NORMA CUBANA

NC

IEC 61508-3: 2012
(Publicada por la IEC en el 1998)

SEGURIDAD FUNCIONAL DE LOS SISTEMAS ELÉCTRICOS/ELECTRÓNICOS/ ELECTRÓNICOS PROGRAMABLES RELACIONADOS CON LA SEGURIDAD — PARTE 3: REQUISITOS DEL SOFTWARE (SOPORTE LÓGICO) (IEC 61508-3: 1998 + Corr. 1999)

Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 3: Software requirements.

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 de la versión oficial en español de la Norma Europea EN 61508-3: 2001 *Functional safety of electrical/programmable electronic safety-related systems. Part 3: Software requirements* que a su vez adopta de forma idéntica a la Norma Internacional IEC 61508-3: 1998 + Corr 1999 de igual título.

Oficina Nacional de Normalización (NC)
Calle E No. 261, El Vedado, La Habana, Habana 4, Cuba.

Impreso en Cuba.

NORMA EUROPEA
EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

EN 61508-3

Diciembre 2001

ICS 25.040.40

Versión en español

Seguridad funcional de los sistemas eléctricos/electrónicos/ electrónicos programables relacionados con la seguridad Parte 3: Requisitos del software (soporte lógico)

(CEI 61508-3:1998 + Corrigendum 1999)

Functional safety of electrical/electronic/ programmable electronic safety-related systems.
Part 3: Software requirements.
(IEC 61508-3:1998 + Corrigendum 1999).

Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité.
Partie 3: Prescriptions concernant les logiciels.
(CEI 61508-3:1998 + Corrigendum 1999).

Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/ programmierbarer elektronischer Systeme.
Teil 3: Anforderungen an Software.
(IEC 61508-3:1998 + Corrigendum 1999).

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

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 61508-3:1998 y su corrigendum de abril de 1999 fue aprobado por CENELEC como norma europea sin ninguna modificación.

ÍNDICE

Páginas

Tablas

Figuras

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 3: Requisitos del software (soporte lógico)

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 de las Normas CEI 61508-1 y CEI 61508-2.

b) Se aplica a todo software[1)] que forma parte de un sistema relacionado con la seguridad, o utilizado para desarrollar un sistema relacionado con la seguridad entrando en el campo de aplicación de las Normas CEI 61508-1 y CEI 61508-2. Este tipo de software se denomina “software relacionado con la seguridad”.

   – Los software relacionados con la seguridad comprenden los sistemas de explotación, los software del sistema, los software de las redes de comunicación, las funciones de la interfaz hombre-máquina, las herramientas de soporte y los micro-software, así como la programación de las aplicaciones.

   – Los programas de aplicaciones incluyen los programas de alto nivel, de bajo nivel y los programas especificados en los lenguajes de variabilidad limitada (véase el apartado 3.2.7 de la Norma CEI 61508-4).

c) Necesita que se precisen las funciones de seguridad del software y los niveles de integridad de seguridad.

   NOTA 1 – Si ya ha sido realizado en el marco de la especificación de los sistemas E/E/PE relacionados con la seguridad (véase el apartado 7.2 de la Norma CEI 61508-2), no es necesario repetirlo en esta parte.

   NOTA 2 – Especificar las funciones de seguridad y los niveles de integridad de seguridad del software es un proceso iterativo; véanse las figuras 2 y 6.

   NOTA 3 – Véanse el capítulo 5 y el anexo A de la Norma CEI 61508-1 para la estructura de la documentación. Esta estructura puede tener en cuenta los procesos internos de la empresa y los procesos de trabajo de los sectores de aplicación especificados.

d) Establece los requisitos relativos a las fases y actividades del ciclo de vida de la seguridad que se deben aplicar durante el diseño y el desarrollo del software relacionado con la seguridad (modelo del ciclo de vida de la seguridad del software). Estos requisitos incluyen la aplicación de medidas y de técnicas que siguen una graduación basada en el nivel de integridad de seguridad, con el fin de evitar y de controlar los fallos y las averías del software.

e) Proporciona los requisitos para las informaciones relativas a la validación de la seguridad del software y se deben transmitir a la organización realizando la integración de los E/E/PES.

f) Proporciona los requisitos para la preparación de las informaciones y de los procedimientos relativos al software requeridos por el usuario para el funcionamiento y el mantenimiento de un sistema E/E/PE relacionado con la seguridad.

g) Proporciona los requisitos que deben observarse por la organización realizando las modificaciones del software relacionado con la seguridad.

h) Proporciona, de acuerdo con las Normas CEI 61508-1 y CEI 61508-2, los requisitos para las herramientas de soporte tales como las herramientas de diseño y desarrollo, los traductores de lenguaje, las herramientas de ensayo y la puesta a punto y las herramientas de gestión de la configuración.

   NOTA 4 – Las figuras 4 y 6 muestran las relaciones entre las Normas CEI 61508-2 y CEI 61508-3.

---

1) En esta norma se utilizan los términos "software" y "hardware", para los que también se utilizan los términos "soporte lógico" y "soporte físico".

1.2 Las partes 1, 2, 3 y 4 de esta norma son publicaciones básicas de seguridad, aunque este estado no es 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 – En Estados Unidos de América y en Canadá, las normas nacionales existentes de seguridad de procesos, basadas en la Norma CEI 61508 (por ejemplo, la Norma ANSI/ISA S84.01:1996) pueden aplicarse en el sector de procesos, en lugar de la Norma CEI 61508, hasta que una norma correspondiente a la Norma CEI 61508 (es decir, la Norma CEI 61511), para el sector de procesos, sea publicada en Estados Unidos y Canadá.

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 61508-3 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.

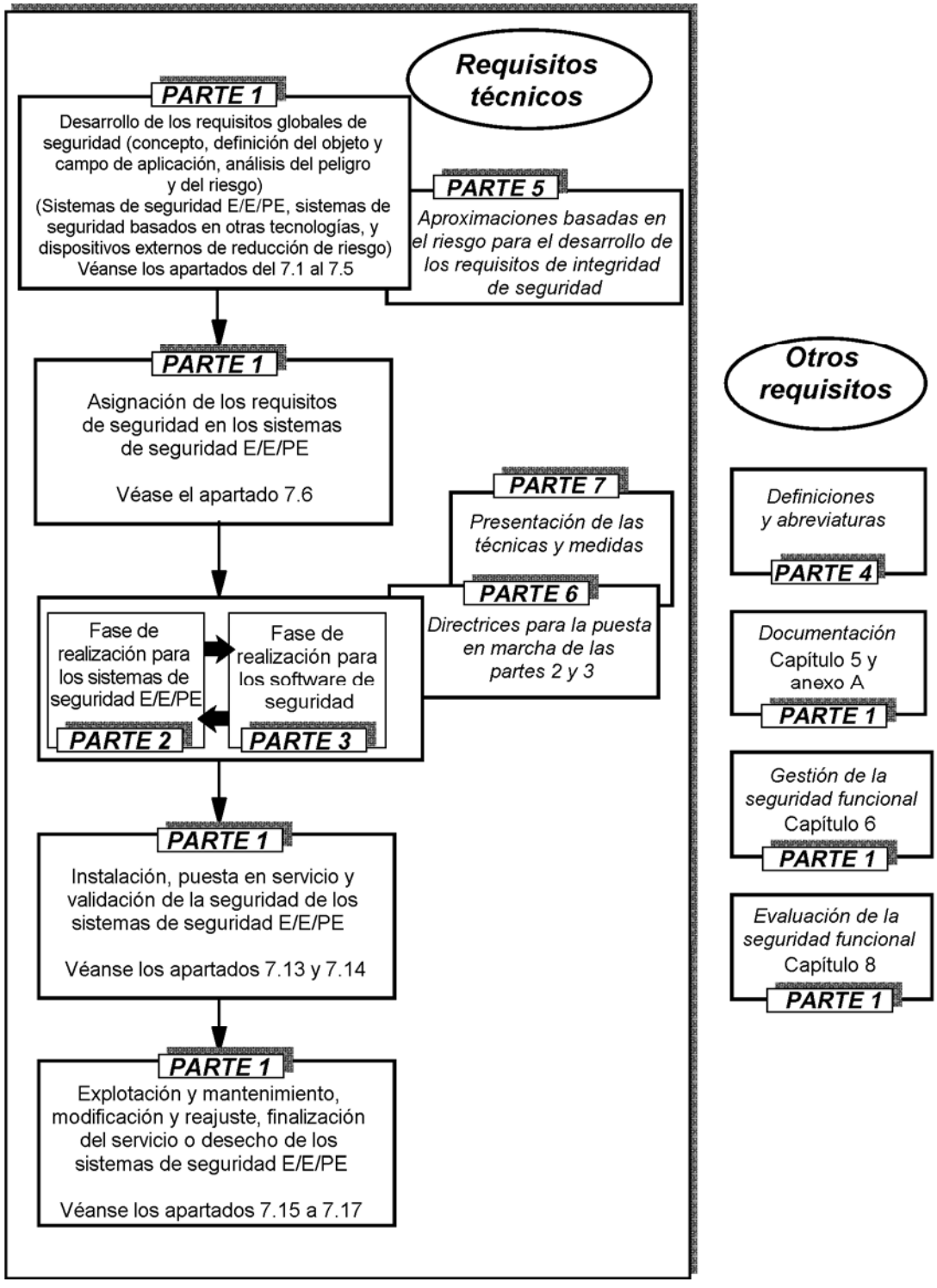


Fig. 1 – Estructura general de la Norma CEI 61508

2 NORMAS PARA CONSULTA

Las normas que a continuación se relacionan contienen disposiciones válidas para esta norma internacional. En el momento de la publicación las ediciones indicadas estaban en vigor. Toda norma está sujeta a revisión por lo que las partes que basen sus acuerdos en esta norma internacional deben estudiar la posibilidad de aplicar la edición más reciente de las normas indicadas a continuación. Los miembros de CEI y de ISO poseen el registro de las normas internacionales en vigor en cada momento.

CEI 61508-1:1998 – *Seguridad funcional de los sistemas eléctricos/electrónicos/electrónicos programables relacionados con la seguridad. Parte 1: Requisitos generales.*

CEI 61508-2:2000 – *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.*

CEI 61508-4:1998 – *Seguridad funcional de los sistemas eléctricos/electrónicos/electrónicos programables relacionados con la seguridad. Parte 4: Definiciones y abreviaturas.*

CEI 61508-5:1998 – *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.*

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.*

CEI 61508-7:2000 – *Seguridad funcional de los sistemas eléctricos/electrónicos/electrónicos programables relacionados con la seguridad. Parte 7: Presentación de técnicas y medidas.*

Guía ISO/CEI 51:1990 – *Directrices para incluir en las normas los aspectos relacionados con la seguridad.*

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.*

3 DEFINICIONES Y ABREVIATURAS

Las definiciones y abreviaturas utilizadas en esta norma se encuentran en la Norma CEI 61508-4.

4 CONFORMIDAD CON ESTA NORMA

Los requisitos de conformidad de esta norma se encuentran en el capítulo 4 de la Norma CEI 61508-1.

5 DOCUMENTACIÓN

Los objetivos y requisitos relativos a la documentación se encuentran en el capítulo 5 de la Norma CEI 61508-1.

6 SISTEMA DE GESTIÓN DE LA CALIDAD DEL SOFTWARE

6.1 Objetivos

Los objetivos se detallan en el apartado 6.1 de la Norma CEI 61508-1.

6.2 Requisitos

6.2.1 Los requisitos incluyen los que se detallan en el apartado 6.2 de la Norma CEI 61508-1 así como los requisitos adicionales siguientes.

6.2.2 La planificación de la seguridad funcional debe definir la estrategia para el aprovisionamiento, el desarrollo, la integración, la verificación, la validación y la modificación del software en los límites requeridos por el nivel de seguridad del sistema E/E/PE relacionado con la seguridad.

NOTA – La filosofía de este acercamiento es utilizar la planificación de la seguridad funcional como una oportunidad de adaptar esta norma para tener en cuenta la integridad de seguridad variable requerida por los componentes de los sistemas E/E/PE relacionados con la seguridad. Conviene tener en consideración el apartado 7.4.2.8 de la parte 3 cuando los componentes de nivel de integridad de seguridad diferente se utilicen juntos en un sistema E/E/PE relacionado con la seguridad.

6.2.3 Conviene que la gestión de la configuración del software

a) controle administrativa y técnicamente, a lo largo del ciclo de vida de la seguridad del software, la gestión de las modificaciones del software, asegurando la conformidad permanente de los requisitos específicos de seguridad del software;

b) garantice que todas las operaciones necesarias se han realizado para demostrar que el nivel requerido de integridad de seguridad del software se ha alcanzado;

c) mantenga de forma precisa y por medio de una única identificación todos los elementos de configuración que son necesarios para mantener el sistema E/E/PE relacionado con la seguridad. La configuración comprende al menos los elementos siguientes: requisitos y análisis de seguridad, documentos de diseño y de especificación del software, módulos de código fuente del software, planes de ensayo y resultados, paquetes y componentes de software preexistentes que tienen que ser incorporados al sistema E/E/PE relacionado con la seguridad y todas las herramientas y entornos de desarrollo que se utilizan para crear, probar o realizar una acción sobre el software del sistema E/E/PE relacionados con la seguridad;

d) aplique los procesos de control de las modificaciones con el fin de impedir toda modificación no autorizada; documentar las demandas de modificación; analizar el impacto de una modificación propuesta; y aprobar o rechazar la demanda de modificación; documentar los detalles y las autorizaciones para todas las modificaciones aprobadas; establecer la línea de referencia de la configuración de los puntos clave apropiados en el desarrollo del software, y documentar el ensayo de integración (parcial) que justifica la línea de referencia 7.8); garantizar la composición y la construcción, de todas las líneas de referencia del software (incluyendo la reconstrucción de las líneas de referencia precedentes);

NOTA 1 – Decisiones de gestión y autoridades necesitan dirigir y hacer cumplir el uso de controles técnicos y administrativos.

e) documente las informaciones siguientes con el fin de permitir una auditoría ulterior: estado de la configuración, estado de las versiones, justificación y aprobación de todas las modificaciones, y detalles de las modificaciones;

f) documente de manera formal la versión del software relacionado con la seguridad. Conviene conservar las copias originales del software y toda la documentación asociada con el fin de permitir el mantenimiento de la modificación durante la explotación de la versión del software.

NOTA 2 – Para más información sobre los procesos de gestión de la configuración, véase la Norma ISO/CEI 12207.

7 REQUISITOS RELATIVOS AL CICLO DE VIDA DE LA SEGURIDAD DEL SOFTWARE

7.1 Generalidades

7.1.1 Objetivo. El objetivo de los requisitos de este apartado es estructurar el desarrollo del software mediante fases y actividades definidas (véase la tabla 1 y las figuras 2 a 5).

7.1.2 Requisitos

7.1.2.1 Se debe seleccionar y especificar un ciclo de vida de seguridad para el desarrollo del software durante la planificación de la seguridad de acuerdo con el capítulo 6 de la Norma CEI 61508-1.

NOTA – Puede resultar necesario un modelo del ciclo de vida de seguridad particularizado para las necesidades particulares del proyecto o la organización, que cumpla los requisitos del capítulo 7 de la Norma CEI 61508-1.

7.1.2.2 Los procedimientos que aseguran la calidad y la seguridad se deben integrar en las actividades del ciclo de vida de la seguridad.

7.1.2.3 Cada fase del ciclo de vida de la seguridad del software se debe dividir en actividades elementales con el dominio de aplicación, las entradas y las salidas específicas para cada fase.

NOTA 1 – Para cualquier información complementaria relativa a las fases del ciclo de vida, véase la Norma ISO/CEI 12207.

NOTA 2 – El capítulo 5 de la Norma CEI 61508-1 tiene en cuenta las salidas de las fases del ciclo de vida de la seguridad. Durante el desarrollo de algunos sistemas E/E/PE relacionados con la seguridad, la salida de algunas fases del ciclo de vida de la seguridad puede ser un documento distinto ya que las salidas documentadas de varias fases se pueden fusionar. El requisito principal es que la salida de la fase del ciclo de vida de la seguridad se adapte al objetivo previsto. Para los desarrollos simples, algunas fases del ciclo de vida de la seguridad también se pueden fusionar. (véase el apartado 7.4.5).

7.1.2.4 A condición de que el ciclo de vida de la seguridad del software satisfaga los requisitos de la figura 3 y de la tabla 1, se acepta adaptar la profundidad, el número y la cantidad de trabajo de las fases del modelo en V (véase la figura 5), con el fin de tener en cuenta la integridad de seguridad y la complejidad del proyecto.

NOTA – La lista completa de las fases del ciclo de vida realizado en la tabla 1 conviene para los grandes sistemas nuevamente desarrollados. Para los sistemas pequeños, puede ser apropiado, por ejemplo, fusionar las fases de diseño del sistema de software y de diseño de la arquitectura.

7.1.2.5 Se acepta ordenar el proyecto de software de forma diferente de la organización de esta norma (es decir, utilizar otro modelo de ciclo de vida de la seguridad) con la condición de que todos los objetivos y requisitos de este capítulo sean cumplidos.

7.1.2.6 Para cada fase del ciclo de vida, se deben utilizar las técnicas y medidas apropiadas. Los anexos A y B (guía para la selección de técnicas y medidas) proporcionan recomendaciones. Seleccionar las técnicas en los anexos A y B no garantizan que la integridad de seguridad requerida se alcance.

7.1.2.7 Los resultados de las actividades del ciclo de vida de la seguridad del software se deben documentar (véase el capítulo 5).

7.1.2.8 Si, en un estado cualquiera del ciclo de vida de la seguridad del software, se necesita realizar una modificación soportada sobre una fase precedente del ciclo de vida, esta fase precedente del ciclo de vida de la seguridad se debe repetir así como las fases siguientes.

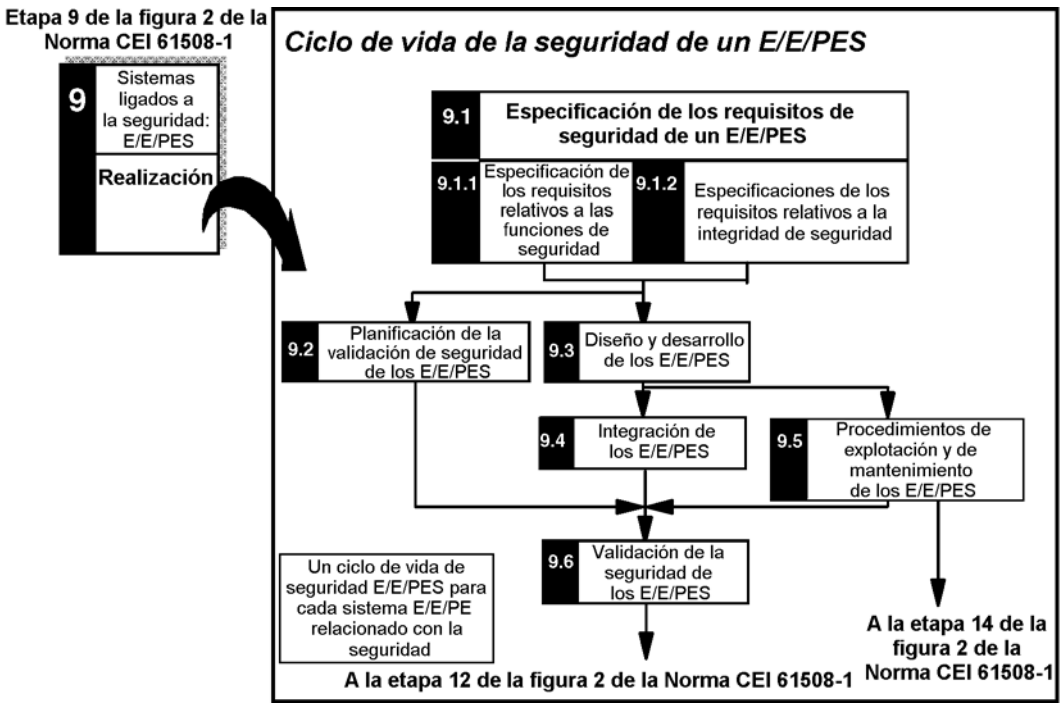


Fig. 2 – Ciclo de vida de seguridad de un E/E/PES (en fase de realización)

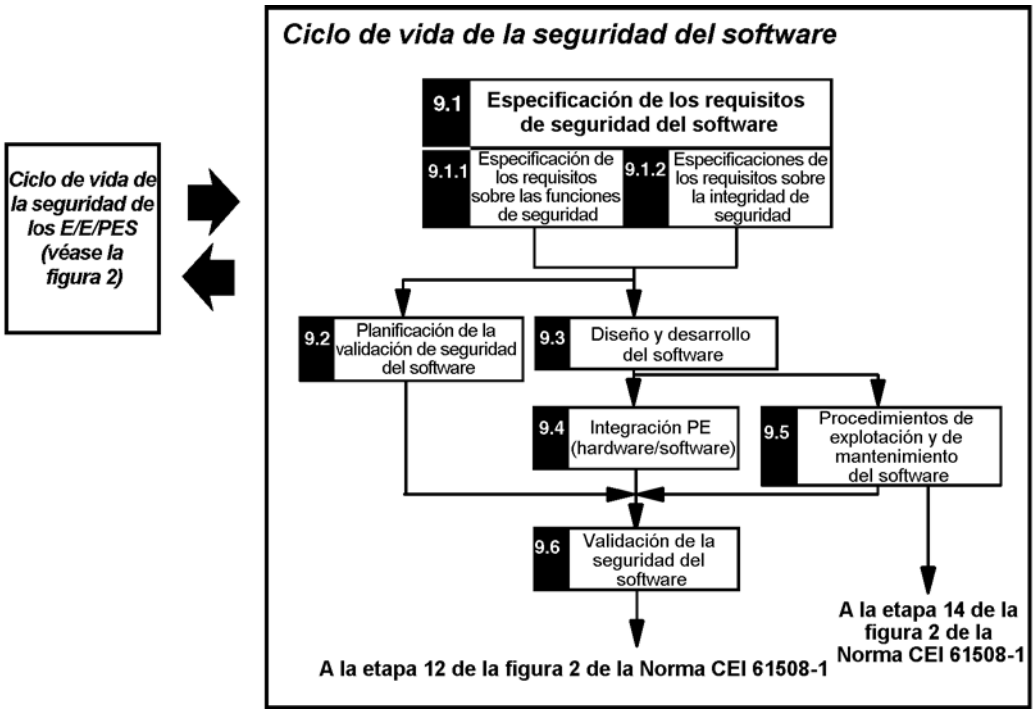


Fig. 3 – Ciclo de vida de seguridad del software (en fase de realización)

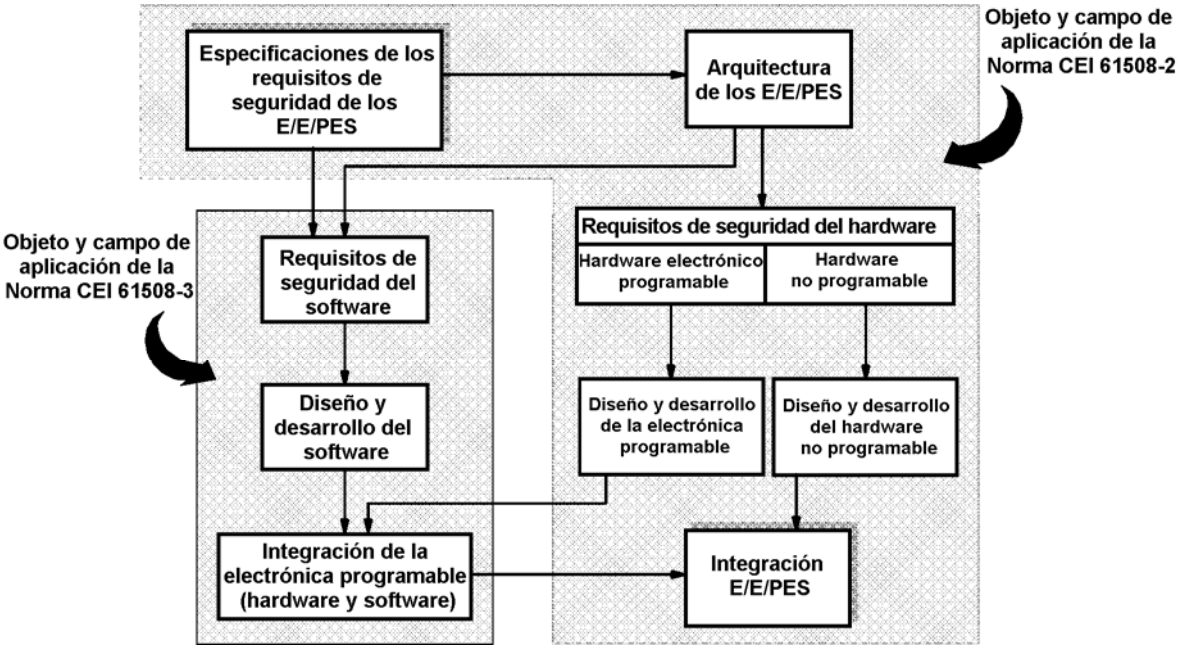


Fig. 4 – Relaciones entre la Norma CEI 61508-2 y la Norma CEI 61508-3 y sus objetos y campos de aplicación respectivos

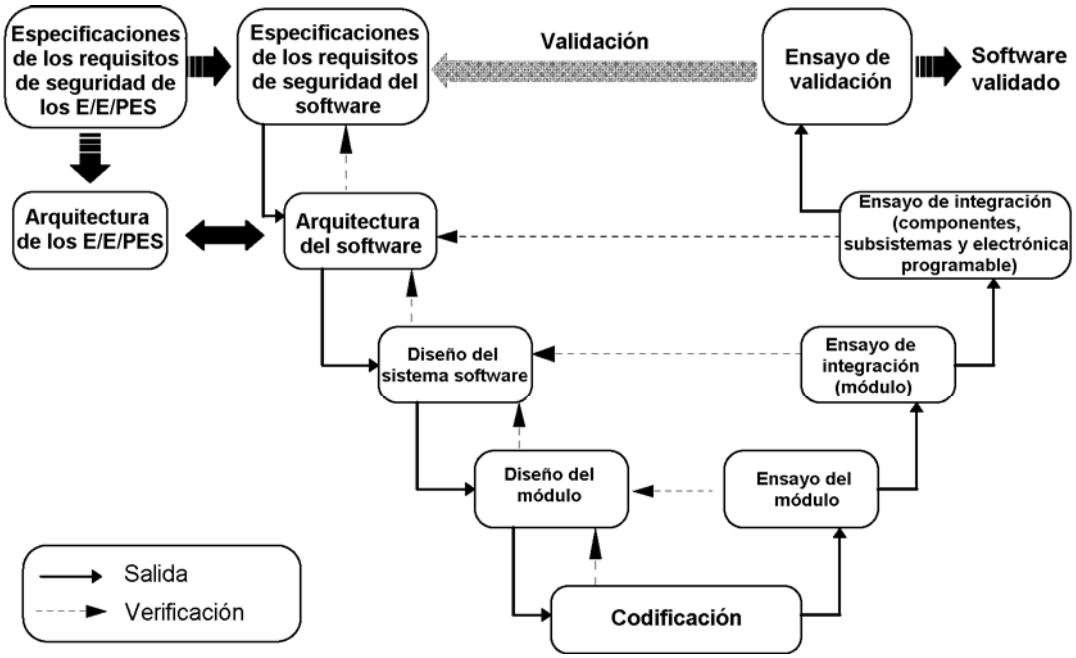


Fig. 5 – Integridad de seguridad del software y ciclo de vida del desarrollo (modelo en V)

Tabla 1
Ciclo de vida de la seguridad del software: presentación

Fase del ciclo de vida de la seguridad		Objetivos	Objeto y campo de aplicación	Apartado de los requisitos	Entradas (información requerida)	Salidas (información producida)
Número de etapa de la figura 3	Título					
9.1	Especificación de los requisitos de seguridad del software	Especificar los requisitos de seguridad el software relativos a los requisitos de las funciones de seguridad del software y los requisitos de integridad de seguridad del software; Especificar los requisitos de las funciones de seguridad del software para cada sistema E/E/PE relacionado con la seguridad necesario para la implantación de las funciones de seguridad requeridas; Especificar los requisitos de integridad de seguridad del software para cada sistema E/E/PE relacionado con la seguridad permitiendo alcanzar el nivel de integridad de seguridad específico para cada función de seguridad que se le atribuye	PES; Sistema de software	7.2.2	Especificación de los requisitos de seguridad de los E/E/PES (Norma CEI 61508-2).	Especificación de los requisitos de seguridad del software
9.2	Planificación de la validación de la seguridad del software	Desarrollar un plan permitiendo validar la seguridad del software	PES; Sistema de software	7.3.2	Especificación de los requisitos de seguridad del software	Plan de validación de la seguridad del software
9.3	Diseño y desarrollo del software	**Arquitectura:** Crear una arquitectura del software de acuerdo con los requisitos específicos para la seguridad del software en relación al nivel de integridad de seguridad requerida; Revisar y evaluar los requisitos impuestos al software por la arquitectura del hardware del sistema E/E/PE relacionado con la seguridad, incluyendo las consecuencias de las interacciones Hardware/software sobre la seguridad del equipo bajo control	PES; Sistema de software	7.4.3	Especificación de los requisitos de seguridad del software; Diseño de la arquitectura del hardware E/E/PES (Norma CEI 61508-2).	Descripción del diseño de la arquitectura del software; Especificación del ensayo de integración de la arquitectura del software; Especificación del ensayo de integración del software/electrónico programable (idéntico al requerido en la Norma CEI 61508-2).
9.3	Diseño y desarrollo del software	**Herramientas de soporte y lenguajes de programación**: Seleccionar un conjunto adecuado de herramientas de ayuda a la verificación, validación, evaluación y modificación, incluyendo lenguajes y compiladores, para el nivel de integridad de seguridad requerido durante el ciclo de vida de la seguridad completa del software	PES; Sistema de software; Herramientas de soporte; Lenguaje de programación	7.4.4	Especificación de los requisitos de seguridad del software; Descripción del diseño de la arquitectura del software	Herramientas de desarrollo y reglas de codificación; Selección de las herramientas de desarrollo

(Continúa)

Tabla 1 *(Continuación)*
Ciclo de vida de la seguridad del software: presentación

Fase del ciclo de vida de la seguridad		Objetivos	Objeto y campo de aplicación	Apartado de los requisitos	Entradas (información requerida)	Salidas (información producida)
Número de etapa de la figura 3	Título					
9.3	Diseño y desarrollo del software	**Diseño detallado (diseño del sistema del software):** Diseñar e implementar un software que responda a los requisitos específicos para la seguridad del software de acuerdo con los niveles de integridad de seguridad requerido, que sea analizable y verificable, y que sea modificable en toda seguridad	Principales componentes y subsistemas del diseño de la arquitectura del software	7.4.5	Descripción del diseño de la arquitectura del software; Herramientas de soporte y reglas de codificación	Especificación del diseño del software; Especificación del ensayo de integración del sistema del software
9.3	Diseño y desarrollo del software	**Diseño detallado (diseño del módulo del software individual):** Diseñar e implementar un software que responda a los requisitos específicos para la seguridad del software de acuerdo con los niveles de integridad de seguridad requerido, que sea analizable y verificable, y que sea modificable en toda seguridad	Diseño del sistema del software	7.4.5	Especificación del diseño del sistema del software; Herramientas de soporte y reglas de codificación	Especificación del diseño del módulo del software; Especificación del ensayo del módulo del software
9.3	Diseño y desarrollo del software	**Implantación del diseño detallado:** Diseñar e implementar un software que responda a los requisitos específicos para la seguridad del software de acuerdo con los niveles de integridad de seguridad requerido, que sea analizable y verificable, y que sea modificable en toda seguridad	Módulos de los software individuales	7.4.6	Especificación del diseño del módulo del software; Herramientas de soporte y reglas de codificación	Listado de los códigos fuente; Informe de revisión del código
9.3	Diseño y desarrollo del software	**Ensayo del módulo del software:** Verificar que los requisitos para la seguridad del software (en términos de funciones de seguridad de los software requeridos y de la integridad de seguridad del software) se cumplen para mostrar que cada módulo del software ejecuta su función prevista y no ejecuta ninguna función no prevista	Módulos de los software	7.4.7	Especificación del ensayo del módulo del software; Listado del código fuente; Informe de revisión del código	Resultados de los ensayos del módulo del software; Módulos del software verificados y probados
9.3	Diseño y desarrollo del software	**Ensayo de integración del software:** Verificar que los requisitos para la seguridad del software (en términos de funciones de seguridad de los software requeridos y de la integridad de seguridad del software) se cumplen para mostrar que cada módulo del software ejecuta su función prevista y no ejecuta ninguna función no prevista	Arquitectura del software; Sistema del software	7.4.8	Especificación del ensayo de integración del sistema del software	Resultados del ensayo de integración del sistema del software; Sistema del software verificado y probado

(Continúa)

Tabla 1 *(Fin)*
Ciclo de vida de la seguridad del software: presentación

Fase del ciclo de vida de la seguridad		Objetivos	Objeto y campo de aplicación	Apartado de los requisitos	Entradas (información requerida)	Salidas (información producida)
Número de etapa de la figura 3	Título					
9.4	Integración de la electrónica programable (hardware y software)	Integrar el software en el hardware electrónico programable objetivo; Combinar el software y el hardware en la electrónica programable relacionada con la seguridad para asegurar su compatibilidad y respuesta a los requisitos del nivel de integridad de seguridad previsto	Hardware electrónico programable; Software integrado	7.5.2	Especificación del ensayo de integración de la arquitectura del software; Especificación del ensayo de integración de la electrónica programable (idéntica a la requerida en la Norma CEI 61508-2); Electrónica programable integrada	Resultados del ensayo de integración de la arquitectura del software; Resultados del ensayo de integración de la electrónica programable; Electrónica programable integrada, verificada y probada
9.5	Procedimientos de explotación y de modificación del software	Recopilar las informaciones y los procedimientos relativos al software permitiendo asegurar el mantenimiento de la seguridad funcional del sistema E/E/PE relacionado con la seguridad durante la explotación y las modificaciones	El mismo que las fases anteriores	7.6.2	Todas las entradas de arriba, según el caso	Procedimientos de explotación y de modificación del software
9.6	Validación de la seguridad del software	Asegurarse que el sistema integrado está de acuerdo con los requisitos especificados para la seguridad del software al nivel de la integridad de seguridad previsto	El mismo que las fases anteriores	7.7.2	Plan de validación de la seguridad del software	Resultados de validación de la seguridad del software; Software validado
–	Modificación del software	Realizar las correcciones, las mejoras o las adaptaciones del software validado asegurando el mantenimiento del nivel de integridad de seguridad del software	El mismo que las fases anteriores	7.8.2	Procedimientos de modificación del software; Petición de modificación del software	Resultados del análisis del impacto de la modificación del software; Registro de las modificaciones del software
–	Verificación del software	En los límites impuestos por el nivel de integridad de seguridad, probar y evaluar las salidas de una fase dada del ciclo de vida de la seguridad del software con el fin de verificar la conformidad y la coherencia en relación a las salidas y a las normas proporcionadas en la entrada de esta fase	Depende de la fase	7.9.2	Plan de verificación apropiado (en función de la fase)	Informe de verificación apropiado (en función de la fase)
–	Evaluación de la seguridad funcional del software	Buscar y llegar a un juicio sobre la seguridad funcional alcanzada por los sistemas E/E/PE relacionados con la seguridad	Todas las fases anteriores	8	Plan de la evaluación de la seguridad funcional del software	Informe de evaluación de la seguridad funcional del software

7.2 Especificación de los requisitos de seguridad del software

NOTA 1 – Véanse también las tablas A.1 y B.7.

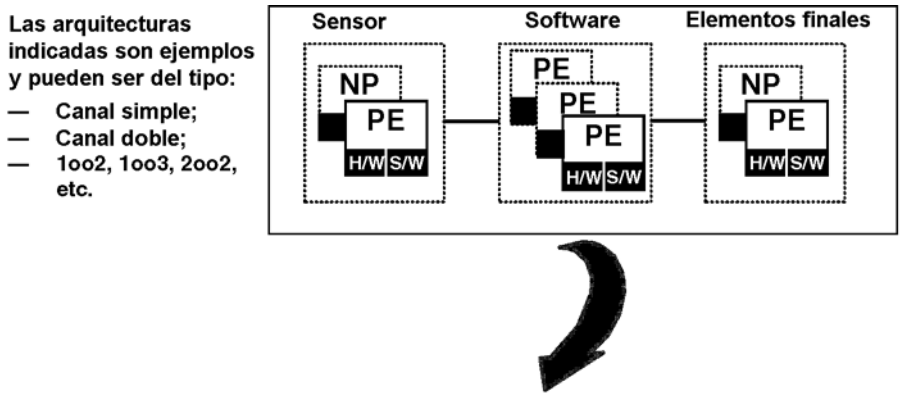
NOTA 2 – Esta fase corresponde a la etapa 9.1 de la figura 3.

7.2.1 Objetivos

7.2.1.1 El primer objetivo de los requisitos de este apartado es especificar los requisitos de seguridad del software incluyendo los requisitos relativos a las funciones de seguridad del software y los requisitos relativos a la integridad de seguridad del software.

7.2.1.2 El segundo objetivo de los requisitos de este apartado es especificar los requisitos relativos a las funciones de seguridad del software para cada sistema E/E/PE relacionado con la seguridad necesaria para implementar las funciones de seguridad requeridas.

7.2.1.3 El tercer objetivo de los requisitos de este apartado es especificar los requisitos relativos a la integridad de seguridad del software para cada sistema E/E/PE relacionado con la seguridad permitiendo alcanzar el nivel de integridad de seguridad específico para cada función de seguridad atribuida a este sistema E/E/PE relacionado con la seguridad.



Arquitectura de la electrónica programable		
Arquitectura del hardware PE	**Arquitectura del software PE (la arquitectura del software incluye los software incorporados y los software de aplicación)**	
Características generales y específicas de la aplicación relativa al hardware PE. Ejemplos: — Ensayos de diagnóstico; — Procesadores redundantes; — Tarjetas E/S duales.	**Software incorporado PE**	**Software de aplicación PE**
	Ejemplos: — Controladores de la comunicación; — Gestión de fallos; — Software ejecutable.	Ejemplos: — Funciones de entrada/salida; — Funciones derivadas (por ejemplo verificación de los sensores si no proporciona el servicio del software incorporado).

Leyenda:

PE	**Electrónico programable**
NP	**Equipo no programable**
H/W	**Hardware**
S/W	**Software**
MooN	**M sobre N (por ejemplo 1oo2 es 1 sobre 2)**

Fig. 6 – Relación entre las arquitecturas del hardware y del software para la electrónica programable

7.2.2 Requisitos

NOTA – Estos requisitos se satisfarán, en la mayoría de los casos, por combinación del software incorporado y del software de aplicación. Esta combinación de los dos que se requiere para lograr las características cumplirán los siguientes apartados. La separación exacta entre el software general y el software específico de la aplicación dependen de la arquitectura del software elegida (véase el apartado 7.4.3 y la figura 6).

7.2.2.1 Si los requisitos para la seguridad del software ya han sido especificados en los requisitos para el sistema E/E/PE relacionado con la seguridad (véase el apartado 7.2 de la Norma CEI 61508-2), no es necesario repetir la especificación de los requisitos de seguridad del software.

7.2.2.2 La especificación de los requisitos relacionados con la seguridad del software se debe derivar de los requisitos de seguridad especificados del sistema E/E/PE relacionado con la seguridad (Véase la Norma CEI 61508-2), y de todo requisito de la planificación de la seguridad (véase el capítulo 6). Estas informaciones deben estar disponibles para el desarrollo del software.

NOTA – Este requisito no significa una ausencia de iteración entre el desarrollo del E/E/PES y el desarrollo del software (Normas CEI 61508-2 y CEI 61508-3). A medida que los requisitos de seguridad del software y la arquitectura del software (véase el apartado 7.4.3) se precisan, existe un impacto en las arquitecturas del hardware de los E/E/PES, y por esta razón es esencial que exista una cooperación muy próxima entre el desarrollo del hardware y del software. Véase la figura 4.

7.2.2.3 La especificación de los requisitos para la seguridad del software debe estar suficientemente detallada para permitir obtener la integridad de seguridad requerida durante el diseño y la implantación, y permitir una evaluación de la seguridad funcional.

NOTA – El nivel de detalle de la especificación puede variar en función de la aplicación.

7.2.2.4 El programador del software debe revisar las informaciones del apartado 7.2.2.2 con el fin de asegurarse que los requisitos están correctamente especificados. Particularmente, se debe tener en cuenta:

a) las funciones de seguridad;

b) la configuración o la arquitectura del sistema;

c) los requisitos de integridad de seguridad del hardware (electrónica programable, sensores y accionadores);

d) los requisitos de integridad de seguridad del software;

e) los rendimientos de capacidad y el tiempo de respuesta;

f) las interfaces operador y equipo.

7.2.2.5 El programador del software debe establecer los procedimientos para resolver cualquier divergencia relativa a la atribución del nivel de integridad de seguridad del software.

7.2.2.6 En los límites impuestos para el nivel de integridad de seguridad, los requisitos especificados para la seguridad del software se deben expresar y estructurar de forma

a) clara, precisa, unívoca, verificable, ensayable, mantenible y realizable, y que corresponda al nivel de integridad de seguridad;

b) rastreable en relación con las especificaciones de los registros de seguridad del sistema E/E/PE relacionado con la seguridad;

c) exentos de toda terminología y descripción ambigua y/o susceptible de mal interpretarse por los usuarios del documentos en cualquier etapa del ciclo de vida de la seguridad del software.

7.2.2.7 Si no se han definido de forma adecuada en los requisitos de seguridad del sistema E/E/PE relacionado con la seguridad, todos los modos de explotación relativas al equipo bajo control se deben detallar en los requisitos para la seguridad del software.

NOTA – Este requisito se cumple en la mayoría de los casos por combinación del software general incorporado y el software específico de la aplicación. Esta combinación se requiere para alcanzar las características que satisfagan las exigencias. La separación exacta entre el software general y el software específico de la aplicación depende de la arquitectura del software elegida (véase el apartado 7.4.3 y la figura 6).

7.2.2.8 La especificación de los requisitos de seguridad del software debe especificar y documentar toda limitación entre el hardware y el software, relacionado con la seguridad o importante para ella.

7.2.2.9 En los límites impuestos por la descripción del diseño de la arquitectura del equipo E/E/PE, la especificación de los requisitos de seguridad del software debe tener en cuenta:

a) la auto-vigilancia del software (véanse los ejemplos C.2.5 y C.3.10 de la Norma CEI 61508-7);

b) la vigilancia del equipo electrónico programable, de los sensores y de los accionadores;

c) los ensayos periódicas de las funciones de seguridad durante la explotación del sistema;

d) la posibilidad de probar las funciones de seguridad mientras el equipo bajo control está en explotación.

7.2.2.10 Mientras el sistema E/E/PE relacionado con la seguridad se requiere para ejecutar funciones que no son de seguridad, los requisitos especificados para la seguridad del software deben identificar claramente estas funciones.

7.2.2.11 La especificación de los requisitos de seguridad del software debe expresar las propiedades de seguridad requeridas del producto, pero no del proyecto. En referencia a los apartados del 7.2.2.1 al 7.2.2.10, se deben especificar los siguientes puntos, según el caso:

a) Los requisitos para las funciones de seguridad del software:
   - funciones que permitan al equipo bajo control alcanzar o mantener un estado de seguridad;
   - funciones ligadas a la detección, señalización y gestión de las averías del hardware electrónico programable;
   - funciones ligadas a la detección, señalización y gestión de las averías de los sensores y accionadores;
   - funciones ligadas a la detección, señalización y gestión de las averías del software propiamente dicho (auto-vigilancia del software);
   - funciones ligadas a los ensayos periódicas de las funciones en línea;
   - funciones ligadas a los ensayos periódicas de las funciones fuera de línea;
   - funciones que permiten la modificación segura del PES;
   - interfaces con funciones no relacionadas con la seguridad;
   - rendimientos de capacidad y tiempo de respuesta;
   - interfaces entre el software y el PES.

   NOTA 1 – Las interfaces incluyen las facilidades de programación en línea y fuera de línea.

b) El requisito para la integridad de seguridad del software:
   - el o los niveles de integridad de seguridad requeridos para cada una de las funciones mencionadas en el apartado a) anterior.

   NOTA 2 – Véase el anexo A de la Norma CEI 61508-5 para cualquier información relativa a la asignación de la integridad de seguridad de los componentes del software.

7.3 Planificación de la validación de seguridad del software

NOTA – Esta fase corresponde a la etapa 9.2 de la figura 3.

7.3.1 Objetivo. El objetivo de los requisitos de este apartado es elaborar un plan para validar la seguridad del software.

7.3.2 Requisitos

7.3.2.1 La planificación se debe realizar con el fin de especificar las etapas, de proceso o técnicas, que serán utilizadas para demostrar que el software satisface los requisitos de seguridad (véase el apartado 7.2).

7.3.2.2 El plan para validar la seguridad del software debe tener en cuenta lo siguiente:

a) los detalles sobre cuando tendrá lugar la validación;

b) los detalles relativos a las personas que deben realizar la validación;

c) la identificación de los modos de explotación relativos al equipo bajo control, incluyendo:

   – los preparativos de utilización, incluyendo la inicialización y el ajuste;

   – el arranque, el aprendizaje, el modo automático, el modo manual, el modo semiautomático y el funcionamiento en estado estable;

   – la puesta a cero, la parada y el mantenimiento;

   – las condiciones anormales razonablemente previsibles;

d) la identificación del software relacionado con la seguridad necesitando una validación para cada modo de explotación del equipo bajo control antes de la puesta en servicio;

e) la estrategia técnica de la validación (por ejemplo los métodos analíticos, los ensayos estadísticas, etc.) (véase el apartado 7.3.2.3);

f) en consonancia con el punto e), las medidas (técnicas) y los procedimientos que se deben utilizar para confirmar cada función de seguridad deben ser de acuerdo con con los requisitos especificados para las funciones de seguridad del software (véase el apartado 7.2) y con los requisitos especificados para la integridad de seguridad del software (véase el apartado 7.2);

g) referencia específica a los requisitos especificados para la seguridad del software (véase el apartado 7.2);

h) el entorno requerido en el que las actividades de validación deben tener lugar (por ejemplo, para los ensayos, este entorno incluye las herramientas calibradas así como los equipos de ensayos);

i) los criterios de aceptación o de rechazo (véase el apartado 7.3.2.5);

j) las políticas y los procedimientos de evaluación de los resultados de validación, en particular en lo que concierne a los resultados que conducen al rechazo.

NOTA – Estos requisitos se basan en las especificaciones generales descritas en el apartado 7.8 de la Norma CEI 61508-1.

7.3.2.3 La estrategia técnica relativa a la validación de un software relacionado con la seguridad (véase la tabla A.7) debe incluir las siguientes informaciones:

a) la elección entre las técnicas manuales o automáticas, o las dos;

b) la elección entre las técnicas estáticas o dinámicas, o las dos;

c) la elección entre las técnicas analíticas o estáticas, o las dos.

7.3.2.4 En el marco del procedimiento de validación de un software relacionado con la seguridad, el objeto y campo de aplicación y el contenido de la planificación para validar la seguridad del software se deben revisar con un evaluador o un representante del evaluador, si se requiere por el nivel de integridad de seguridad (véase el apartado 8.2.12 de la Norma CEI 61508-1). Este procedimiento debe contener una cláusula relativa a la presencia del evaluador durante el ensayo.

7.3.2.5 Los criterios de aceptación o de rechazo del ensayo de validación del software deben incluir:

a) las señales de entrada requeridas con sus secuencias y sus valores;

b) las señales de salida previstas con sus secuencias y sus valores;

c) los otros criterios de evaluación, tales como la utilización de la memoria, la sincronización y las tolerancias aplicables a los valores.

7.4 Diseño y desarrollo del software

NOTA – Esta fase es la etapa 9.3 de la figura 3.

7.4.1 Objetivos

7.4.1.1 El primer objetivo de los requisitos de este apartado es crear una arquitectura del software satisfaciendo los requisitos especificados para la seguridad del software (véase el apartado 7.2) en función del nivel de integridad de seguridad requerido.

7.4.1.2 El segundo de los objetivos de los requisitos de este apartado es revisar y evaluar los requisitos impuestos al software por la arquitectura del hardware del sistema E/E/PE relacionado con la seguridad, incluyendo las consecuencias de las interacciones hardware/software del E/E/PE sobre la seguridad del equipo bajo control.

7.4.1.3 El tercer objetivo de los requisitos de este apartado es seleccionar un conjunto adecuado de herramientas de ayuda a la verificación, validación, evaluación y modificación, incluyendo lenguajes y compiladores, para el nivel de integridad de seguridad requerido durante el ciclo de vida de la seguridad completo del software.

7.4.1.4 El cuarto objetivo de los requisitos de este apartado es diseñar e implementar un software que responda a los requisitos especificados para la seguridad del software (véase el apartado 7.2) en función del nivel de integridad de seguridad requerido, que sea analizable y verificable, y que sea modificable de forma segura.

7.4.1.5 El quinto objetivo de los requisitos de este apartado es verificar que los requisitos de seguridad del software (en términos de funciones de seguridad del software requeridas y de integridad de seguridad del software) se logren.

7.4.2 Requisitos generales

7.4.2.1 En función de la naturaleza del desarrollo del software, la responsabilidad en lo referente a los requisitos mencionados en el apartado 7.4 incumbe solo al suministrador, solo al usuario, o a los dos juntos. La atribución de responsabilidades se debe determinar durante la planificación de la seguridad (véase el capítulo 6).

7.4.2.2 De acuerdo con el nivel de integridad de seguridad requerida, el método de diseño elegido debe tener unas características que faciliten:

a) la abstracción, la modularidad y otras características para controlar la complejidad;

b) la expresión

- de la funcionalidad,
- del flujo de información entre los componentes,
- de la secuencia y de las informaciones ligadas al tiempo,

- de los límites de tiempo,
- de los conflictos de acceso,
- de las estructuras dadas y de sus propiedades,
- de las hipótesis de diseño y sus propiedades;

c) la comprensión por los programadores y todos los que necesitan entender el diseño;

d) la verificación y la validación.

NOTA – Véanse también las tablas en los anexos A y B.

7.4.2.3 La ensayabilidad y la aptitud a la modificación segura se deben tener en cuenta durante las actividades de diseño con el fin de facilitar la puesta en marcha de estas propiedades en el sistema final relacionado con la seguridad.

NOTA – Como ejemplo, se citan los modos de mantenimiento en las industrias de máquinas-herramientas y de procesos.

7.4.2.4 El método de diseño elegido debe tener unas características que faciliten la modificación del software. Estas características permiten por ejemplo la modularidad, ocultar la información, y encapsulación.

7.4.2.5 La representación del diseño se debe basar en una notación claramente definida o limitada a las características claramente definidas.

7.4.2.6 En la medida de lo posible, el diseño debe minimizar la parte del software relacionado con la seguridad.

7.4.2.7 Cuando el software debe implementar a la vez unas funciones de seguridad y unas funciones que no son de seguridad, entonces el software en su conjunto se debe considerar como relacionado con la seguridad, a menos que sea posible demostrar al nivel del diseño la independencia de las funciones de forma apropiada.

7.4.2.8 Cuando el software debe implementar unas funciones de seguridad correspondientes a los distintos niveles de integridad de seguridad, el software en su conjunto se debe considerar como perteneciente al nivel de integridad de seguridad más alto, a menos que se demuestre al nivel de diseño una independencia suficiente de las funciones de seguridad correspondientes a los diferentes niveles de integridad de seguridad. La justificación de la independencia de las funciones se debe documentar.

NOTA – Es necesario que el nivel de integridad de seguridad del software sea al menos tan alto como el nivel de integridad de seguridad de la función de seguridad a la que pertenece. Sin embargo, el nivel de integridad de seguridad de un componente del software puede ser inferior al nivel de integridad de seguridad de la función de seguridad a la que el componente del software pertenece si el componente está combinado con otros componentes del hardware, de forma que el nivel de integridad de seguridad de la combinación sea al menos igual a la de la función de seguridad.

7.4.2.9 En la medida de lo posible, el diseño debe incluir las funciones lógicas para ejecutar los ensayos periódicos y todos los ensayos de diagnóstico de forma que satisfaga el requisito de integridad de seguridad del sistema E/E/PE relacionado con la seguridad (así como lo expuesto en la Norma CEI 61508-2).

7.4.2.10 El diseño del software debe incluir, en función del nivel de integridad de seguridad requerido, una auto-vigilancia de los flujos de control y de los flujos de datos. En caso de detección de una avería, se deben tomar las medidas apropiadas. Véanse las tablas A.2 y A.4.

7.4.2.11 Si un software normalizado o desarrollado anteriormente se utiliza para el diseño (véanse las tablas A.3 y A.4), debe ser claramente identificado. La capacidad del software para satisfacer la especificación de los requisitos de seguridad del software (véase el apartado 7.2) se debe justificar. Esta capacidad del software se debe establecer a partir de la constatación de un funcionamiento satisfaciendo en una aplicación similar, o de la aplicación de los mismos procedimientos de verificación y de validación que aquellos a los se someten los software desarrollados que son nuevos. Conviene evaluar las limitaciones impuestas por el entorno del software precedente (por ejemplo las dependencias al sistema de explotación y al compilador).

NOTA – La justificación se puede realizar durante la planificación de la seguridad (véase el capítulo 6).

7.4.2.12 Este apartado (7.4) debe, en la medida de lo posible, aplicarse a todos los datos, incluyendo los lenguajes de generación de los datos.

7.4.3 Requisitos relativos a la arquitectura del software

NOTA 1 – Véanse también las tablas A.2 y B.7.

NOTA 2 – La arquitectura del software define los principales componentes y subsistemas del software, cómo están interconectados, cómo los atributos requeridos, en particular la integridad de seguridad, se obtienen. Los principales componentes del software incluyen normalmente los sistemas de explotación, las bases de datos, los subsistemas de entrada/salida de la instalación, los subsistemas de comunicación, el o los programas de aplicación, las herramientas de programación y de diagnóstico, etc.

NOTA 3 – En algunos sectores industriales, la arquitectura del software se llama “descripción funcional” o “especificación de diseño funcional” (aunque estos documentos también incluyen el hardware).

NOTA 4 – Para la programación de la aplicación del usuario en los lenguajes de variabilidad limitada, particularmente en los PLC (véase el anexo E de la Norma CEI 61508-6), la arquitectura se proporciona por el suministrador como una característica estándar del PLC. El suministrador será requerido, en el marco de esta norma, para garantizar al usuario la conformidad de los productos con los requisitos mencionados en el apartado 7.4. El usuario adapta el PLC a su aplicación programando en forma estándar, por ejemplo en el lenguaje de "lógica en cascada". Los requisitos de los apartados del 7.4.3 al 7.4.8 también se aplican. El requisito de definir y documentar la arquitectura se puede considerar como una información utilizable por el usuario para seleccionar el PLC (o equivalentemente) para su aplicación.

NOTA 5 – Por otro lado, en algunas aplicaciones incorporadas utilizan un lenguaje de variabilidad total como, por ejemplo, una máquina controlada por un microprocesador, será necesario que el suministrador cree una arquitectura especial para esa aplicación (o clase de aplicación). El usuario, normalmente, no dispone de medios de programación. En este caso, el suministrador es el responsable de la conformidad de su producto con los requisitos mencionados en el apartado 7.4.

NOTA 6 – Algunos sistemas pertenecen a los dos tipos de sistemas mencionados en las notas 4 y 5. El usuario y el suministrador se reparten en consecuencia la responsabilidad de la conformidad.

NOTA 7 – Bajo el punto de vista de la seguridad, en la fase de la arquitectura del software es donde se desarrolla la estrategia de seguridad básica para el software.

7.4.3.1 Dependiendo del tipo de desarrollo del software, la responsabilidad en lo relativo a la conformidad con los requisitos mencionados en el apartado 7.4.3 puede incumbir solamente al suministrador, sólo al usuario, o a los dos juntos (véanse las notas anteriores). La repartición de la responsabilidad se debe documentar durante la planificación de la seguridad (véase el capítulo 6).

7.4.3.2 El diseño de la arquitectura del software propuesto debe definirse por el suministrador y/o el programador y debe realizarse una descripción detallada de dicho diseño. La descripción debe:

a) seleccionar y justificar un conjunto íntegro de técnicas y de medidas necesarias durante la fase del ciclo de vida de la seguridad del software para satisfacer la especificación de los requisitos de seguridad del software en función del nivel de integridad de seguridad requerido (véase el apartado 7.2). Estas técnicas y medidas incluyen las estrategias de diseño del software para la tolerancia a los fallos (coherente con el hardware) y para evitar los fallos, incluyendo (cuando sea apropiado) la redundancia y la diversidad;

b) basarse sobre una partición en subsistemas/componentes, con las informaciones siguientes realizadas por cada uno de ellos:

   – subsistema/componente nuevo, existente o propietario;

   – subsistema/componente verificado anteriormente o no y, si ha sido verificado, condiciones de la verificación;

   – subsistema/componente relacionado o no con la seguridad;

   – nivel de integridad de seguridad del subsistema/componente;

c) determinar todas las interacciones hardware/software, y evaluar y detallar su importancia;

d) utilizar una notación para representar la arquitectura definida de forma no ambigua o limitada a las características definidas de forma no ambigua;

e) seleccionar las características de arquitectura a utilizar para mantener la integridad de seguridad de todos los datos. Estos datos incluyen los datos de entrada/salida de la instalación, los datos de comunicación, los datos de la interfaz del operador, los datos de mantenimiento y los de la base de datos interna;

f) especificar los ensayos de integración de la arquitectura lógica apropiadas para asegurar que esta arquitectura satisface la especificación de los requisitos para la seguridad del software en función del nivel de integridad de seguridad requerido (véase el apartado 7.2).

7.4.3.3 Toda modificación de los requisitos de seguridad específicos del sistema E/E/PE relacionado con la seguridad después de la aplicación del apartado 7.4.3.2 debe estar de acuerdo con el programador del sistema E/E/PE y documentarse.

NOTA – Habrá inevitablemente interacción entre la arquitectura del hardware y la arquitectura del software (véase la figura 5). Por lo tanto, es necesario discutir con el programador del hardware los problemas relativos a, por ejemplo, la especificación de los ensayos para la integración del software y del hardware de la electrónica programable (véase el apartado 7.5).

7.4.4 Requisitos relativos a las herramientas de soporte y a los lenguajes de programación

NOTA 1 – Véase también la tabla A.3.

NOTA 2 – La elección de las herramientas de desarrollo dependerá de la naturaleza de las actividades de desarrollo del software y de la arquitectura del software (véase el apartado 7.4.3).

- Para la programación de la aplicación del usuario en un lenguaje de variabilidad limitada a bajos niveles de integridad de seguridad, se permite que los lenguajes de programación y las herramientas requeridas se limiten a los lenguajes PLC normalizados y a los programas de edición y de carga. La responsabilidad del cumplimiento del apartado 7.4.4 incumbirá principalmente al suministrador.

- Para los niveles de integridad de seguridad superiores, es necesaria la utilización de los subconjuntos limitados de lenguaje PLC y las herramientas de verificación y validación tales como los analizadores de código y los simuladores. En este caso, la responsabilidad incumbe a la vez al suministrador y al usuario.

- Las herramientas para las aplicaciones incorporadas que utilizan un lenguaje de variabilidad total deberán estar más detalladas, igual que para los niveles de integridad inferiores. La responsabilidad del cumplimiento del apartado 7.4.4 incumbirá principalmente al programador del software. Esto se aplica al suministrador del lenguaje PLC que utilizaría lenguajes de variabilidad total en la elaboración del lenguaje de variabilidad limitada para la programación de las aplicaciones del usuario.

7.4.4.1 Dependiendo del tipo de desarrollo del software, la responsabilidad en lo relativo a la conformidad con los requisitos mencionados en el apartado 7.4.4 puede incumbir solamente al suministrador, sólo al usuario, o a los dos juntos (véase la nota 2 anterior). La repartición de la responsabilidad se debe documentar durante la planificación de la seguridad (véase el capítulo 6).

7.4.4.2 Un conjunto adaptado de herramientas integradas incluyendo los lenguajes, los compiladores, las herramientas de gestión de la configuración y, cuando aplique, las herramientas de ensayo automática se debe seleccionar en función del nivel de integridad de seguridad requerido. La capacidad de las herramientas adaptadas (no necesariamente las utilizadas durante el desarrollo inicial del sistema E/E/PE relacionado con la seguridad) debe tenerse en cuenta.

7.4.4.3 En los límites descritos por el nivel de integridad de seguridad, el lenguaje de programación seleccionado debe:

a) incluir un traductor/compilador que, o bien sea cubierto por un certificado de validación de acuerdo con una norma nacional o internacional reconocida, o bien sea evaluado para establecer su aptitud a la utilización prevista;

b) estar totalmente definido de forma no ambigua, o limitado a las características definidas de forma no ambigua;

c) corresponder a las características de aplicación;

d) contener las características que faciliten la detección de los errores de programación;

e) soportar las características adaptadas al método de diseño.

7.4.4.4 Si no es posible satisfacer los requisitos mencionados en el apartado 7.4.4.3, la justificación de todo lenguaje alternativo utilizado se debe documentar durante la descripción del diseño de la arquitectura del software (véase el apartado 7.4.3). La justificación debe detallar la aptitud del lenguaje a cumplir el objetivo previsto y todas las medidas suplementarias para resolver los inconvenientes identificados del lenguaje.

7.4.4.5 Las reglas de codificación deben estar:

a) revisadas por el evaluador para verificar que son adecuadas;

b) utilizadas para el desarrollo de todos los software relacionados con la seguridad.

7.4.4.6 Las reglas de codificación deben especificar una buena práctica de la programación, prohibir las características del lenguaje poco seguras (por ejemplo, las características del lenguaje no definidas, los diseños no estructurados, etc.) y especificar los procedimientos para documentar el código fuente. Conviene que esta documentación contenga al menos las informaciones siguientes:

a) la entidad legal (ejemplo: la sociedad, el o los autores, etc.);

b) la descripción;

c) las entradas y las salidas;

d) el histórico de la gestión de la configuración.

7.4.5 Requisitos relativos al diseño detallado y al desarrollo

NOTA 1 – Véanse también las tablas A.4, B.1, B.7 y B.9.

NOTA 2 – El diseño detallado se define aquí como el diseño del sistema del software (partición de los principales componentes de la arquitectura en un sistema de módulos del software), el diseño de los módulos del software individuales y la codificación. En las pequeñas aplicaciones, el diseño del sistema del software y de la arquitectura se pueden combinar.

NOTA 3 – La naturaleza del diseño detallado y del desarrollo variará según el desarrollo de las actividades de desarrollo del software y la arquitectura del software (véase el apartado 7.4.3). Para la programación de las aplicaciones del usuario con la ayuda de un lenguaje de variabilidad limitada, como por ejemplo, lenguaje de "lógica en cascada" y bloques funcionales, el diseño detallado se puede considerar como de la configuración más que de la programación. Sin embargo, también es de buena práctica concebir el software de forma estructurada, incluyendo la organización del software en una estructura modular separando (en la medida de lo posible) las partes relacionadas con la seguridad; una verificación de los límites y de otras características alcanzando una protección contra los errores de entrada dados; la utilización de módulos ya verificados y la realización de un diseño facilitan las modificaciones ulteriores del software.

7.4.5.1 Dependiendo del tipo de desarrollo del software, la responsabilidad en lo relativo a la conformidad con los requisitos mencionados en el apartado 7.4.5 puede incumbir solamente al suministrador, sólo al usuario, o a los dos juntos (véase la nota 3 anterior). La repartición de la responsabilidad se debe documentar durante la planificación de la seguridad (véase el capítulo 6).

7.4.5.2 Conviene que las informaciones siguientes estén disponibles antes del comienzo del proceso de diseño detallado: la especificación de los requisitos de seguridad del software (véase el apartado 7.2); la descripción del diseño de la arquitectura del software (véase el apartado 7.4.3); el plan para validar la seguridad del software (véase el apartado 7.3).

7.4.5.3 Conviene que el software sea producido para obtener la modularidad, la ensayabilidad y la capacidad de modificación segura.

7.4.5.4 Para cada componente/subsistema principal identificado en la descripción del diseño de la arquitectura del software (véase el apartado 7.4.3), un refinamiento adicional del diseño se debe basar sobre la partición de módulos del software (es decir, la especificación del diseño del sistema del software). De debe especificar el diseño de cada módulo del software y de los ensayos a aplicar a cada módulo.

NOTA – Para los módulos del software o componentes del software normalizados o anteriormente desarrollados, no es necesaria ninguna especificación de diseño o de ensayo si se puede demostrar que estos elementos satisfacen los requisitos mencionados en el apartado 7.4.2.11.

7.4.5.5 Conviene que los ensayos de integración del sistema del software apropiado se especifiquen para asegurar que el sistema del software satisface los requisitos de seguridad del software especificados, correspondientes al nivel de integridad de seguridad requerido (véase el apartado 7.2).

7.4.6 Requisitos relativos a la codificación

NOTA 1 – Véanse también las tablas A.4, B.1, B.7 y B.9.

7.4.6.1 El código fuente debe:

a) ser legible, comprensible y ensayable;

b) satisfacer los requisitos especificados para el diseño de los módulos del software (véase el apartado 7.4.5);

c) satisfacer los requisitos especificados en las reglas de codificación (véase el apartado 7.4.4);

d) satisfacer a todos los requisitos relevantes identificados durante la planificación de la seguridad (véase el capítulo 6).

7.4.6.2 Conviene que cada módulo de código del software sea revisado.

NOTA – La revisión del código es una actividad de verificación (véase el apartado 7.9).

7.4.7 Requisitos relativos al ensayo de los módulos del software

NOTA 1 – Véanse también las tablas A.5, B.2 y B.6.

NOTA 2 – El hecho de asegurar que un módulo del software satisface la especificación de ensayo correspondiente constituye una actividad de verificación (véase el apartado 7.9). Es la combinación de la revisión del código y del ensayo del módulo del software que asegura que un módulo del software satisface la especificación correspondiente, es decir, que es verificado.

7.4.7.1 Cada módulo del software debe ensayarse como se especifica durante el diseño del software (véase el apartado 7.4.5).

7.4.7.2 Estas ensayos deben mostrar que cada módulo del software realiza la función prevista y no realiza ninguna función no prevista.

NOTA 1 – Esto no implica el ensayo de todas las combinaciones de las entradas, ni tampoco todas las combinaciones de salidas. Permite hacer los ensayos de todas las clases de equivalencias (véase el apartado C.5.7 de la Norma CEI 61508-7) o de los ensayos basadas en la estructura (véase el apartado C.5.8 de la Norma 61508-7). El análisis de los valores límites (véase el apartado C.5.4 de la Norma CEI 61508-7), el análisis de los flujos de control (véase el apartado C.5.9 de la Norma CEI 61508-7) o el análisis del circuito de fuga (véase el apartado C.5.11 de la Norma 61508-7) reducen los casos de ensayo a un número aceptable. Los programas analizables (véase el apartado C.2.7 de la Norma CEI 61508-7) hacen que el cumplimiento de los requisitos sea más fácil.

NOTA 2 – La extensión de los ensayos se puede red ucir en el caso del desarrollo con la ayuda de los métodos formales (véase el apartado C.2.4 de la Norma CEI 61508-7), de las previsiones formales (véase el apartado C.5.13 de la Norma CEI 61508-7) o de las reafirmaciones (véase el apartado C.3.3 de la Norma CEI 61508-7).

NOTA 3 – Se permite utilizar las técnicas estadísticas (véase el anexo D de la Norma CEI 61508-7).

7.4.7.3 Los resultados del ensayo de los módulos del software se deben documentar.

7.4.7.4 Se deben especificar los procedimientos para las acciones correctivas en caso de fallo de un ensayo.

7.4.8 Requisitos relativos a la integración del software

NOTA 1 – Véanse también las tablas A.5, B.2, B.3 y B.6.

NOTA 2 – Probar que el software está correctamente integrado constituye una actividad de verificación (véase el apartado 7.9).

7.4.8.1 Las ensayos de integración del software se deben especificar durante la fase de diseño y desarrollo.

7.4.8.2 La especificación del ensayo de integración del software debe incluir:

a) la repartición del software en conjuntos de integración manejables;

b) los casos del ensayo y los datos del ensayo;

c) los tipos de ensayo a realizar;

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

e) los criterios de ensayo sobre los que se juzgará el ensayo;

f) los procedimientos de las acciones correctivas en el caso de fallo de un ensayo.

7.4.8.3 El software se debe probar de acuerdo con la especificación del ensayo de integración del software. Estos ensayos deben mostrar que todos los módulos del software y los componentes/subsistemas del software se integran correctamente de manera que realiza su función prevista y no realiza ninguna función no prevista.

NOTA 1 – Esto no implica el ensayo de todas las combinaciones de las entradas, ni tampoco todas las combinaciones de salidas. Permite hacer los ensayos de todas las clases de equivalencias (véase el apartado C.5.7 de la Norma CEI 61508-7) o de los ensayos basados en la estructura (véase el apartado C.5.8 de la Norma 61508-7). El análisis de los valores límites (véase el apartado C.5.4 de la Norma CEI 61508-7), el análisis de los flujos de control (véase el apartado C.5.9 de la Norma CEI 61508-7) o el análisis del circuito de fuga (véase el apartado C.5.11 de la Norma CEI 61508-7) reducen los casos de ensayo a un número aceptable. Los programas analizables (véase el apartado C.2.7 de la Norma CEI 61508-7) hacen que el cumplimiento de los requisitos sea más fácil.

NOTA 2 – La extensión de los ensayos se puede reducir en el caso del de sarrollo con la ayuda de los métodos formales (véase el apartado C.2.4 de la Norma CEI 61508-7), de las previsiones formales (véase el apartado C.5.13 de la Norma CEI 61508-7) o de las reafirmaciones (véase el apartado C.3.3 de la Norma CEI 61508-7).

NOTA 3 – Se permite utilizar las técnicas estadísticas (véase el anexo D de la Norma CEI 61508-7).

7.4.8.4 Los resultados del ensayo de integración del software se deben documentar estableciendo los resultados del ensayo y si los objetivos y los criterios de ensayo se han alcanzado. En caso de fallo, las causas del fallo se deben documentar.

7.4.8.5 Durante la integración del software, cualquier modificación o cambio en el software debe ser sujeto a un análisis de impacto que debe determinar todos los módulos tocados y las actividades necesarias rediseño y reverificación.

7.5 Integración de la electrónica programable (hardware y software)

NOTA 1 – Véanse también las tablas A.6, B.3 y B.6.

NOTA 2 – Esta fase corresponde a la etapa 9.4 de la figura 3.

7.5.1 Objetivos

7.5.1.1 El primer objetivo de los requisitos de este apartado es integrar el software al del hardware de la electrónica programable objetivo.

7.5.1.2 El segundo objetivo de los requisitos de este apartado es combinar el software y el del hardware de la electrónica programable relacionada con la seguridad para asegurar su compatibilidad y su conformidad con los requisitos del nivel de integridad de seguridad previsto.

NOTA 1 – Ensayar que el software está correctamente integrado al hardware de la electrónica programable que constituye una actividad de verificación (véase el apartado 7.9).

NOTA 2 – Según la naturaleza de la aplicación, estas actividades se pueden combinar con las mencionadas en el apartado 7.4.8.

7.5.2 Requisitos

7.5.2.1 Los ensayos de integración se deben especificar durante la fase de diseño y desarrollo con el fin de asegurar la compatibilidad del hardware y el del software de la electrónica programable relacionada con la seguridad.

NOTA – Se puede requerir de una estrecha cooperación con el programador del E/E/PES para el desarrollo de los ensayos de integración.

7.5.2.2 Los ensayos de integración de la electrónica programable (hardware y software) se deben especificar de forma que trate los siguientes puntos:

a) la división del sistema en niveles de integración;

b) los casos del ensayo y los datos del ensayo;

c) los tipos de ensayo a realizar;

d) la descripción del entorno del ensayo incluyendo las herramientas, el software y la configuración;

e) los criterios de ensayo sobre los que se juzgará el ensayo.

7.5.2.3 Los ensayos de integración especificadas para la electrónica programable(hardware y software) deben hacer distinción entre las actividades que el programador es capaz de realizar sobre su propio sitio y las actividades en las que se necesita acceder desde el sitio del usuario.

7.5.2.4 Las ensayos de integración especificados para la electrónica programable (hardware y software) deben hacer distinción entre las actividades siguientes:

a) la integración del sistema del software al sistema del hardware electrónica programable objetivo;

b) la integración de E/E/PE, es decir, la incorporación de las interfaces tales como de los sensores y de los accionadores;

c) la integración total del EUC y del sistema E/E/PE relacionado con la seguridad.

NOTA – Los puntos b)y c) se tratan en la Norma CEI 61508-1 y en la Norma CEI 61508-2 y se citan aquí con el fin de localizar el elemento (a) en su contexto y lograr la integridad de las informaciones.

7.5.2.5 El software se debe integrar al hardware de la electrónica programable relacionada con la seguridad de acuerdo con los ensayos de integración especificados de la electrónica programable (hardware y software).

7.5.2.6 Durante el ensayo de integración de la electrónica programable relacionada con la seguridad (hardware y software), toda modificación o cambio realizado al sistema integrado se debe someter a un análisis de impacto que debe determinar todos los módulos del software afectados y las actividades de reverificación necesarias.

7.5.2.7 Los casos de ensayo y sus resultados deben documentarse para análisis posteriores.

7.5.2.8 El ensayo de integración de la electrónica programable relacionado con la seguridad (hardware y software) debe documentarse, incluyendo los resultados del ensayo y si los objetivos y criterios del criterio de ensayo han sido cumplidos. Si existe un fallo, las razones del fallo deben documentarse. Cualquier modificación resultante o cambio del software debe estar sujeto a un análisis de impacto que debe determinar todos los componentes/módulos del software afectados, y las actividades necesarias de reverificación y rediseño.

7.6 Procedimientos de explotación y de modificación del software

NOTA 1 – Véase también la tabla A.8.

NOTA 2 – Esta fase corresponde a la etapa 9.5 de la figura 3.

7.6.1 Objetivo. El objetivo de los requisitos de este apartado es proporcionar las informaciones y los procedimientos relativos al software necesario para verificar que la seguridad funcional del sistema E/E/PE relacionado con la seguridad se mantiene durante la explotación y las modificaciones.

7.6.2 Requisitos. Los requisitos se dan en el apartado 7.6 de la Norma CEI 61508-2 y el apartado 7.8 de esta norma.

NOTA – En esta norma, el software (a diferencia del hardware) no se puede mantener: es siempre modificado.

7.7 Validación de la seguridad del software

NOTA 1 – Véanse también las tablas A.7, B.3 y B.5.

NOTA 2 – Esta fase corresponde a la etapa 9.6 de la figura 3.

7.7.1 Objetivos. El objetivo de los requisitos de este párrafo es asegurar que el sistema integrado está de acuerdo con los requisitos especificados para la seguridad del software (véase el apartado 7.2) al nivel de integridad de seguridad esperado.

7.7.2 Requisitos

7.7.2.1 Si la conformidad a los requisitos para la seguridad del software ya se ha establecido con parte del sistema E/E/PE relacionado con la seguridad (véase el apartado 7.7 de la Norma CEI 61508-2), no es necesario repetir la validación.

7.7.2.2 Las actividades de validación se deben realizar como se especifica en la planificación de la validación de la seguridad del software (véase el apartado 7.3).

7.7.2.3 Los resultados de la validación de la seguridad del software se deben documentar.

7.7.2.4 Para cada función de seguridad, la validación de la seguridad del software debe documentar los siguientes resultados:

a) un registro cronológico de las actividades de validación;

b) la versión del plan de validación de la seguridad del software utilizado (véase el apartado 7.3);

c) la función de seguridad sometida a la validación (por ensayo o análisis), con la referencia al plan de validación de la seguridad del software (véase el apartado 7.3);

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

e) los resultados de la actividad de validación;

f) las diferencias entre los resultados previstos y los resultados obtenidos.

7.7.2.5 Si los resultados obtenidos no corresponden a los resultados previstos, el análisis realizado así como las decisiones de continuar la validación, o de dictar una petición de modificación y de volver a una fase anterior del ciclo de vida del desarrollo se deben documentar con los resultados de la validación de seguridad del software.

NOTA – Los requisitos mencionados en los apartados 7.7.2.2 y 7.7.2.5 se basan en los requisitos generales mencionados en el apartado 7.14 de la Norma CEI 61508-1.

7.7.2.6 La validación de un software relacionado con la seguridad debe satisfacer los siguientes requisitos:

a) el ensayo debe ser el método principal de validación para el software; las actividades de validación se pueden completar con las operaciones de animación y modelización;

b) el software se debe ejecutar simulando

- las señales de entrada presentes en la explotación normal;
- los sucesos previstos;
- las condiciones no deseadas requiriendo una acción del sistema.

c) el suministrador y/o el programador deben facilitar al programador del sistema la accesibilidad a los resultados documentados de la validación de la seguridad del software así como toda documentación útil con el fin de permitir que cumpla los requisitos de las Normas CEI 61508-1 y CEI 61508-2.

7.7.2.7 Los requisitos relativos a la cualificación de las herramientas del software son los siguientes:

a) todos los equipos utilizados para la validación deben estar cualificados de acuerdo con una especificación en relación con una norma internacional o nacional (si estas normas están disponibles) o a un procedimiento debidamente reconocido;

b) los equipos utilizados para la validación del software deben estar cualificados de forma apropiada y debe mostrar que todas las herramientas utilizadas, hardware o software, están adaptadas a su función.

NOTA – En esta norma, la cualificación es la actividad que muestra si una especificación particular se cumple, mejor que los procedimientos de ensayo de conformidad generales que se aplicarían a una especificación cualquiera.

7.7.2.8 Los requisitos relativos a los resultados de validación del software son los siguientes:

a) los ensayos deben mostrar que todos los requisitos especificados para la seguridad del software (véase el apartado 7.2) se cumplen y que el sistema del software no realiza ninguna función no prevista;

b) los casos de ensayo y los resultados se deben documentar para un análisis ulterior y una evaluación independiente, como se requiere por el nivel de integridad de seguridad (véase el apartado 8.2.12 de la Norma CEI 61508-1);

c) los resultados documentados de la validación de la seguridad del software establecen o bien la validación efectiva del software o bien las razones de la no-validación.

7.8 Modificación del software

NOTA 1 – Véase también la tabla A.8.

NOTA 2 – Esta fase corresponde a la etapa 9.5 de la figura 3.

7.8.1 Objetivo. El objetivo de los requisitos de esta norma es aportar las correcciones, las mejoras y adaptaciones al software validado asegurando mantener el nivel de integridad de seguridad requerido.

NOTA – En esta norma, el software (a diferencia del hardware) no se puede mantener. Es continuamente modificado.

7.8.2 Requisitos

7.8.2.1 Antes de realizar cualquier modificación, se debe asegurar que los procedimientos de modificación del software están disponibles (véase el apartado 7.16 de la Norma CEI 61508-1).

NOTA 1 – Los apartados del 7.8.2.1 al 7.8.2.9 se aplican principalmente a los cambios que ocurren durante la fase de explotación del software. También se puede aplicar durante las fases de integración de la electrónica programable y de instalación global y puesta en marcha (véase el apartado 7.13 de la Norma CEI 61508-1).

NOTA 2 – La figura 9 de la Norma CEI 61508-1 muestra un ejemplo de un modelo de procedimiento de modificación.

7.8.2.2 Una modificación no se debe realizar hasta que la petición de modificación del software sea aprobada de acuerdo con los procedimientos especificados durante la planificación de la seguridad (véase el capítulo 6), que describe en detalle:

a) los peligros que pueden afectar;

b) la modificación propuesta;

c) las razones de la modificación.

NOTA – La petición de modificación puede, por ejemplo, motivarse por:

- una seguridad funcional inferior a la especificada;
- un fallo sistemático descubierta por experimentación;
- una legislación de seguridad nueva o modificada;
- unas modificaciones realizadas al equipo sometido a control o a su utilización;
- una modificación de los requisitos globales de seguridad;
- un análisis de los rendimientos de explotación y de mantenimiento, indicando que los rendimientos son inferiores a los previstos;
- las auditorías de seguridad funcional sistemática.

7.8.2.3 Se debe realizar un análisis sobre el impacto de la modificación del software propuesta sobre la seguridad funcional del sistema E/E/PE relacionado con la seguridad.

a) para determinar si es necesario o no un análisis de peligro o riesgo;

b) para determinar que fases del ciclo de vida de la seguridad del software necesitaras repetirse.

7.8.2.4 Los resultados del análisis de impacto obtenidos en el apartado 7.8.2.3 se deben documentar.

7.8.2.5 Todas las modificaciones que tengan un impacto sobre la seguridad funcional del sistema E/E/PE relacionado con la seguridad deberían volver a una fase adecuada del ciclo de vida de la seguridad del software. Todas las fases ulteriores se deben ejecutar de acuerdo con los procedimientos especificados por las fases específicas de acuerdo con los requisitos de esta norma. Conviene que la planificación de la seguridad (véase el capítulo 6) detalle todas las actividades ulteriores.

NOTA – Puede ser necesario realizar un análisis completo de peligro y de riesgo, que implicar la necesidad de modificar los niveles de integridad de seguridad en relación con los especificados por los sistemas relacionados con la seguridad y los dispositivos externos de reducción del riesgo.

7.8.2.6 La planificación de la seguridad para la modificación de un software relacionado con la seguridad debe contener las siguientes informaciones:

a) identificación del personal y especificación de sus competencias requeridas;

b) especificación detallada de la modificación;

c) planificación de la verificación;

d) dominio de revalidación y ensayo de la modificación en los límites requeridos por el nivel de integridad de seguridad.

7.8.2.7 La modificación se debe realizar según la planificación.

7.8.2.8 Los detalles de toda modificación se deben documentar haciendo referencia a:

a) la petición de modificación/puesta a punto;

b) los resultados del análisis de impacto evaluando el impacto de la modificación del software propuesta sobre la seguridad funcional así como las decisiones tomadas acompañadas de sus justificaciones;

c) el histórico de la gestión de la configuración del software;

d) las desviaciones en relación con los modos de explotación y las condiciones normales;

e) todas las informaciones documentadas afectadas por la actividad de la modificación.

7.8.2.9 Las informaciones (por ejemplo, un registro) relativas al detalle de todas las modificaciones se deben documentar. la documentación debe contener la reverificación y la revalidación de los datos así como de los resultados.

NOTA – Los apartados del 7.8.2.1 al 7.8.2.9 se aplican principalmente a los cambios realizados durante las fases de explotación del software. Se puede aplicar durante la integración de la electrónica programable y de la integración global y puesta en servicio (véase el apartado 7.13 de la Norma CEI 61508-1).

7.8.2.10 La evaluación de la actividad de modificación o renovación requerida debe depender de los resultados del análisis de impacto y del nivel de integridad de seguridad del software.

7.9 Verificación del software

NOTA – Véanse también las tablas A.9, B.2 y B.8.

7.9.1 Objetivos. El objetivo de los requisitos de este apartado es, en los límites requeridos por el nivel de integridad de seguridad, verificar y evaluar las salidas de una fase dada del ciclo de vida de la seguridad del software para asegurar la conformidad y la coherencia en relación a las salidas y a las normas dadas en la entrada de esta fase.

NOTA 1 – Este apartado tiene en cuenta los aspectos generales de la verificación que son comunes a varias fases del ciclo de vida de la seguridad. No implica ningún requisito adicional para los elementos de ensayo de las verificaciones realizadas en los apartados 7.4.7 (ensayo de los módulos del software), 7.4.8 (integración del software) y 7.5 (integración de la electrónica programable) y ellos mismos constituyen las actividades de verificación. Además, no se requiere ninguna verificación en este apartado más que la validación del software (véase el apartado 7.7) que, en esta norma, es el proceso que consiste en demostrar la conformidad de la especificación de los requisitos de seguridad (verificación uno tras otro). El control de la especificación de los requisitos de seguridad propiamente dichos se realiza por los expertos en el dominio.

NOTA 2 – Según la arquitectura del software, la responsabilidad de la actividad de verificación se puede repartir entre todas las organizaciones implicadas en el desarrollo y la modificación del software.

7.9.2 Requisitos

7.9.2.1 La verificación del software se debe planificar (véase el apartado 7.4) paralelamente al desarrollo, para cada fase del ciclo de vida de la seguridad del software. Estas informaciones se deben documentar.

7.9.2.2 La planificación de la verificación del software debe hacer referencia a los criterios, técnicas y herramientas utilizadas en el transcurso de las actividades de verificación y debe incluir:

a) la evaluación de los requisitos de integridad de seguridad;

b) la selección y la documentación de las estrategias, actividades y técnicas de verificación;

c) la selección y utilización de las herramientas de verificación (banco de ensayos, ensayo especial del software, simuladores de entradas/salidas, etc.);

d) la evaluación de los resultados de la verificación;

e) las acciones correctivas a ser tomadas.

7.9.2.3 La verificación del software se debe realizar según la planificación.

NOTA – La selección de las técnicas, las medidas de verificación y el grado de independencia de las actividades de verificación dependen de un gran número de factores y se pueden especificar en las normas específicas del sector de aplicación. Estos factores podrían, por ejemplo, incluir:

- el tamaño del proyecto,
- el grado de complejidad,
- el grado de innovación del diseño,
- el grado de innovación tecnológico.

7.9.2.4 Los ensayos se deben documentar para mostrar que la fase que es verificada se ha completado satisfactoriamente en todos los aspectos.

7.9.2.5 Después de cada verificación, conviene que la documentación de verificación incluya:

a) la identificación de los elementos a verificar;

b) la verificación de las informaciones en relación a las informaciones de la verificación que ha sido realizada;

c) las no-conformidades.

NOTA – Los ejemplos de no-conformidad incluyen los módulos del software, las estructuras de datos y los algoritmos poco adaptados al problema.

7.9.2.6 Todas las informaciones esenciales de la fase N del ciclo de vida de la seguridad del software necesarias para la ejecución correcta de la fase siguiente N+1 deben estar disponibles y conviene verificarlas. Las salidas de la fase N incluyen:

a) la adecuación de la especificación, de la descripción del diseño o del código de la fase N en lo que concierne a:
   - la funcionalidad;
   - la integridad de seguridad, los rendimientos y otros requisitos de la planificación de la seguridad (véase el capítulo 6);
   - la legibilidad del equipo de desarrollo;
   - la ensayabilidad para la verificación ulterior;
   - la modificación segura permitiendo una evolución ulterior;

b) la adecuación de la planificación de la validación y/o los ensayos especificados para la fase N para especificar y describir el diseño de la fase N;

c) el control de las incompatibilidades entre:
   - los ensayos especificados durante la fase N y los ensayos especificados en la fase precedente N-1;
   - las salidas de la fase N.

7.9.2.7 Bajo los requisitos mencionados en el apartado 7.1.2.1, las actividades de verificación siguiente se deben realizar:

a) verificación de los requisitos de seguridad del software (véase el apartado 7.9.2.8);

b) verificación de la arquitectura del software (véase el apartado 7.9.2.9);

c) verificación del diseño del sistema del software (véase el apartado 7.9.2.10);

d) verificación del diseño de los módulos del software (véase el apartado 7.9.2.11);

e) verificación del código (véase el apartado 7.9.2.12);

f) verificación de los datos (véase el apartado 7.9.2.13);

g) ensayo de los módulos del software (véase el apartado 7.4.7);

h) ensayo de integración del software (véase el apartado 7.4.8);

i) ensayo de integración de la electrónica programable (véase el apartado 7.5);

j) ensayo de los requisitos de seguridad del software (validación del software) (véase el apartado 7.7).

7.9.2.8 Verificación de los requisitos de seguridad del software: una vez que los requisitos de seguridad del software se han especificado (véase el apartado 7.2), y antes de lanzar la fase siguiente de diseño y desarrollo del software, la verificación debe:

a) tener en cuenta el hecho que los requisitos especificados de seguridad del software (véase el apartado 7.2) cumplen de forma adecuada los requisitos de seguridad de los E/E/PES especificados (véase la Norma CEI 61508-2) en lo que concierne a la funcionalidad, la integridad de seguridad, los rendimientos y los otros requisitos de la planificación de la seguridad;

b) tener en cuenta el hecho que la planificación de la validación de la seguridad del software (véase el apartado 7.3) satisface de forma adecuada los requisitos de seguridad del software especificados (véase el apartado 7.2);

c) controlar las incompatibilidades entre:

   – los requisitos de seguridad del software especificados (véase el apartado 7.2) y los requisitos de seguridad del sistema E/E/PES especificados (véase la Norma CEI 61508-2);

   – los requisitos de seguridad del software especificados (véase el apartado 7.2) y la planificación de la validación de seguridad del software (véase el apartado 7.3).

7.9.2.9 Verificación de la arquitectura del software: después que se ha establecido el diseño de la arquitectura del software, la verificación debe:

a) tener en cuenta el hecho que la descripción del diseño de la arquitectura del software (véase el apartado 7.4.3) satisface de forma adecuada los requisitos de seguridad del software especificado (véase el apartado 7.2);

b) tener en cuenta el hecho que los ensayos de integración de la arquitectura del software especificado (véase el apartado 7.4.3)se adaptan al diseño de la arquitectura del software (véase el apartado 7.4.3);

c) Tener en cuenta el hecho que los atributos de cada componente/subsistema principal son apropiados en referencia a:

   – viabilidad de los rendimientos de seguridad requeridos;

   – ensayabilidad para la verificación ulterior;

   – legibilidad por el equipo de desarrollo y de verificación;

   – modificación segura permitiendo una evolución ulterior.

d) controlar las incompatibilidades entre:

   – la descripción del diseño de la arquitectura del software (véase el apartado 7.4.3) y los requisitos de seguridad del software específico (véase el apartado 7.2);

– la descripción del diseño de la arquitectura del software (véase el apartado 7.4.3) y los ensayos de integración de la arquitectura del software específicas (véase el apartado 7.4.3);

– los ensayos de integración de la arquitectura del software específico (véase el apartado 7.4.3) y la planificación de la validación de seguridad del software (véase el apartado 7.3).

7.9.2.10 Verificación del diseño del sistema del software: después que el diseño del sistema del software se haya especificado, la verificación debe:

a) tener en cuenta el hecho que el diseño específico del sistema del software (véase el apartado 7.4.5) satisface de forma adecuada el diseño de la arquitectura del software (véase el apartado 7.4.3);

b) tener en cuenta el hecho que los ensayos específicos de la integración del sistema del software (véase el apartado 7.4.5) satisface de forma adecuada el diseño específico del sistema del software (véase el apartado 7.4.5);

c) tener en cuenta el hecho que los atributos de cada componente principal del diseño específico del sistema del software (véase el apartado 7.4.5) son apropiados en lo referente a:

– viabilidad de los rendimientos de seguridad requeridos;

– ensayabilidad para la verificación ulterior;

– legibilidad por el equipo de desarrollo y de verificación;

– modificación segura permitiendo una evolución ulterior.

NOTA – Las ensayos de integración del sistema del software se pueden especificar como parte de los ensayos de la arquitectura del software.

d) controlar las incompatibilidades entre:

– el diseño específico del sistema del software (véase el apartado 7.4.5) y la descripción del diseño de la arquitectura del software (véase el apartado 7.4.3);

– la descripción del diseño del sistema del software (véase el apartado 7.4.5) y los ensayos específicas de integración del sistema del software (véase el apartado 7.4.5);

– los ensayos específicos de la integración del sistema del software (véase el apartado 7.4.5) y los ensayos específicos de la integración de la arquitectura (véase el apartado 7.4.3);

7.9.2.11 Verificación del diseño de los módulos del software: después que el diseño de cada módulo del software se haya especificado, la verificación debe:

a) tener en cuenta el hecho que el diseño específico de los módulos del software (véase el apartado 7.4.5) satisface de forma adecuada el diseño específico del sistema del software (véase el apartado 7.4.5);

b) tener en cuenta el hecho que los ensayos específicos para cada módulo del software (véase el apartado 7.4.5) se adaptan al diseño específico de los módulos del software (véase el apartado 7.4.5);

c) tener en cuenta el hecho que los atributos de cada módulo del software son apropiados en lo referente a:

– viabilidad de los rendimientos de seguridad requeridos (véase el apartado 7.2);

– ensayabilidad para la verificación ulterior;

– legibilidad por el equipo de desarrollo y de verificación;

– modificación segura permitiendo una evolución ulterior.

d) verificar las incompatibilidades entre:

- el diseño específico de los módulos del software (véase el apartado 7.4.5) y el diseño específico del sistema del software (véase el apartado 7.4.5);
- (para cada módulo del software) el diseño específico de los módulos del software (véase el apartado 7.4.5) y los ensayos específicas de los módulos del software (véase el apartado 7.4.5);
- los ensayos específicos de los módulos del software (véase el apartado 7.4.5) y los ensayos específicos de la integración del sistema del software (véase el apartado 7.4.5).

7.9.2.12 Verificación del código: El código fuente se debe verificar por los métodos estáticos permitiendo asegurar la conformidad al diseño específico del módulo del software (véase el apartado 7.4.5) con las reglas de codificación requeridas (véase el apartado 7.4.4) y con los requisitos de la planificación de seguridad (véase el apartado 7.3).

NOTA – Durante las primeras fases del ciclo de vida de la seguridad del software, la verificación es estática (por ejemplo, inspección, revisión, ensayo formal, etc.). La verificación del código incluye las técnicas como las inspecciones del software y las lecturas cruzadas. Es la combinación de los resultados de la verificación del código y del ensayo de los módulos del software que permiten asegurar que cada módulo del software satisface la especificación que se le ha asociado. A partir de esto, los ensayos son el principal medio de verificación.

7.9.2.13 Verificación de los datos

a) Las estructuras de datos especificadas durante el diseño se deben verificar en lo referente a:

- estado de cumplimiento total de registros;
- autocoherencia;
- protección contra el deterioro o la alteración;
- coherencia con los requisitos funcionales del sistema orientado a los datos.

b) Los datos de la aplicación se deben verificar en lo referente a:

- coherencia con las estructuras dadas;
- estado de cumplimiento total de registros;
- compatibilidad con el software del sistema de base (por ejemplo: secuencia de ejecución, duración de ejecución, etc.);
- exactitud de los valores de los datos.

NOTA – Un ejemplo de datos de la aplicación es el programa por partes previsto para una máquina bajo control digital. El software del sistema (típicamente un conjunto de subprogramas) actúa como interpretador de los datos de la aplicación. En otros contextos, estos datos de la aplicación se consideraran como un programa de aplicación.

c) Todos los parámetros modificables se deben verificar en lo relativo a la protección contra:

- valores iniciales no válidos o no definidos;
- valores erróneos, incoherentes o idel softwares;
- modificaciones no autorizadas;
- alteración de los datos.

d) Todas las interfaces de instalación y su software asociado (es decir, sensores y accionadores, interfaz fuera de línea: véase el apartado 7.2.2.11) se deben verificar en lo referente a:

- detección de las averías de la interfaz previstas;
- tolerancia de las averías de la interfaz previstas.

e) Todas las interfaces de comunicación y sus software asociados se deben verificar para asegurar que tienen un nivel adecuado de:

- detección de averías;
- protección contra la alteración;
- validación de los datos.

8 EVALUACIÓN DE LA SEGURIDAD FUNCIONAL

8.1 El objetivo y los requisitos del capítulo 8 de la Norma CEI 61508-1 se aplican a la evaluación del software relacionado con la seguridad.

8.2 Excepto indicación contraria en las normas internacionales ligadas a los sectores de aplicación, el nivel mínimo de independencia del personal encargado de la evaluación de la seguridad funcional se debe especificar en el apartado 8.2.12 de la Norma CEI 61508-1.

8.3 Los resultados de las actividades mencionadas en la tabla A.10 se pueden utilizar para la evaluación de la seguridad funcional.

NOTA – Seleccionar las técnicas en los anexos A y B no es suficiente para garantizar que la integridad de seguridad requerida se alcance (véase el apartado 7.1.2.6). Conviene que el evaluador considere también:

- la coherencia y la complementación de los métodos, lenguajes y herramientas elegidas para el conjunto del ciclo de desarrollo;
- si los programadores utilizan métodos, lenguajes y herramientas que se comprenden perfectamente;
- si los métodos, lenguajes y herramientas están bien adaptados a los problemas específicos encontrados durante el desarrollo.

ANEXO A (Normativo)

GUÍA DE SELECCIÓN DE TÉCNICAS Y MEDIDAS

Algunos apartados de esta norma están asociados a una tabla. Por ejemplo, el apartado 7.2. (especificación de los requisitos de seguridad del software) está asociado a la tabla A.1. El anexo B incluye tablas más detalladas que toman algunas entradas de las tablas del anexo A. Por ejemplo, la tabla B.2 toma los términos del ensayo y del análisis dinámico de la tabla A.5.

Véase la Norma CEI 61508-7 para una presentación de las técnicas y medidas referenciadas en el anexo A y B.

Cada técnica o medida mencionada en las tablas tiene una recomendación para los niveles de integridad de seguridad (SIL)[1)] del 1 al 4. Estas recomendaciones se presentan de la forma siguiente:

- HR: La técnica o medida es altamente recomendada para este nivel de integridad de seguridad. Si esta técnica o medida no se utiliza, conviene que la razón de esta no-utilización sea detallada durante la planificación de la seguridad y el acuerdo con el evaluador.

- R: La técnica o medida se recomienda para este nivel de integridad de seguridad. Se trata de una recomendación de nivel más bajo que una recomendación HR.

- ---: La utilización de la técnica o medida ni se recomienda ni se desaconseja.

- NR: La técnica o medida no se recomienda para este nivel de integridad de seguridad. Si esta técnica o medida se utiliza, conviene que la razón de esta utilización sea detallada durante la planificación de la seguridad y el acuerdo con el evaluador.

Las técnicas/medidas apropiadas se deben seleccionar en función del nivel de integridad de seguridad. Las técnicas o medidas equivalentes o alternativas se indican con la ayuda de una letra seguida por el número. Debe satisfacerse una sola de las técnicas/medidas equivalentes o alternativas.

La clasificación de las técnicas y de las medidas se liga al concepto de *eficacia* definido en la Norma CEI 61508-2. Mientras que todos los otros factores son iguales, las técnicas clasificadas HR serán más eficaces que las de la clase R bien sea para impedir la introducción de fallos sistemáticos durante el desarrollo del software, o bien (en el caso de la arquitectura del software) para controlar los fallos residuales del software surgidas durante la ejecución.

Debido al gran número de factores que pueden afectar a la integridad de seguridad del software, no es posible elaborar un algoritmo combinando las técnicas y las medidas que serán corregidas por cualquier aplicación dada. De todos modos, en la Norma CEI 61508-6, se proporciona la guía de utilización de las tablas dando dos ejemplos de trabajo.

Para una aplicación particular, se debe establecer la combinación apropiada de las técnicas o medidas durante la planificación de la seguridad seleccionando las técnicas o medidas apropiadas, excepto si figuran otros requisitos en las notas de la tabla.

La Norma CEI 61508-6 proporciona una primera guía sobre la interpretación de las tablas relativas a la programación de las aplicaciones del usuario.

1) SIL, del inglés: "Safety Integrity Levels".

Tabla A.1
Especificación de los requisitos de seguridad del software (véase el apartado 7.2)

	Técnica/Medida*	Ref.	SIL1	SIL2	SIL3	SIL4
1	Herramientas de especificación asistida por ordenador	B.2.4	R	R	HR	HR
2a	Métodos semiformales	Tabla B.7	R	R	HR	HR
2b	Métodos formales incluyendo, por ejemplo, CCS, CSP, HOL, LOTOS, OBJ, lógica temporal, VDM y Z	C.2.4	---	R	R	HR

NOTA 1 – La especificación de los requisitos de seguridad del software necesitará siempre una descripción del problema en lenguaje natural y el empleo de toda notificación matemática necesaria que representa la aplicación.

NOTA 2 – La tabla indica los requisitos adicionales para especificar los requisitos de integridad de seguridad del software de forma clara y precisa.

* Las técnicas y medidas apropiadas se deben seleccionar en función del nivel de integridad de seguridad. Las técnicas/medidas equivalentes o alternativas se indican con la ayuda de una letra seguida por el número. Se debe cumplir una sola de las técnicas/medidas equivalentes o alternativas.

Tabla A.2
Diseño y desarrollo del software: diseño de la arquitectura del software (véase el apartado 7.4.3)

	Técnica/Medida*	Ref.	SIL1	SIL2	SIL3	SIL4
1	Detección de fallo y diagnóstico	C.3.1	---	R	HR	HR
2	Códigos de detección y corrección de los errores	C.3.2	R	R	R	HR
3a	Programación por reafirmación de averías	C.3.3	R	R	R	HR
3b	Técnicas basándose en dispositivos externos de seguridad	C.3.4	---	R	R	R
3c	Programación diversa	C.3.5	R	R	R	HR
3d	Bloque de recuperación	C.3.6	R	R	R	R
3e	Recuperación hacia atrás	C.3.7	R	R	R	R
3f	Recuperación hacia delante	C.3.8	R	R	R	R
3g	Mecanismos de recuperación del fallo por relanzamiento de ejecución	C.3.9	R	R	R	HR
3h	Casos de memorización ejecutada	C.3.10	---	R	R	HR
4	Degradación “elegante”	C.3.11	R	R	HR	HR
5	Inteligencia artificial – corrección de fallo	C.3.12	---	NR	NR	NR
6	Reconfiguración dinámica	C.3.13	---	NR	NR	NR
7a	Métodos estructurados incluyendo por ejemplo, JSD, MASCOT, SADT Y Yourdon	C.2.1	HR	HR	HR	HR
7b	Métodos semiformales	Tabla B.7	R	R	HR	HR
7c	Métodos estructurados incluyendo, por ejemplo, CCS, CSP, HOL, LOTOS, OBJ, lógica temporal, VDM y Z	C.2.4	---	R	R	HR
8	Herramientas de verificación asistida por ordenador	B.2.4	R	R	HR	HR

NOTA – Conviene tener en cuenta las medidas de esta tabla relativas a la tolerancia de los fallos (control de las averías) en relación con los requisitos relativos a la arquitectura y el control de las averías para el software de los equipos electrónicos programables de la Norma CEI 61508-2.

* Las técnicas y medidas apropiadas se deben seleccionar en función del nivel de integridad de seguridad. Las técnicas/medidas equivalentes o alternativas se indican con la ayuda de una letra seguida por el número. Se debe cumplir una sola de las técnicas/medidas equivalentes o alternativas.

Tabla A.3
Diseño y desarrollo del software: herramientas de soporte y lenguaje de programación (véase el apartado 7.4.4)

	Técnica/Medida*	Ref.	SIL1	SIL2	SIL3	SIL4
1	Lenguaje de programación adecuado	C.4.6	HR	HR	HR	HR
2	Lenguaje de programación fuertemente modelizado	C.4.1	HR	HR	HR	HR
3	Subconjunto de lenguaje	C.4.2	---	---	HR	HR
4a	Herramientas certificadas	C.4.3	R	HR	HR	HR
4b	Herramientas en las que la confianza aumenta como resultado de su utilización	C.4.4	HR	HR	HR	HR
5a	Traductor certificado	C.4.3	R	HR	HR	HR
5b	Traductor: la confianza aumenta con su utilización	C.4.4	HR	HR	HR	HR
6	Biblioteca de módulos del software y componentes ensayados/verificados	C.4.5	R	HR	HR	HR

* Las técnicas y medidas apropiadas se deben seleccionar en función del nivel de integridad de seguridad. Las técnicas/medidas equivalentes o alternativas se indican con la ayuda de una letra seguida por el número. Se debe cumplir una sola de las técnicas/medidas equivalentes o alternativas.

Tabla A.4
Diseño y desarrollo del software: diseño detallado (véanse los apartados 7.4.5 y 7.4.6)
(Incluye el diseño del sistema del software, el diseño de los módulos del software y la codificación)

	Técnica/Medida*	Ref.	SIL1	SIL2	SIL3	SIL4
1a	Métodos estructurados incluyendo, por ejemplo, JDS, MASCOT, SADT y Yourdon	C.2.1	HR	HR	HR	HR
1b	Métodos semiformales	Tabla B.7	R	HR	HR	HR
1c	Métodos formales incluyendo, por ejemplo, CCS, CSP, HOL, LOTOS, OBJ, lógica temporal, VDM y Z	C.2.4	---	R	R	HR
2	Herramientas de diseño asistidas por ordenador	B.3.5	R	R	HR	HR
3	Programación defensiva	C.2.5	---	R	HR	HR
4	Aproximación modular	Tabla B.9	HR	HR	HR	HR
5	Reglas de diseño y de codificación	Tabla B.1	R	HR	HR	HR
6	Programación estructurada	C.2.7	HR	HR	HR	HR
7	Utilización de módulos del software y componentes ensayados/verificados (si es posible)	C.2.10 C.4.5	R	HR	HR	HR

* Las técnicas y medidas apropiadas se deben seleccionar en función del nivel de integridad de seguridad. Las técnicas/medidas equivalentes o alternativas se indican con la ayuda de una letra seguida por el número. Se debe cumplir una sola de las técnicas/medidas equivalentes o alternativas.

Tabla A.5
Diseño y desarrollo del software: ensayo e integración de los módulos del software
(véanse los apartados 7.4.7 y 7.4.8)

	Técnica/Medida*	Ref.	SIL1	SIL2	SIL3	SIL4
1	Ensayo probabilístico	C.5.1	---	R	R	HR
2	Análisis dinámico y ensayo	B.6.5 Tabla B.2	R	HR	HR	HR
3	Registro y análisis de los datos	C.5.2	HR	HR	HR	HR
4	Ensayo funcional y caja negra	B.5.1 B.5.2 Tabla B.3	HR	HR	HR	HR
5	Modelización del funcionamiento	C.5.20 Tabla B.6	R	R	HR	HR
6	Ensayo de interfaz	C.5.3	R	R	HR	HR

NOTA 1 – El ensayo de integración de los módulos del software son actividades de verificación (véase la tabla A.9).

NOTA 2 – Las técnicas/medidas apropiadas se deben seleccionar en función del nivel de integridad de seguridad.

* Se debe seleccionar una técnica/medida numerada en función del nivel de integridad de seguridad.

Tabla A.6
Integración de la electrónica programables (hardware y software) (véase el apartado 7.5)

	Técnica/Medida*	Ref.	SIL1	SIL2	SIL3	SIL4
1	Ensayo funcional y caja negra	B.5.1 B.5.2 Tabla B.3	HR	HR	HR	HR
2	Modelización del funcionamiento	C.5.20 Tabla B.6	R	R	HR	HR

NOTA 1 – La integración de la electrónica programable es una actividad de verificación (véase la tabla A.9).

NOTA 2 – Las técnicas/medidas apropiadas se deben seleccionar en función del nivel de integridad de seguridad.

* Se debe seleccionar una técnica/medida numerada en función del nivel de integridad de seguridad.

Tabla A.7
Validación de la seguridad del software (véase el apartado 7.7)

	Técnica/Medida*	Ref.	SIL1	SIL2	SIL3	SIL4
1	Ensayo probabilístico	C.5.1	---	R	R	HR
2	Simulación/Modelización	Tabla B.5	R	R	HR	HR
3	Ensayo funcional y caja negra	B.5.1 B.5.2 Tabla B.3	HR	HR	HR	HR

* Se debe seleccionar una técnica/medida numerada en función del nivel de integridad de seguridad.

NOTA – Las técnicas/medidas apropiadas se deben seleccionar en función del nivel de integridad de seguridad.

Tabla A.8
Modificación del software (véase el apartado 7.8)

	Técnica/Medida*	Ref.	SIL1	SIL2	SIL3	SIL4
1	Análisis de impacto	C.5.23	HR	HR	HR	HR
2	Reverificación de un módulo del software modificado	C.5.23	HR	HR	HR	HR
3	Reverificación de los módulos del software afectados	C.5.23	R	HR	HR	HR
4	Revalidación del sistema completo	C.5.23	---	R	HR	HR
5	Gestión de la configuración del software	C.5.24	HR	HR	HR	HR
6	Registro y análisis de los datos	C.5.2	HR	HR	HR	HR

* Se debe seleccionar una técnica/medida numerada en función del nivel de integridad de seguridad.
Las técnicas/medidas apropiadas se deben seleccionar en función del nivel de integridad de seguridad.

Tabla A.9
Verificación del software (véase el apartado 7.9)

	Técnica/Medida*	Ref.	SIL1	SIL2	SIL3	SIL4
1	Ensayo funcional	C.5.13	---	R	R	HR
2	Ensayo probabilístico	C.5.1	---	R	R	HR
3	Análisis estático	B.6.4 Tabla B.8	R	HR	HR	HR
4	Análisis dinámico y ensayo	B.6.5 Tabla B.2	R	HR	HR	HR
5	Métricas de complejidad del software	C.5.14	R	R	R	R
Ensayo de los módulos del software y de integración		Véase la tabla A.5				
Ensayo de integración de la electrónica programable		Véase la tabla A.6				
Ensayo del sistema del software (validación)		Véase la tabla A.7				

NOTA 1 – Por razones prácticas, todas las actividades de verificación se reúnen en esta tabla. Sin embargo, ésta no implica ningún requisito adicional para los elementos del ensayo dinámico de verificación de la tabla A.5 y de la tabla A.6 que constituyen en sí mismas las actividades de verificación. Además, no se requiere ningún ensayo de verificación en esta tabla, a parte de la validación del software (tabla A.7) que, en esta norma, es la demostración de la conformidad a la especificación de los requisitos de seguridad (verificación uno tras otro).

NOTA 2 – La verificación cubre la Norma CEI 61508-1, la Norma CEI 61508-2 y la Norma CEI 61508-3. La primera verificación del sistema relacionado con la seguridad se realiza en relación a las especificaciones del nivel anterior del sistema.

NOTA 3 – Durante las primeras fases del ciclo de vida de la seguridad del software, la verificación es estática, por ejemplo, inspección, revisión, control formal, etc. Cuando el código es producido, se puede realizar un ensayo dinámico. Se exige para la verificación la combinación de estas dos clases de información. Por ejemplo, la verificación del código de un módulo del software por los medios estáticos incluye las técnicas de inspección del software, las lecturas cruzadas, el análisis estático, el ensayo formal, etc. La verificación del código por los medios dinámicos incluye el ensayo funcional, el ensayo de la caja blanca y el ensayo estático. La combinación de estos dos tipos de ensayos logra asegurar que cada módulo del software satisface su especificación.

* Se debe seleccionar una técnica/medida numerada en función del nivel de integridad de seguridad.
Las técnicas/medidas apropiadas se deben seleccionar en función del nivel de integridad de seguridad.

Tabla A.10
Evaluación de la seguridad funcional (véase el capítulo 8)

	Evaluación/Técnica*	Ref.	SIL1	SIL2	SIL3	SIL4
1	Lista de control	B.2.5	R	R	R	R
2	Tablas de decisión/de verdad	C.6.1	R	R	R	R
3	Métricas de complejidad del software	C.5.14	R	R	R	R
4	Análisis de las averías	Tabla B.4	R	R	HR	HR
5	Análisis de las averías de causa común de un software diversificado (si el software diversificado se utiliza)	C.6.3	---	R	HR	HR
6	Diagrama de bloques de fiabilidad	C.6.5	R	R	R	R
*	Las técnicas y medidas apropiadas se deben seleccionar en función del nivel de integridad de seguridad.					

ANEXO B (Normativo)

TABLAS DETALLADAS

NOTA – Las referencias reenvían a los requisitos detallados de las técnicas/medidas que figuran en la Norma CEI 61508-7.

Tabla B.1
Normas de diseño y codificación
(referenciadas en la tabla A.4)

	Técnica/Medida*	Ref.	SIL1	SIL2	SIL3	SIL4
1	Utilización de las reglas de codificación	C.2.6.2	HR	HR	HR	HR
2	Sin objetos dinámicos	C.2.6.3	R	HR	HR	HR
3a	Sin variables dinámicas	C.2.6.3	---	R	HR	HR
3b	Control en línea durante la creación de las variables dinámicas	C.2.6.4	---	R	HR	HR
4	Utilización limitada de las interrupciones	C.2.6.5	R	R	HR	HR
5	Utilización limitada de los punteros	C.2.6.6	---	R	HR	HR
6	Utilización limitada de recurrencias	C.2.6.7	---	R	HR	HR
7	Sin ampliaciones incondicionales en los programas en lenguajes de alto nivel	C.2.6.2	R	HR	HR	HR
NOTA – La aplicación de las medidas 2 y 3a no son necesarias en caso de utilización de un compilador que asegure que un espacio de memoria suficiente está afectado antes de la ejecución de todos los objetos y variables dinámicas, o que introduzca controles de asignación correcta de memoria en línea en el momento de la ejecución.						
* Las técnicas y medidas apropiadas se deben seleccionar en función del nivel de integridad de seguridad. Las técnicas/medidas equivalentes o alternativas se indican con la ayuda de una letra seguida por el número. Se debe cumplir una sola de las técnicas/medidas equivalentes o alternativas.						

Tabla B.2
Análisis dinámico y ensayos
(referenciados en las tablas A.5 y A.9)

	Técnica/Medida*	Ref.	SIL1	SIL2	SIL3	SIL4
1	Ejecución del caso de ensayo a partir del análisis de los valores en los límites	C.5.4	R	HR	HR	HR
2	Ejecución del caso de ensayo a partir de la estimación de los errores	C.5.5	R	R	R	R
3	Ejecución del caso de ensayo a partir de la implantación de los errores	C.5.6	---	R	R	R
4	Modelización del funcionamiento	C.5.20	R	R	R	HR
5	Clases de equivalencia y ensayo de las particiones de entrada	C.5.7	R	R	R	HR
6	Ensayos basados en la estructura	C.5.8	R	R	HR	HR
NOTA – El análisis de los casos de ensayo se realizan al nivel del subsistema y se basa en la especificación y/o la especificación y el código.						
* Las técnicas y medidas apropiadas se deben seleccionar en función del nivel de integridad de seguridad.						

Tabla B.3
Ensayos funcionales y de caja negra
(referenciados en las tablas A.5, A.6 y A.7)

	Técnica/Medida*	Ref.	SIL1	SIL2	SIL3	SIL4
1	Ejecución del caso de ensayo a partir de diagramas causa/consecuencia	B.6.6.2	---	---	R	R
2	Prototipo/Animación	C.5.17	---	---	R	R
3	Análisis de los valores límites	C.5.4	R	HR	HR	HR
4	Clases de equivalencia y ensayo de las particiones de entrada	C.5.7	R	HR	HR	HR
5	Simulación del proceso	C.5.18	R	R	R	R
NOTA 1 – El análisis de los casos de ensayo se efectúa a nivel del subsistema del software y se basa únicamente en la especificación.						
NOTA 2 – El estado de cumplimiento total de registros de la simulación dependerá del nivel de integridad de seguridad, de la complejidad y de la aplicación.						
* Las técnicas y medidas apropiadas se deben seleccionar en función del nivel de integridad de seguridad.						

Tabla B.4
Análisis de avería
(referenciada en la tabla A.10)

	Técnica/Medida*	Ref.	SIL1	SIL2	SIL3	SIL4
1a	Diagramas causa/consecuencia	B.6.6.2	R	R	R	R
1b	Análisis por árbol de eventos	B.6.6.3	R	R	R	R
2	Análisis por árbol de avería	B.6.6.5	R	R	HR	HR
3	Análisis de los modos de avería, de sus efectos y de su criticidad	B.6.6.4	R	R	HR	HR
4	Simulación de Monte-Carlo	C.6.6	R	R	R	R
NOTA – Conviene realizar un análisis de riesgo preliminar con el fin de clasificar el software en relación al nivel de integridad de seguridad más apropiado.						
* Las técnicas y medidas apropiadas se deben seleccionar en función del nivel de integridad de seguridad. Las técnicas/medidas equivalentes o alternativas se indican con la ayuda de una letra seguida por el número. Se debe cumplir una sola de las técnicas/medidas equivalentes o alternativas.						

Tabla B.5
Modelización
(referenciada en la tabla A.7)

	Técnica/Medida*	Ref.	SIL1	SIL2	SIL3	SIL4
1	Diagrama de flujo de datos	C.2.2	R	R	R	R
2	Autómatas de estados finitos	B.2.3.2	---	R	HR	HR
3	Métodos formales	C.2.4	---	R	R	HR
4	Modelización del funcionamiento	C.5.20	R	HR	HR	HR
5	Redes de Petri temporales	B.2.3.3	---	R	HR	HR
6	Prototipo/Animación	C.5.17	R	R	R	R
7	Diagramas de estructuras	C.2.3	R	R	R	HR
NOTA – Si una técnica específica no se menciona en la tabla, no se debe considerar como excluida. Conviene asegurarse su conformidad con esta norma.						
* Las técnicas y medidas apropiadas se deben seleccionar en función del nivel de integridad de seguridad.						

Tabla B.6
Ensayo de prestaciones
(referenciado en las tablas A.5 y A.6)

	Técnica/Medida*	Ref.	SIL1	SIL2	SIL3	SIL4
1	Ensayo de avalancha/estrés	C.5.21	R	R	HR	HR
2	Tiempo de respuesta y limitaciones de memoria	C.5.22	HR	HR	HR	HR
3	Requisitos de prestaciones	C.5.19	HR	HR	HR	HR
*	Las técnicas y medidas apropiadas se deben seleccionar en función del nivel de integridad de seguridad.					

Tabla B.7
Métodos semiformales
(referenciados en las tablas A.1, A.2 y A.4)

	Técnica/Medida*	Ref.	SIL1	SIL2	SIL3	SIL4
1	Diagramas de bloques lógicos/funcionales	Véase la nota	R	R	HR	HR
2	Diagramas de secuencia	Véase la nota	R	R	HR	HR
3	Diagramas de flujo de datos	C.2.2	R	R	R	R
4	Autómatas de estados finitos/diagramas de cambios de estado	B.2.3.2	R	R	HR	HR
5	Redes de Petri temporales	B.2.3.3	R	R	HR	HR
6	Tablas de decisión/de verdad	C.6.1	R	R	HR	HR
NOTA – Los diagramas de bloques del softwares/funcionales y los diagramas de secuencia se describen en la Norma CEI 61131-3.						
*	Las técnicas y medidas apropiadas se deben seleccionar en función del nivel de integridad de seguridad.					

Tabla B.8
Análisis estático
(referenciado en la tabla A.9)

	Técnica/Medida*	Ref.	SIL1	SIL2	SIL3	SIL4
1	Análisis de valores límites	C.5.4	R	R	HR	HR
2	Lista de control	B.2.5	R	R	R	R
3	Análisis de flujo de control	C.5.9	R	HR	HR	HR
4	Análisis de flujo de datos	C.5.10	R	HR	HR	HR
5	Estimación de errores	C.5.5	R	R	R	R
6	Inspección de acuerdo con Fagan	C.5.15	---	R	R	HR
7	Análisis del circuito de fuga	C.5.11	---	---	R	R
8	Ejecución simbólica	C.5.12	R	R	HR	HR
9	Lecturas cruzadas/revisión de diseño	C.5.16	HR	HR	HR	HR
*	Las técnicas y medidas apropiadas se deben seleccionar en función del nivel de integridad de seguridad.					

Tabla B.9
Aproximación modular
(referenciada en la tabla A.4)

	Técnica/Medida*	Ref.	SIL1	SIL2	SIL3	SIL4
1	Limitación del tamaño de los módulos del software	C.2.9	HR	HR	HR	HR
2	Ocultación/encapsulación de la información	C.2.8	R	HR	HR	HR
3	Limitación del número de parámetros	C.2.9	R	R	R	R
4	Un punto de entrada/un punto de salida en las subrutinas y las funciones	C.2.9	HR	HR	HR	HR
5	Interfaz totalmente definida	C.2.9	HR	HR	HR	HR
NOTA – Para obtener información sobre las técnicas, a excepción de la técnica de ocultación/encapsulación de la información, véase el apartado C.2.9 de la Norma CEI 61508-7.						
* Ninguna de estas técnicas es suficiente por sí misma. Se deben tener en consideración todas las técnicas apropiadas.						

ANEXO C (Informativo)

BIBLIOGRAFÍA

CEI 61151:1992 – *Instrumentación nuclear. Amplificadores y preamplificadores utilizados con los detectores de radiaciones ionizantes. Métodos de ensayo. (Nuclear instrumentation. Amplifiers and preamplifiers used with detectors of ionizing radiation. Test procedures).*

ISO/CEI 12207:1995 – *Tecnologías de la información. Procesos del ciclo de vida del software. (Information technology. Software life cycle processes).*

ANSI/ISA S84:1996 – *Aplicación de los sistemas de seguridad con instrumentación para las industrias de proceso. (Application of safety instrumented systems for the process industries).*

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 61508-1 + corr. mayo	1998 1999	Seguridad funcional de los sistemas eléctricos/electrónicos/electrónicos programables relacionados con la seguridad. Parte 1: Requisitos generales	EN 61508-5	2001	UNE-EN 61508-1:2003
CEI 61508-2	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	EN 61508-2	2001	UNE-EN 61508-2:2003
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
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 ISO/CEI 51	1990	Directrices para incluir en las normas los aspectos relacionados con la seguridad	–	–	–
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	–	–	–

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