.1 a B.5 pueden utilizarse con una eficacia variable como indica la tabla B.6 que da ejemplos de eficacia baja y alta. El esfuerzo necesario para una eficacia media se sitúa entre la especificada para una eficacia baja y la especificada para una eficacia alta.

Si una medida no es obligatoria, puede, en principio, reemplazarse por otras medidas (bien tomadas separadamente, o bien en combinación); esto se rige por el sombreado de la zona correspondiente como se explica en cada tabla.

El hecho de conformarse con las directrices de este anexo no garantiza por sí mismo la integridad de seguridad. Es importante tener en cuenta los elementos siguientes:

– la coherencia de las técnicas y medidas elegidas así como la forma en la que se completen;

– las técnicas y medidas que convienen a cada fase del ciclo de vida del desarrollo; y

– las técnicas y medidas que son las mejor adaptadas a los problemas específicos encontrados durante el desarrollo de cada sistema E/E/PE diferente relacionado con la seguridad particular.

Tabla B.1
Recomendaciones para evitar los errores durante la especificación de los requisitos de los E/E/PES
(véase el apartado 7.2)

	Técnica/medida	Véase la Norma CEI 61508-7 (apartados)	SIL1	SIL2	SIL3	SIL4
	Gestión de proyecto	B.1.1	HR baja	HR baja	HR media	HR alta
	Documentación	B.1.2	HR baja	HR baja	HR media	HR alta
	Separación de los sistemas E/E/PE relacionados con las seguridad y de los sistemas no relacionados con la seguridad	B.1.3	HR baja	HR baja	HR media	HR alta
	Especificación estructurada	B.2.1	HR baja	HR baja	HR media	HR alta
	Inspección de la especificación	B.2.6	– baja	HR baja	HR media	HR alta
	Métodos semiformales	Apartado B.2.3, véase también el capítulo B.7 de la Norma CEI 61508-3	R baja	R baja	HR media	HR alta
	Listas de control	B.2.5	R baja	R baja	R media	R alta
	Herramientas de especificación asistida por ordenador	B.2.4	– baja	R baja	R media	R alta
	Métodos formales	B.2.2	– baja	– baja	R media	R alta

Todas las técnicas marcadas por “R” en el grupo sombreado son reemplazables, pero al menos una de estas se requiere.

Para la verificación de esta fase del ciclo de vida de la seguridad, debe utilizarse al menos una de las técnicas o medidas sombreadas en esta tabla o enumeradas en la tabla B.5.

NOTA 1 – Para el significado de las entradas en cada nivel de integridad de seguridad, véase el texto que precede a esta tabla.

NOTA 2 – En esta tabla, las medidas pueden utilizarse para hacer variar la eficacia de acuerdo con la tabla B.6 que proporciona ejemplo de eficacia baja y alta. El esfuerzo requerido para una eficacia media se encuentra entre la eficacia baja y la elevada.

NOTA 3 – La presentación general de las técnicas y medidas examinadas en esta tabla se proporciona en el anexo B de la Norma CEI 61508-7. Los apartados aplicables se referencian en la segunda columna.

Tabla B.2
Recomendaciones para evitar la introducción de anomalías durante el diseño y el desarrollo de los E/E/PES (véase el apartado 7.4)

	Técnica/medida	Véase la Norma CEI 61508-7 (apartados)	SIL1	SIL2	SIL3	SIL4
	Seguimiento de las directrices y normas	B.3.1	HR obligatoria	HR obligatoria	HR obligatoria	HR obligatoria
	Gestión de proyectos	B.1.1	HR baja	HR baja	HR media	HR alta
	Documentación	B.1.2	HR baja	HR baja	HR media	HR alta
	Diseño estructurado	B.3.2	HR baja	HR baja	HR media	HR alta
	Modularización	B.3.4	HR baja	HR baja	HR media	HR alta
	Utilización de los componentes probados	B.3.3	R baja	R baja	R media	R alta
	Métodos semiformales	Apartado B.2.3, véase también el capítulo B.7 de la Norma CEI 61508-3	R baja	R baja	HR media	HR alta
	Listas de control	B.2.5	– baja	R baja	R media	R alta
	Herramientas de diseño asistido por ordenador	B.3.5	– baja	R baja	R media	R alta
	Simulación	B.3.6	– baja	R baja	R media	R alta
	Inspección del hardware o sondeo del hardware	B.3.7 B.3.8	– baja	R baja	R media	R alta
	Métodos formales	B.2.2	– baja	– baja	R media	R alta

Todas las técnicas marcadas por “R” en el grupo sombreado son reemplazables, pero al menos una de estas se requiere.

Para la verificación de esta fase del ciclo de vida de la seguridad, debe utilizarse al menos una de las técnicas o medidas sombreadas en esta tabla o enumeradas en la tabla B.5.

NOTA 1 – Para el significado de las entradas en cada nivel de integridad de seguridad, véase el texto que precede a la tabla B.1.

NOTA 2 – En esta tabla, las medidas pueden utilizarse para hacer variar la eficacia de acuerdo con la tabla B.6 que proporciona ejemplo de eficacia baja y alta. El esfuerzo requerido para una eficacia media se encuentra entre la eficacia baja y la elevada.

NOTA 3 – La presentación general de las técnicas y medidas examinadas en esta tabla se proporciona en el anexo B de la Norma CEI 61508-7. Los apartados aplicables se referencian en la segunda columna.

Tabla B.3
Recomendaciones para evitar las anomalías durante la integración de los E/E/PES (véase el apartado 7.5)

	Técnica/medida	Véase la Norma CEI 61508-7 (apartados)	SIL1	SIL2	SIL3	SIL4
	Ensayos funcionales	B.5.1	HR obligatoria	HR obligatoria	HR obligatoria	HR obligatoria
	Gestión de proyecto	B.1.1	HR baja	HR baja	HR media	HR alta
	Documentación	B.1.2	HR baja	HR baja	HR media	HR alta
	Ensayo de “caja negra”	B.5.2	R baja	R baja	R media	R alta
	Eficacia probada	B.5.2	R baja	R baja	R media	R alta
	Ensayos estadísticos	B.5.3	– baja	– baja	R media	R alta

Todas las técnicas marcadas por “R” en el grupo sombreado son reemplazables, pero al menos una de estas se requiere.

Para la verificación de esta fase del ciclo de vida de la seguridad, debe utilizarse al menos una de las técnicas o medidas sombreadas en esta tabla o enumeradas en la tabla B.5.

NOTA 1 – Para el significado de las entradas en cada nivel de integridad de seguridad, véase el texto que precede a la tabla B.1.

NOTA 2 – En esta tabla, las medidas pueden utilizarse para hacer variar la eficacia de acuerdo con la tabla B.6 que proporciona ejemplo de eficacia baja y alta. El esfuerzo requerido para una eficacia media se encuentra entre la eficacia baja y la elevada.

NOTA 3 – La presentación general de las técnicas y medidas examinadas en esta tabla se proporciona en el anexo B de la Norma CEI 61508-7. Los apartados aplicables se referencian en la segunda columna.

Tabla B.4
Recomendaciones para evitar las anomalías y los fallos durante los procedimientos de explotación y de mantenimiento de los E/E/PES (véase el apartado 7.6)

	Técnica/medida	Véase la Norma CEI 61508-7 (apartados)	SIL1	SIL2	SIL3	SIL4
	Instrucciones de explotación y de mantenimiento	B.4.1	HR obligatoria	HR obligatoria	HR obligatoria	HR obligatoria
	Afabilidad en términos de utilización	B.4.2	HR obligatoria	HR obligatoria	HR obligatoria	HR obligatoria
	Afabilidad en términos de mantenimiento	B.4.3	HR obligatoria	HR obligatoria	HR obligatoria	HR obligatoria
	Gestión de proyecto	B.1.1	HR baja	HR baja	HR media	HR alta
	Documentación	B.1.2	HR baja	HR baja	HR media	HR alta
	Posibilidades de explotación limitadas	B.4.4	– baja	R baja	HR media	HR alta
	Protección contra los errores humanos	B.4.6	– baja	R baja	HR media	HR alta
	Explotación únicamente por operarios cualificados	B.4.5	– baja	R baja	R media	HR alta

Todas las técnicas marcadas por “R” en el grupo sombreado son reemplazables, pero al menos una de estas se requiere.

La verificación de esta fase del ciclo de vida de la seguridad debe realizarse por medio de listas de control (véase le apartado B.2.5 de la Norma CEI 61508-7) o por inspección (véase el apartado B.2.6 de la Norma CEI 61508-7).

NOTA 1 – Para el significado de las entradas en cada nivel de integridad de seguridad, véase el texto que precede a la tabla B.1.

NOTA 2 – En esta tabla, las medidas pueden utilizarse para hacer variar la eficacia de acuerdo con la tabla B.6 que proporciona ejemplo de eficacia baja y alta. El esfuerzo requerido para una eficacia media se encuentra entre la eficacia baja y la elevada.

NOTA 3 – La presentación general de las técnicas y medidas examinadas en esta tabla se proporciona en el anexo B de la Norma CEI 61508-7. Los apartados aplicables se referencian en la segunda columna.

Tabla B.5
Recomendaciones para evitar las anomalías durante la validación de la seguridad de los E/E/PES
(véase el apartado 7.7)

	Técnica/medida	Véase la Norma CEI 61508-7 (apartados)	SIL1	SIL2	SIL3	SIL4
	Ensayos funcionales	B.5.1	HR obligatoria	HR obligatoria	HR obligatoria	HR obligatoria
	Ensayos funcionales en las condiciones del entorno	B.6.1	HR obligatoria	HR obligatoria	HR obligatoria	HR obligatoria
	Ensayo de inmunidad a las interferencias/ y a las ondas de choque	B.6.2	HR obligatoria	HR obligatoria	HR obligatoria	HR obligatoria
	Ensayo de inserción de anomalías (cuando se requiera una cobertura de diagnóstico ≥ 90%)	B.6.10	HR obligatoria	HR obligatoria	HR obligatoria	HR obligatoria
	Gestión de proyecto	B.1.1	HR baja	HR baja	HR media	HR alta
	Documentación	B.1.2	HR baja	HR baja	HR media	HR alta
	Análisis estático, análisis dinámico y análisis de fallos	B.6.4 B.6.5 B.6.6	– baja	R baja	R media	R alta
	Simulación y análisis de fallos	B.3.6 B.6.6	– baja	R baja	R media	R alta
	Análisis del “caso más desfavorable”, análisis dinámico y análisis de fallos	B.6.7 B.6.5 B.6.6	– baja	– baja	R media	R alta
	Análisis estático y análisis de fallos (véase la nota 4)	B.6.4 B.6.6	R baja	R baja	NR	NR
	Ensayo funcional extendido	B.6.8	– baja	HR baja	HR media	HR alta
	Ensayos de “caja negra”	B.5.2	R baja	R baja	R media	R alta
	Ensayo de inserción de anomalías (cuando se requiera una cobertura de diagnostico < 90%)	B.6.10	R baja	R baja	R media	R alta
	Ensayos estadísticos	B.5.3	– baja	– baja	R media	R alta
	Ensayo del “caso más desfavorable”	B.6.9	– baja	– baja	R media	R alta
	Eficacia probada	B.5.4	R baja	R baja	R media	NR

Esta tabla se divida en tres grupos , como indica el sombreado de la barra lateral. Todas las técnicas marcadas con “R” en los grupos sombreados de color gris y negro pueden reemplazarse por otras técnicas de este mismo grupo, pero se requiere al menos una de las técnicas del grupo sombreado en gris (técnicas analíticas) y al menos una de las técnicas del grupo sombreado en negro (técnicas de ensayo).

NOTA 1 – Para el significado de las entradas en cada nivel de integridad de seguridad, véase el texto que precede a la tabla B.1.

NOTA 2 – En esta tabla, las medidas pueden utilizarse para hacer variar la eficacia de acuerdo con la tabla B.6 que proporciona ejemplo de eficacia baja y alta. El esfuerzo requerido para una eficacia media se encuentra entre la eficacia baja y la elevada.

NOTA 3 – La presentación general de las técnicas y medidas examinadas en esta tabla se proporciona en el anexo B de la Norma CEI 61508-7. Los apartados aplicables se referencian en la segunda columna.

NOTA 4 – No se recomienda el análisis estático ni el análisis de los fallos para los niveles SIL3 y SIL4 ya que estas técnicas no son suficientes a menos que sean utilizadas en asociación con un análisis dinámico.

Tabla B.6
Eficacia de las técnicas y medidas de prevención de fallos sistemáticos

Técnica /medida	Véase la Norma CEI 61508-7 (apartados)	Baja eficacia	Alta eficacia
Gestión de proyecto (véase la nota)	B.1.1	Definición de las acciones y responsabilidades; programación y asignación de los recursos; formación del personal correspondiente; verificación de coherencia después de las modificaciones	Validación independiente del diseño; supervisión de proyecto; procedimiento de validación normalizado; gestión de configuración; estadística de los fallos; ingeniería asistida por ordenador; ingeniería del software asistida por ordenador
Documentación (véase la nota)	B.1.2	Descripción en lenguaje gráfico y natural, por ejemplo, diagramas de bloques, diagramas de flujo	Directrices para el contenido consistente y la representación coherente de los documentos en toda la organización; listas de control del contenido; gestión de la documentación asistida por ordenador; control formal de las modificaciones
Separación entre sistemas E/E/PE relacionados con la seguridad y sistemas no relacionados con la seguridad	B.1.3	Interfaces bien definidas entre sistemas E/E/PE relacionados con la seguridad y sistemas no relacionados con la seguridad	Separación total entre los sistemas E/E/PE relacionados con la seguridad y los sistemas no relacionados con la seguridad, es decir, ningún intercambio de datos ni reemplazamientos físicos separados para evitar las influencias de causa común
Especificación estructurada	B.2.1	Separación jerárquica manual entre los subrequisitos; descripción de las interfaces	Separación jerárquica descrita utilizando herramientas informáticas de ayuda a la ingeniería; controles de coherencia automática; ajuste hasta el nivel de funcionamiento
Métodos formales	B.2.2	Utilizado por personal con experiencia en métodos formales	Utilizado por personal con experiencia en métodos formales para aplicaciones similares, por medio de herramientas informáticas
Métodos semiformales	B.2.3	Descripción de ciertas partes críticas por medio de métodos semiformales	Descripción del conjunto de los sistemas E/E/PE relacionados con la seguridad por medio de diferentes métodos semiformales para mostrar los diferentes aspectos, control de coherencia entre los métodos
Herramientas de especificación asistidas por ordenador	B.2.4	Herramientas sin ninguna preferencia por un método de diseño particular	Modelo de procedimientos orientados con subdivisión jerárquica, descripción de todos los objetos y de sus relaciones; base de datos común; control de coherencia automática
Listas de control	B.2.5	Listas de control preparadas para todas las fases del ciclo de vida de la seguridad; concentración sobre los principales problemas de seguridad	Listas de control detalladas preparadas para todas las fases del ciclo de vida de la seguridad
Inspección de la especificación	B.2.6	Inspección de la especificación de los requisitos de seguridad por una persona independiente	Inspección y revisión por un organismo independiente utilizando un procedimiento formal, con corrección de todas las anomalías encontradas
Diseño estructurado	B.3.2	Diseño jerárquico de los circuitos, producido manualmente	Reutilización de las partes del circuito enyadas; trazabilidad entre especificación, diseño, diagrama de circuito y listas de piezas; ayuda informática; basado sobre los métodos definidos (véase también el apartado 7.4.4)
Utilización de los componentes probados (véase la nota)	B.3.3	Sobredimensionamiento suficiente; características de construcción	Eficacia probada (véase el apartado 7.4.7.6)
Modularización (véase la nota)	B.3.4	Módulos de tamaño limitado; cada módulo funcionalmente aislado	Reutilización de los módulos probados; módulos fácilmente comprensibles; cada módulo tiene un máximo de una entrada, una salida y una salida de fallos

(Continúa)

Tabla B.6 *(Continuación)*
Eficacia de las técnicas y medidas de prevención de fallos sistemáticos

Técnica /medida	Véase la Norma CEI 61508-7 (apartados)	Baja eficacia	Alta eficacia
Herramientas de diseño asistido por ordenador	B.3.5	Soporte informático para las fases complejas del ciclo de vida de la seguridad	Utilización de herramientas que se han probado o validado (véase el apartado 7.4.7.6); desarrollo general informatizado para todas las fases del ciclo de vida de la seguridad
Simulación	B.3.6	Modelización al nivel modular, incluyendo los datos límites de las unidades periféricas	Modelización a nivel de componente, incluyendo los datos límites
Inspección del hardware	B.3.7	Inspección por una persona independiente del diseño	Inspección por un organismo independiente, utilizando un procedimiento formal con corrección de todas las anomalías encontradas
Sondeo del hardware	B.3.8	El sondeo incluye una persona independiente del diseño	El sondeo incluye un organismo independiente y seguir un procedimiento formal con corrección de todas las anomalías encontradas
Posibilidades de explotación limitadas (véase la nota)	B.4.4	Conmutador con clave o contraseña para regir los cambios del modo de explotación	Procedimiento definido y robusto para permitir la explotación
Explotación sólo para personal cualificado	B.4.5	Formación de base en el tipo de sistema de seguridad en explotación, más dos años de experiencia del trabajo correspondiente	Formación anual de todos los operarios; cada operario tiene al menos cinco años de experiencia en materia de dispositivos relacionados con la seguridad, en dos niveles de integridad de seguridad inferiores
Protección contra los errores humanos (véase la nota)	B.4.6	Acuse de recepción de entradas	Confirmación y controles de coherencia sobre cada comando de entrada
Ensayos de “caja negra” (véase la nota)	B.5.2	Clases de equivalencia y ensayos de partición de entradas, ensayos de los valores límites, utilizando los ensayos elementales previamente escritos	Ejecución del ensayo elemental a partir de diagramas causa consecuencia, combinando los casos críticos en los límites de explotación extremos
Ensayos estadísticos (véase la nota)	B.5.3	Repartición estadística de todos los datos de entrada	Informes de los ensayos realizados por medio de herramientas; ensayos elementales muy numerosos; repartición de los datos de entrada de acuerdo con las condiciones de aplicación reales y a los modelos de fallo supuestos
Eficacia probada (véase la nota)	B.5.4	10 000 h de tiempo de explotación; al menos un año de experiencia con al menos 10 dispositivos en diferentes aplicaciones; precisión estadística del 95%; ningún fallo crítico para la seguridad	10 millones de horas de tiempo de explotación; al menos dos años de experiencia con al menos 10 dispositivos en diferentes aplicaciones; precisión estadística de 99,9%; documentación detallada de todas las modificaciones (incluyendo las modificaciones menores) efectuadas durante una explotación anterior
Ensayo de inmunidad a las ondas de choque	B.6.2		Debe ser posible demostrar que la inmunidad a las ondas de choque es superior a los valores límites para las condiciones de funcionamiento reales
Análisis estático	B.6.4	Sobre la base de los esquemas funcionales; destacando los puntos débiles; especificando los ensayos elementales	Sobre la base de los diagramas detallados; previendo el comportamiento esperado durante los ensayos elementales; utilizando las herramientas de ensayo

(Continúa)

Tabla B.6 *(Fin)*
Eficacia de las técnicas y medidas de prevención de fallos sistemáticos

Técnica /medida	Véase la Norma CEI 61508-7 (apartados)	Baja eficacia	Alta eficacia
Análisis dinámico	B.6.5	Sobre la base de los esquemas funcionales; destacando los puntos débiles, especificando los ensayos elementales	Sobre la base de los diagramas detallados; previendo el comportamiento esperado durante los ensayos elementales; utilizando herramientas de ensayo
Análisis de fallos	B.6.6	A nivel de módulo, incluyendo los datos límites de las unidades periféricas	Al nivel de componente, incluyendo los datos límites
Análisis del "caso más desfavorable"	B.6.7	Realizado sobre las funciones relacionadas con la seguridad; deducidas utilizando combinaciones de valores límites para unas condiciones reales de funcionamiento	Realizado sobre las funciones normales; deducido utilizando combinaciones de valores límites para unas condiciones reales de funcionamiento
Ensayo funcional extendido	B.6.8	Ensayo que permite asegurar que las funciones relativas a la seguridad se mantienen en caso de estados de entradas estáticos debidos a un proceso defectuoso o a malas condiciones de explotación	Ensayo que permite asegurar que todas las funciones relacionadas con la seguridad se mantienen en caso de estados de entrada estáticos y/o cambios no habituales de entrada debidos a un proceso defectuoso o a malas condiciones de explotación (incluyendo las que podrían ser muy raras)
Ensayo del "caso más desfavorable"	B.6.9	Ensayo que permite asegurar que todas las funciones relacionadas con la seguridad se mantienen para una combinación de valores límites encontrados en unas condiciones de funcionamiento reales	Ensayo que permite asegurar que todas las funciones normales se mantienen para una combinación de valores límites encontrados en unas condiciones de explotación reales
Ensayo de inserción de anomalías	B.6.10	A nivel de subunidad incluyen datos límites o unidades periféricas	A nivel de componente incluyendo unos datos límites

NOTA – En el caso de las técnicas referenciadas B.1.1, B.1.2, B.3.3, B.3.4, B.4.4, B.4.6, B.5.2, B.5.3 y B.5.4, se supone, para una eficacia alta de la técnica o la medida, que las aproximaciones de baja eficacia también se utilizan.

ANEXO C (Normativo)

COBERTURA DEL DIAGNÓSTICO Y PROPORCIÓN DE FALLOS EN SEGURIDAD

C.1 Cálculo de la cobertura del diagnóstico y de la proporción de fallos en seguridad de un subsistema

La cobertura del diagnóstico y la proporción de fallos en seguridad de un subsistema debe calcularse de la forma siguiente:

a) Realizar el análisis de los modos de fallo y de sus efectos con el fin de determinar el efecto de cada modo de fallo de cada componente o grupo de componentes del subsistema sobre el comportamiento del sistema E/E/PE relacionado con la seguridad en ausencia de ensayos de diagnóstico. Debe estar disponible la información suficiente (véanse las notas 1 y 2) para facilitar el análisis de los modos de fallo y sus efectos así como para establecer un nivel de confianza apropiado en relación con los requisitos de integridad de seguridad.

NOTA 1 – Para comenzar este análisis, es necesaria la información siguiente:

- un diagrama detallado del sistema E/E/PE relacionado con la seguridad, describiendo los subsistemas con sus interconexiones para la parte del sistema E/E/PE que afecta a la función de seguridad considerada;
- el esquema del hardware del subsistema describiendo cada componente o grupo de componentes así como las interconexiones entre los componentes;
- los modos y niveles de fallo de cada componente o grupo de componentes y los porcentajes correspondientes a la probabilidad de fallo total para los fallos en seguridad y los fallos peligrosos.

NOTA 2 – El rigor necesario de este análisis depende de un gran número de factores (véase la Norma CEI 61508-1, apartado 4.1). En particular, conviene que el nivel de integridad de seguridad de las funciones de seguridad implicadas sea tenido en cuenta. Para los niveles de integridad de seguridad más elevados, el análisis de los modos de fallo y de sus efectos será más específico, en función de los tipos particulares de componentes y del entorno de la aplicación. Igualmente, un análisis exhaustivo y detallado es muy importante para un subsistema previsto para una utilización en una arquitectura del hardware que tiene una tolerancia nula a las anomalías del hardware.

b) Clasificar cada modo de fallo por categorías, según si da lugar (en ausencia de ensayos de diagnóstico) a:

- un fallo en seguridad (es decir, que no compromete la integridad de seguridad del sistema E/E/PE relacionado con la seguridad, por ejemplo un fallo que da lugar a una parada de seguridad o que no tiene impacto sobre la integridad de seguridad del sistema E/E/PE relacionado con la seguridad); o
- un fallo peligroso (es decir, que da lugar a un no funcionamiento de un sistema E/E/PE relacionado con la seguridad, o de una parte de este sistema, o que compromete a parte la integridad de seguridad del sistema E/E/PE relacionado con la seguridad.

c) A partir de una estimación de la probabilidad de fallo de cada componente o grupo de componentes, λ (véanse las notas 2 y 3) y de los resultados del análisis de los modos de fallo y de sus efectos, para cada componente o grupo de componentes, calcular la probabilidad de fallo en seguridad, λ_S, y la probabilidad de fallo peligroso, λ_D.

NOTA 3 – La probabilidad de fallo de cada componente o grupo de componentes es la probabilidad de aparición de una fallo en un periodo de tiempo relativamente corto, t. Puede considerarse igual a λ, nivel de fallo por unidad de tiempo, t, en el caso en el que λ_t es inferior a 1.

NOTA 4 – El nivel de fallo de cada componente o grupo de componentes puede estimarse sobre la base de datos que proviene de un origen industrial conocido, teniendo en cuenta el entorno de aplicación. De todos modos, son preferibles unos datos específicos de la aplicación, particularmente en el caso en el que el subsistema consta de un pequeño número de componentes y en donde el error en la estimación de las probabilidades de fallo en seguridad y de fallos peligrosos de un componente particular es susceptible de tener un impacto significativo sobre la estimación de la proporción de fallos en seguridad.

d) Para cada componente o grupo de componentes, estimar la proporción de fallos peligrosos que se detectan por los ensayos de diagnóstico (véase el capítulo C.2) y, en consecuencia, la probabilidad de fallos peligrosos detectados por los ensayos de diagnóstico, λ_{DD}.

e) Para el subsistema, calcular la probabilidad total de fallos peligrosos, $\Sigma\lambda_D$, la probabilidad total de fallos peligrosos detectados por los ensayos de diagnóstico, $\Sigma\lambda_{DD}$, y la probabilidad total de fallos en seguridad, $\Sigma\lambda_S$.

f) Calcular la cobertura del diagnóstico del subsistema como $\Sigma\lambda_{DD}/\Sigma\lambda_D$.

g) Calcular la proporción de fallos en seguridad del subsistema como $(\Sigma\lambda_S + \Sigma\lambda_{DD})/(\Sigma\lambda_S + \Sigma\lambda_D)$.

NOTA 5 – La cobertura del diagnóstico (en su caso) de cada subsistema E/E/PE relacionado con la seguridad se tiene en cuenta en el cálculo de la probabilidad de fallos aleatorios del hardware (véase al apartado 7.4.3.2.2). La proporción de fallos en seguridad se tiene en cuenta durante la determinación de las limitaciones de la arquitectura sobre la integridad de seguridad del hardware (véase el apartado 7.4.3.1).

El análisis para determinar la cobertura del diagnóstico y la proporción de fallos en seguridad debe cubrir todos los componentes, ya sean eléctricos, electromecánicos, mecánicos, etc., necesarios para permitir la ejecución de las funciones de seguridad del subsistema, según los requisitos del sistema E/E/PE relacionado con la seguridad. Todos los modos de fallos peligrosos posibles que conducen a un estado no seguro, impidiendo una respuesta en seguridad cuando se demanda dicha respuesta, o comprometiendo la integridad de seguridad del sistema E/E/PE relacionado con la seguridad, deben considerarse para cada uno de los componentes.

La tabla A.1 proporciona las anomalías y los fallos que deben, como mínimo, detectarse con el fin de realizar la cobertura de diagnóstico apropiada o que, como mínimo, deben formar parte de la determinación de la proporción de fallos en seguridad.

Si se utilizan unos datos experimentales en el análisis de los modos de fallo y de sus efectos, deben ser suficientes en relación con los requisitos de integridad de seguridad. Se requiere como mínimo, un límite inferior, unilateral, de confianza de al menos el 70%.

NOTA 6 – En el anexo C de la Norma CEI 61508-6 se integra un ejemplo de cálculo de la cobertura deL diagnóstico y de la proporción de fallos en seguridad.

NOTA 7 – Se dispone de otros métodos para el cálculo de la cobertura de diagnóstico, incluyendo, por ejemplo, la simulación de anomalías por utilización de un modelo informático que describe a la vez los circuitos del sistema E/E/PE relacionado con la seguridad y los componentes electrónicos utilizados para su diseño (por ejemplo, hasta el nivel del transistor en un circuito integrado).

C.2 Determinación de los factores de cobertura del diagnóstico

En el cálculo de la cobertura del diagnóstico para un subsistema (véase le capítulo C.1) es necesario estimar, para cada componente o grupo de componentes, la proporción de fallos peligrosos detectados por los ensayos de diagnóstico. Los ensayos del diagnóstico que pueden contribuir a la cobertura de diagnóstico incluyen, pero no están limitados a:

– las verificaciones por comparación, por ejemplo supervisión y comparación de señales redundantes;

– los ensayos periódicos integrados suplementarios, por ejemplo las sumas de verificación de una memoria;

– los ensayos por estímulos externos, por ejemplo el envío de una señal de pulso por las rutas de control;

– la supervisión de una señal analógica , por ejemplo para detectar los valores fuera de rango que indican el fallo de un sensor.

Con el fin de calcular la cobertura del diagnóstico, es necesario determinar los modos de fallo que se detectan por los ensayos de diagnóstico. Es posible que los fallos por circuitos abiertos o por cortocircuitos, para los componentes simples (resistencias, condensadores, transistores), sean detectables con una cobertura del 100%. De todos modos, para los componentes más complejos del tipo B (véase el apartado 7.4.3.1.3), conviene tener en cuenta las limitaciones presentadas en la tabla A.1 relativas a la cobertura de diagnóstico de varios componentes. Este análisis debe realizarse para cada componente o grupo de componentes y para cada subsistema de los sistemas E/E/PE relacionados con la seguridad.

NOTA 1 – Las tablas de la A.2 a la A.15 recomiendan técnicas y medidas para los ensayos del diagnóstico y la cobertura de diagnóstico máxima que puede anunciarse. Estos ensayos pueden ser permanentes o periódicos (en función del intervalo de ensayos de diagnóstico). Estas tablas no sustituyen a los requisitos del anexo C.

NOTA 2 – Puede proporcionarse un beneficio significativo de los ensayos de diagnóstico, en la realización de la seguridad funcional de un sistema E/E/PE relacionado con la seguridad. De todos modos, conviene prestar atención a no aumentar de forma no necesaria la complejidad que, por ejemplo, puede conducir a unas dificultades suplementarias durante las actividades de verificación, de validación, de evaluación de la seguridad funcional, de mantenimiento y de modificación. Una alta complejidad puede hacer más difícil el mantenimiento a largo plazo de la seguridad funcional del sistema E/E/PE relacionado con la seguridad.

NOTA 3 – Los cálculos de obtención de la cobertura del diagnóstico, y la forma de utilizarlos, suponen que el sistema E/E/PE relacionado con la seguridad se explota en seguridad en presencia de otro fallo peligroso detectado por los ensayos de diagnóstico. Si esta hipótesis no es correcta, el sistema E/E/PE relacionado con la seguridad debe tratarse como explotado en modo de alta demanda/continua (véanse los apartados 7.4.6.3 y 7.4.3.2.5).

NOTA 4 – La definición de la cobertura del diagnóstico se proporciona en el apartado 3.8.6 de la Norma CEI 61508-4. Es importante resaltar que algunas veces se tienen en cuenta otras definiciones de la cobertura de diagnóstico como hipótesis pero no son aplicables.

NOTA 5 – Los ensayos de diagnóstico utilizados para detectar un fallo peligroso en un subsistema pueden realizarse por otro subsistema del sistema E/E/PE relacionado con la seguridad.

NOTA 6 – Los ensayos de diagnóstico pueden ser permanentes o periódicos, en función del intervalo de ensayo de diagnóstico. Puede haber casos, o momentos, para los que conviene no realizar un ensayo de diagnóstico por la posibilidad de afectar, por un ensayo, el estado del sistema de forma negativa. En este caso, no puede anunciarse ningún beneficio, para los cálculos, de los ensayos de diagnóstico.

BIBLIOGRAFÍA

CEI 61000-4 – *Compatibilidad electromagnética. Parte 4: Técnicas de ensayo y de medida.*

NOTA – Armonizada como Norma EN 61000-4 (sin ninguna modificación).

CEI 60870-5-1:1990 – *Equipos y sistemas de control. Parte 5: Protocolos de transmisión. Sección 1: Formatos de tramas de transmisión.*

NOTA – Armonizada como Norma EN 60870-5-1:1993 (sin ninguna modificación).

CEI 61164:1995 – *Crecimiento de la fiabilidad. Ensayos y métodos de estimación estadísticos*.

EN 50159-1 – *Aplicaciones ferroviarias. Parte 1: Comunicación segura en sistemas de transmisión cerrados.*

EN 50159-2 – *Aplicaciones ferroviarias. Parte 2: Comunicación segura en sistemas de transmisión abiertos.*

ANSI/ISA-S84.01:1996 – *Aplicación de sistemas de seguridad con instrumentación para las industrias de proceso.*

ANSI/IEEE Std 352:1987 – *Guía IEEE sobre principios generales de análisis de fiabilidad de los sistemas de seguridad de centrales nucleares de generación de energía eléctrica.*

ANEXO ZA (Normativo)

OTRAS NORMAS INTERNACIONALES CITADAS EN ESTA NORMA CON LAS REFERENCIAS DE LAS NORMAS EUROPEAS CORRESPONDIENTES

Esta norma europea incorpora disposiciones de otras normas por su referencia, con o sin fecha. Estas referencias normativas se citan en los lugares apropiados del texto de la norma y se relacionan a continuación. Las revisiones o modificaciones posteriores de cualquiera de las normas citadas con fecha, sólo se aplican a esta norma europea cuando se incorporan mediante revisión o modificación. Para las referencias sin fecha se aplica la última edición de esa norma (incluyendo sus modificaciones).

NOTA – Cuando una norma internacional haya sido modificada por modificaciones comunes CENELEC, indicado por (mod), se aplica la EN/HD correspondiente.

Norma Internacional	Fecha	Título	EN/HD	Fecha	Norma UNE correspondiente[1)]
CEI 60050-371	1984	Vocabulario Electrotécnico Internacional (VEI). Capítulo 371: Telecontrol	–	–	UNE 21302-371:1991
CEI 60300-3-2	1993	Gestión de la confiabilidad. Parte 3: Guía de aplicación. Sección 2: Recogida de datos de confiabilidad en la explotación	–	–	UNE 200001-3-2:2001
CEI 61000-1-1	1992	Compatibilidad electromagnética (CEM). Parte 1: Generalidades. Sección 1: Aplicación e interpretación de definiciones y términos fundamentales	–	–	UNE 21000-1-1 IN:1997
CEI 61000-2-5	1995	Compatibilidad electromagnética (CEM). Parte 2: Entorno. Sección 5: Clasificación de entornos electromagnéticos. Norma básica de CEM	–	–	–
CEI 61508-1 + corr. mayo	1998 1999	Seguridad funcional de los sistemas eléctricos /electrónicos/electrónicos programables relacionados con la seguridad. Parte 1: Requisitos generales	EN 61508-1	2001	UNE-EN 61508-1:2003
CEI 61508-3 + corr. abril	1998 1999	Seguridad funcional de los sistemas eléctricos/ electrónicos/electrónicos programables relacionados con la seguridad. Parte 3: Requisitos del software (soporte lógico).	EN 61508-3	2001	UNE-EN 61508-3:2003
CEI 61508-4 + corr. abril	1998 1999	Seguridad funcional de los sistemas eléctricos/ electrónicos/electrónicos programables relacionados con la seguridad. Parte 4: Definiciones y abreviaturas	EN 61508-4	2001	UNE-EN 61508-4[2)]
CEI 61508-5 + corr. abril	1998 1999	Seguridad funcional de los sistemas eléctricos/ electrónicos/electrónicos programables relacionados con la seguridad. Parte 5: Ejemplos de métodos de determinación de los niveles de integridad de seguridad	EN 61508-5	2001	UNE-EN 61508-5:2003

(Continúa)

Norma Internacional	Fecha	Título	EN/HD	Fecha	Norma UNE correspondiente[1)]
CEI 61508-6	2000	Seguridad funcional de los sistemas eléctricos/ electrónicos/electrónicos programables relacionados con la seguridad. Parte 6: Directrices para la aplicación de las Normas CEI 61508-2 y CEI 61508-3	EN 61508-6	2001	UNE-EN 61508-6[2)]
CEI 61508-7	2000	Seguridad funcional de los sistemas eléctricos/ electrónicos/electrónicos programables relacionados con la seguridad. Parte 7: Presentación de técnicas y medidas	EN 61508-7	2001	UNE-EN 61508-7[2)]
Guía CEI 104	1997	Elaboración de las publicaciones de seguridad y utilización de las publicaciones fundamentales de seguridad y de las publicaciones de grupos de seguridad	–	–	–
Guía ISO/CEI 51	1990	Directrices para incluir en las normas los aspectos relacionados con la seguridad	–	–	–
IEEE 352	1987	Guía IEEE sobre principios generales de análisis de fiabilidad de los sistemas de seguridad de centrales nucleares de generación de energía eléctrica	–	–	–

1) Esta columna se ha introducido en el anexo original de la norma europea únicamente con carácter informativo a nivel nacional.
2) En preparación.

ANEXO NACIONAL (Informativo)

Las normas que se relacionan a continuación, citadas en esta norma europea, han sido incorporadas al cuerpo normativo UNE con los siguientes códigos:

Norma UNE	Título	Normas europeas e internacionales
UNE-EN 50159-1	Aplicaciones ferroviarias. Sistemas de comunicación, señalización y procesamiento. Parte 1: Comunicación segura en sistemas de transmisión cerrados	EN 50159-1
UNE-EN 50159-2	Aplicaciones ferroviarias. Sistemas de comunicación, señalización y procesamiento. Parte 2: Comunicación segura en sistemas de transmisión abiertos	EN 50159-2
UNE-EN 61000-4, serie	Compatibilidad electromagnética (CEM). Parte 4: Técnicas de ensayo y de medida	EN 61000-4, serie CEI 61000-4, serie
UNE-EN 61164[2)]	Crecimiento de la fiabilidad. Ensayos y métodos de estimación estadísticos	EN 61164[2)] CEI 61164
EN 60870-5-1[1)]	Equipos y sistemas de control. Parte 5: Protocolos de transmisión. Sección 1: Formatos de troncos de transmisión.	EN 60870-5-1 CEI 60870-5-1

1) Ratificada por AENOR.
2) En preparación.

AENOR Asociación Española de Normalización y Certificación

Dirección C Génova, 6
28004 MADRID-España

Teléfono 91 432 60 00

Fax 91 310 40 32