NORMA CUBANA

NC

IEC 61508-4: 2012
(Publicada por la IEC en 1998)

SEGURIDAD FUNCIONAL DE LOS SISTEMAS ELÉCTRICOS/ELECTRÓNICOS/ELECTRÓNICOS PROGRAMABLES RELACIONADOS CON LA SEGURIDAD — PARTE 4: DEFINCIONES Y ABREVIATURAS (IEC 61508-4: 1998 + Corr 1999, IDT)

Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 4: Definitions and abbreviations

ICS: 25.040.40; 29.020

1. Edición Diciembre 2012

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

Cuban National Bureau of Standards

Prefacio

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

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

Esta Norma Cubana:

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

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

- Es una adopción idéntica por el método de reimpresión de la versión oficial en español de la Norma Europea EN 61508-4: 2001 *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 4: Definitions and abbreviations* que a su vez adopta de forma idéntica a la Norma Internacional IEC 61508-4: 1998 + Corr 1999)

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 61508-4

Diciembre 2001

ICS 25.040.40; 29.020

Versión en español

Seguridad funcional de los sistemas eléctricos/electrónicos/electrónicos programables relacionados con la seguridad
Parte 4: Definiciones y abreviaturas
(CEI 61508-4:1998 + corrigendum 1999)

Functional safety of electrical/electronic/programmable electronic safety-related systems. Part 4: Definitions and abbreviations. (IEC 61508-4:1998 + corrigendum 1999).

Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité. Partie 4: Définitions et abréviations. (CEI 61508-4:1998 + corrigendum 1999)

Funktionale Sicherheit sicherheitsbezogener elektrischer/ elektronischer/programmierbarer elektronischer Systeme. Teil 4: Begriffe und Abkürzungen. (IEC 61508-4:1998 + 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

ANTECEDENTES

El texto de la Norma Internacional CEI 61508-4:1998 y su corrigendum de abril de 1999, preparado por el Subcomité SC 65A, *Aspectos de sistemas*, del Comité Técnico TC 65, *Medida y control en procesos industriales*, de CEI, fue sometido al Procedimiento de Aceptación Única (UAP) y fue aprobado por CENELEC como Norma Europea EN 61508-4 el 2001-07-03 sin ninguna modificación.

Se fijaron las siguientes fechas:

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

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

Los anexos denominados “informativos” se dan sólo para información.

En esta norma el anexo ZA es normativo y el anexo A es informativo.

El anexo ZA ha sido añadido por CENELEC.

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

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

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

- CEI 61511 – *Seguridad funcional. Sistemas instrumentados de seguridad para el sector de industrias de transformación.*
- CEI 62061 – *Seguridad de las máquinas. Seguridad funcional de los sistemas de control eléctricos, electrónicos y electrónicos programables.*
- CEI 61513 – *Centrales nucleares. Instrumentación y control para los sistemas importantes para la seguridad. Requisitos generales para los sistemas.*

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

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

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

DECLARACIÓN

El texto de la Norma Internacional CEI 61508-4:1998 y su corrigendum de abril de 1999 fue aprobado por CENELEC como norma europea sin ninguna modificación.

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

CEI 61131-3:1993	NOTA – Armonizada como Norma EN 61131-3:1993 (sin ninguna modificación).
ISO 9000-3:1991	NOTA – Armonizada como Norma EN 29000-3:1993 (sin ninguna modificación).

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

ÍNDICE

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. Éstos 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;

- 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;

---

1) PES del inglés: Programmable Electronic Systems.

– 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 4: Definiciones y abreviaturas

1 OBJETO Y CAMPO DE APLICACIÓN

1.1 Esta parte de la Norma CEI 61508 contiene las definiciones y explicaciones de los términos que se usan en las partes 1 a 7 de esta norma.

1.2 Las definiciones están agrupadas bajo títulos generales de forma que los términos relacionados se puedan entender dentro del contexto mutuo. Sin embargo, debería observarse que estos títulos generales no pretenden añadir significado a las definiciones, y en este sentido no se deberían tener en cuenta dichos títulos generales.

1.3 Las partes 1, 2, 3 y 4 de esta norma son publicaciones básicas de seguridad, aunque este estado no se aplica en el contexto de los sistemas E/E/PE relacionados con la seguridad de baja complejidad (véase el apartado 3.4.4 de la parte 4). Como publicaciones básicas de seguridad, están destinadas a su uso por los comités técnicos en 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 están también destinadas a su uso como publicaciones independientes.

Una de las responsabilidades de un comité técnico es, en los casos en que sea aplicable, hacer uso de las publicaciones básicas de seguridad en la preparación de sus publicaciones. En este contexto, no serán aplicables los requisitos, métodos de ensayo o condiciones de ensayo de esta publicación básica de seguridad a no ser que se haga referencia a ellos o se incluyan en las publicaciones preparadas por dichos comités técnicos.

1.4 La figura 1 muestra la estructura general de las partes 1 a 7 de la Norma CEI 61508 e indica el papel que juega la Norma CEI 61058-4 en el logro de la seguridad funcional para los sistemas E/E/PE relacionados con la seguridad.

NOTA – En Estados Unidos y 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 61058 (es decir, la Norma CEI 61511), para el sector de procesos, sea publicada en Estados Unidos y en Canadá

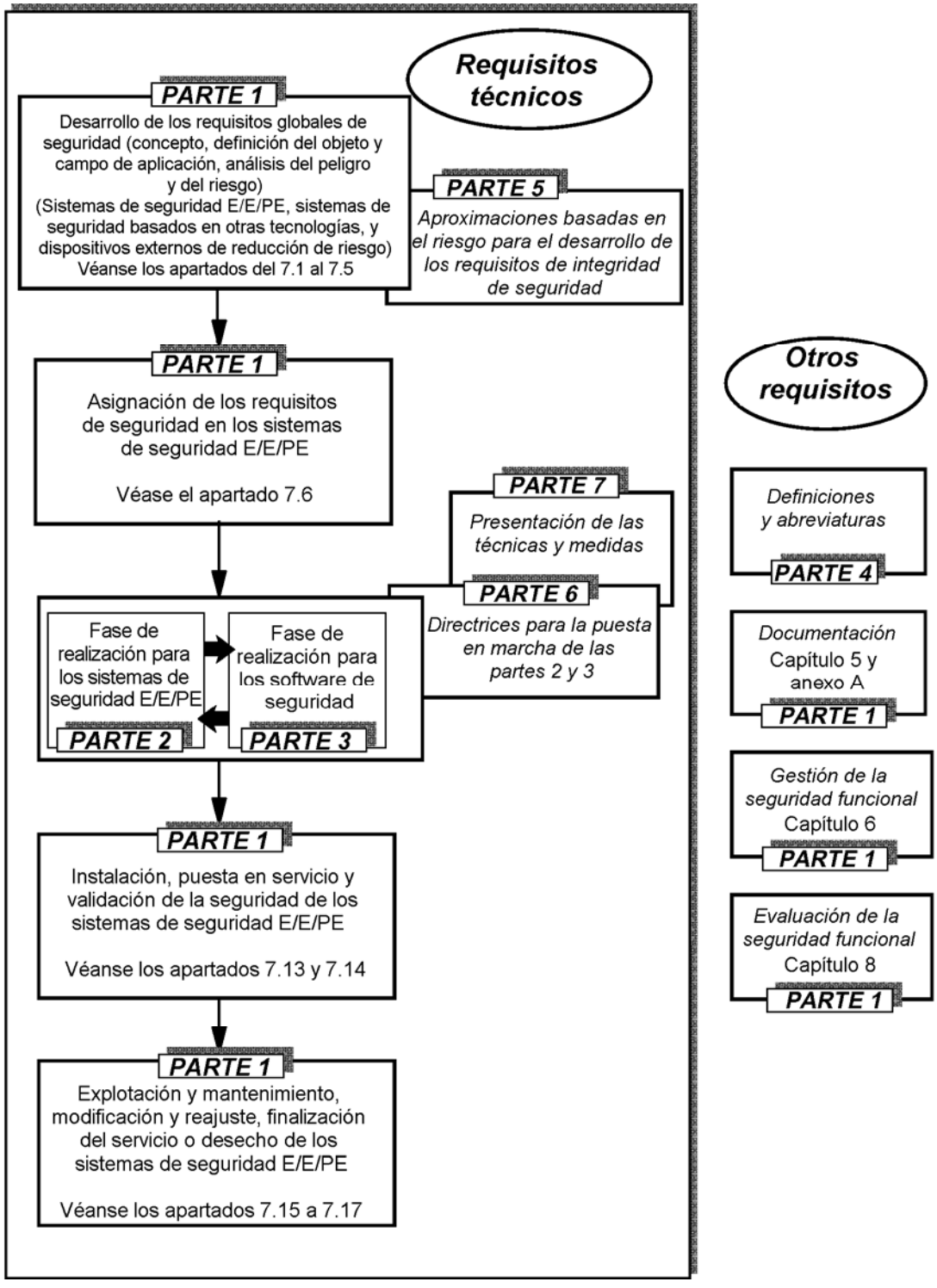


Fig. 1 – Estructura general de esta norma

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 60050-191:1990 – *Vocabulario Electrotécnico Internacional (VEI). Capítulo 191: Compatibilidad y calidad de servicio.*

CEI 60050-351:1975 – *Vocabulario Electrotécnico Internacional (VEI). Capítulo 351: Control automático.*

CEI 61058-1:1998 – *Seguridad funcional de los sistemas eléctricos/electrónicos/electrónicos programables relacionados con la seguridad. Parte 1: Requisitos generales.*

CEI 61058-2:2000 – *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 61058-3:1998 – *Seguridad funcional de los sistemas eléctricos/electrónicos/electrónicos programables relacionados con la seguridad. Parte 3: Requisitos del software (soporte lógico).*

CEI 61058-5:1998 – *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 61058-6:2000 – *Seguridad funcional de los sistemas eléctricos/electrónicos/electrónicos programables relacionados con la seguridad. Parte 6: Directrices para la aplicación de la Norma CEI 61058-2 y de la Norma CEI 61508-3.*

CEI 61058-7:2000 – *Seguridad funcional de los sistemas eléctricos/electrónicos/electrónicos programables relacionados con la seguridad. Parte 7: Presentación de técnicas y medidas.*

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.*

ISO/CEI 2382-14:1998 – *Tecnologías de la información. Vocabulario. Parte 14: Fiabilidad, mantenibilidad y disponibilidad.*

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

ISO 8402:1994 – *Gestión de la calidad y aseguramiento de la calidad. Vocabulario.*

3 DEFINICIONES Y ABREVIATURAS

Para los fines de esta norma internacional, se aplican las definiciones siguientes, así como las abreviaturas dadas en la tabla 1.

Tabla 1
Abreviaturas utilizadas en esta norma

Abreviatura	Expresión completa	Definición y/o explicación del término
MooN	Arquitectura de M canales entre N (por ejemplo 1oo2 es una arquitectura en la que cada uno de los dos canales puede cumplir la función de seguridad)	Anexo B de la Norma CEI 61508-6
MooND	Arquitectura de M canales entre N con diagnóstico	Anexo B de la Norma CEI 61058-6
ALARP	Tan baja como se pueda conseguir en la práctica	Anexo B de la Norma CEI 61058-5
E/E/PE	Eléctrico/electrónico/electrónico programable	Apartado 3.2.6
E/E/PES	Sistema eléctrico/electrónico/electrónico programable	Apartado 3.3.3
EUC	Equipo bajo control	Apartado 3.2.3
PES	Sistema electrónico programable	Apartado 3.3.2
PLC	Autómata programable	Anexo E de la Norma CEI 61058-6
SIL	Nivel de integridad de seguridad	Apartado 3.5.6

3.1 Términos relacionados con la seguridad

3.1.1 daño: Herida física o acción contra la salud que afecta a las personas, sea directamente o sea indirectamente, como consecuencia de un deterioro causado en los bienes o en el medio ambiente.

[Guía ISO/CEI 51:1990 (modificada)]

NOTA – Se debe considerar esta definición en caso de análisis de un fenómeno peligroso y de un riesgo (véase la Norma CEI 61508–1, apartado 7.4). Si se ampliara el objeto y campo de aplicación (para incluir, por ejemplo, los deterioros causados al medio ambiente que no produjeran heridas físicas o acciones contra la salud), debería considerarse en la fase de definición global del objeto y campo de aplicación (véase la Norma CEI 61508-1, apartado 7.3).

3.1.2 fenómeno peligroso; peligro: Fuente potencial de daño [Guía ISO/CEI 51:1990].

NOTA – Este término incluye el peligro para las personas dentro de un intervalo corto de tiempo (por ejemplo fuego o explosión), así como los peligros con efecto a largo plazo sobre la salud de una persona (por ejemplo, el desprendimiento de una sustancia tóxica).

3.1.3 situación peligrosa: Circunstancia en la cual una persona es expuesta a fenómenos peligrosos.

3.1.4 evento peligroso: Situación peligrosa que da lugar a un daño.

3.1.5 riesgo: Combinación de la probabilidad de que se produzca un daño y de su severidad.

[Guía ISO/CEI 51:1990 (modificada)]

NOTA – Para más información sobre este concepto, véase el anexo A de la Norma CEI 61508-5.

3.1.6 riesgo tolerable: Riesgo aceptado en un contexto determinado basado en los valores vigentes de la sociedad.

NOTA – Véase el anexo B de la Norma CEI 61508-5.

3.1.7 riesgo residual: Riesgo que queda después de tomar medidas de protección.

3.1.8 seguridad: Ausencia de riesgo inaceptable.

3.1.9 seguridad funcional: Parte de la seguridad global que se refiere al EUC y al sistema de control del EUC que depende del funcionamiento correcto de los sistemas E/E/EP relacionados con la seguridad, sistemas relacionados con la seguridad basados en otras tecnologías y dispositivos externos de reducción de riesgo.

3.1.10 estado de seguridad: Estado del EUC cuando se logra la seguridad.

NOTA – Durante su evolución desde un estado potencialmente peligroso al estado de seguridad final, el EUC puede pasar por cierto número de estados de seguridad intermedios. En determinadas situaciones, existe sólo un estado seguro durante el tiempo en el que el EUC está continuamente controlado. Este control continuo puede extenderse en un periodo de tiempo corto o indefinido.

3.1.11 mala utilización razonablemente previsible: Utilización de un producto, de un proceso o de un servicio en condiciones o para fines no previstos por el proveedor, pero que puede ser inducida por el producto, el proceso o el servicio en combinación con, o como resultado de un comportamiento humano habitual.

3.2 Equipo y dispositivos

3.2.1 unidad funcional: Entidad de hardware o de software, o de ambos, capaz de cumplir una función determinada.

NOTA – En el VEI 191-01-01, se emplea el término “entidad” en lugar de unidad funcional. En determinados casos una entidad puede incluir personal.

[Norma ISO/CEI 2382-14-01-01)]

3.2.2 software (soporte lógico): Creación intelectual que comprende los programas, procedimientos, datos, reglas y cualquier documentación que se refiera al funcionamiento de un sistema de proceso de datos.

NOTA 1 – El software es independiente del soporte en el que se registra.

NOTA 2 – Esta definición, sin la nota 1, difiere de la Norma ISO 2382-1, y la definición completa difiere de la Norma ISO 9000-3 por la adición de la palabra “datos”.

3.2.3 equipo bajo control (EUC): Equipo, máquina, aparato o planta utilizados para las actividades de fabricación, proceso, transporte, médicas u otras.

NOTA – El sistema de control del EUC es separado y distinto del EUC.

3.2.4 riesgo del EUC: Riesgo que procede del EUC o de su interacción con el sistema de control del EUC.

NOTA 1 – En este contexto, el riesgo es el asociado con el evento peligroso específico para el que se deben usar los sistemas E/E/PE relacionados con la seguridad, los sistemas relacionados con la seguridad basados en otras tecnologías y los dispositivos externos de reducción de riesgo para proporcionar la necesaria reducción de riesgo (es decir, el riesgo asociado a la seguridad funcional).

NOTA 2 – En la figura A.1 de la Norma CEI 61508-5 se aborda el riesgo del EUC. El objetivo principal de determinar el riesgo del EUC es establecer un punto de referencia para el riesgo sin tener en cuenta los sistemas E/E/PE relacionados con la seguridad, los sistemas relacionados con la seguridad basados en otras tecnologías y los dispositivos externos de reducción de riesgo.

NOTA 3 – La evaluación de este riesgo comprende los problemas asociados al factor humano.

3.2.5 electrónico programable (PE): Basado en la tecnología informática, que puede comprender hardware, software, y unidades de entrada y de salida.

NOTA – Este término cubre los dispositivos microelectrónicos basados en una o más unidades centrales de proceso (CPU) junto con sus memorias asociadas, etc.

EJEMPLO Todos los siguientes son dispositivos electrónicos programables:

– los microprocesadores;

– los microcontroladores;

– los autómatas programables (PC);

– los circuitos integrados específicos de una aplicación (ASIC);

– los autómatas lógicos programables (PLC);

– los demás dispositivos basados en la informática (por ejemplo los sensores inteligentes, los transmisores, los accionadores).

3.2.6 eléctrico/electrónico/electrónico programable (E/E/PE): Basado en la tecnología eléctrica (E), y/o electrónica (E) y/o electrónica programable (PE).

NOTA – Este término designa el conjunto de los aparatos y sistemas que funcionan según los principios eléctricos.

EJEMPLO Los dispositivos eléctricos/electrónicos/electrónicos programables comprenden

– los dispositivos electromecánicos (eléctricos);

– los dispositivos electrónicos no programables con circuitos integrados (electrónicos);

– los dispositivos electrónicos basados en la tecnología informática (electrónicos programables), véase el apartado 3.2.5.

3.2.7 lenguaje de variabilidad limitada: Lenguaje de programación de software, textual o gráfico, para autómatas programables, comerciales e industriales, con un rango de capacidades limitado a su aplicación.

EJEMPLO Los siguientes son lenguajes de variabilidad limitada, definidos a partir de la Norma CEI 61131-3 y de otras fuentes, que se usan para representar el programa de aplicación de un sistema de autómatas programables (PLC):

– diagrama de escalera: un lenguaje gráfico que comprende una serie de símbolos de entrada (que representan un comportamiento de dispositivos similares a contactos) interconectados por líneas (para indicar el flujo de corriente) a símbolos de salida (que representan un comportamiento similar a relés);

– álgebra de Boole: un lenguaje de bajo nivel basado en operadores booleanos tales como Y, O y NO con la capacidad de añadir algunas instrucciones mnemotécnicas;

– diagrama de bloques funcionales: además de los operadores booleanos, permite el uso de funciones más complejas, tales como ficheros de transferencia de datos, bloque de transferencia lectura/escritura, registro de desvío e instrucciones de secuenciador;

– diagrama funcional en secuencia: una representación gráfica de un programa secuencial que consiste en etapas interconectadas, acciones y enlaces dirigidos con condiciones de transición.

3.3 Sistemas: aspectos generales

3.3.1 sistema: Conjunto de elementos que interactúan de acuerdo con un diseño, donde un elemento de un sistema puede ser otro sistema, denominado subsistema, el cual puede ser un sistema de control o un sistema controlado y puede incluir hardware, software e interacción humana.

NOTA 1 – Una persona puede formar parte de un sistema (véase también la nota 5 del apartado 3.4.1).

NOTA 2 – Esta definición difiere del VEI 351-01-01.

3.3.2 sistema electrónico programable (PES): Sistema de control, protección o supervisión basado en uno o más dispositivos electrónicos programables, incluyendo todos los elementos del sistema, tales como la alimentación de potencia, los sensores y otros dispositivos de entrada, las líneas de datos y otras vías de comunicación, así como los accionadores y otros dispositivos de salida (véase la figura 2).

NOTA – En la figura 2a) se muestra la estructura de un PES. La figura 2b) ilustra la forma en que se representa un PES en esta norma internacional, con la electrónica programable mostrada como una unidad distinta de los sensores y de los accionadores en el EUC y en sus interfaces. Sin embargo, la electrónica programable puede existir en diversos lugares del PES. La figura 2c) ilustra un PES con dos unidades discretas de electrónica programable. La figura 2d) ilustra un PES provisto de una electrónica programable duplicada (es decir, de dos canales), pero con un solo sensor y un solo accionador.

3.3.3 sistema eléctrico/electrónico /electrónico programable (E/E/PES): Sistema de control, protección o supervisión basado en uno o más dispositivos eléctricos/electrónicos/electrónicos programables (E/E/PE), incluyendo todos los elementos del sistema, tales como la alimentación de potencia, los sensores y otros dispositivos de entrada, las pistas de datos y otras vías de comunicación, así como los accionadores y otros dispositivos de salida (véase la figura 3).

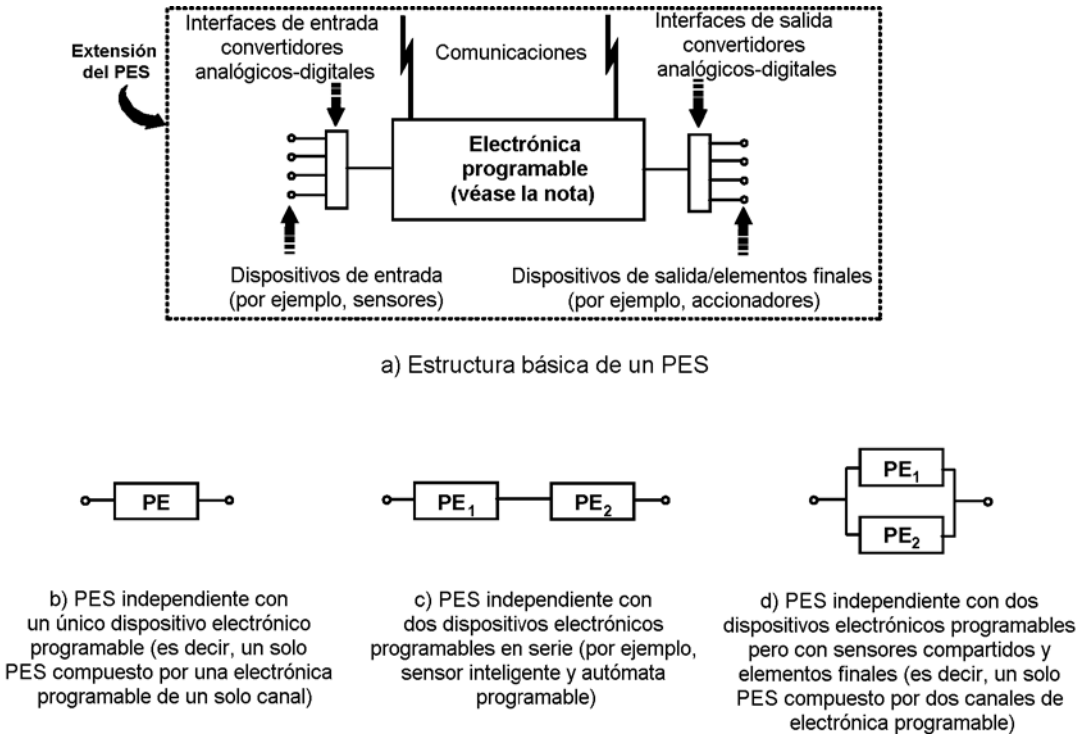
3.3.4 sistema de control del EUC: Sistema que responde a las señales de entrada procedentes del proceso y/o de un operador y genera señales de salida que obligan al EUC a funcionar de la manera deseada.

NOTA – El sistema de control del EUC incluye dispositivos de entrada y elementos finales.

3.3.5 arquitectura: Configuración específica de los elementos de hardware y de software en un sistema.

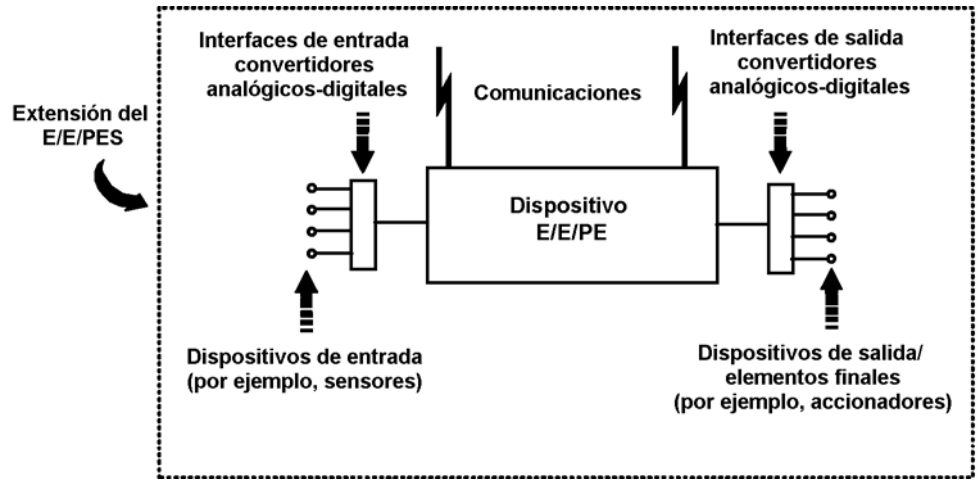
3.3.6 módulo: Componente de serie discreto o un conjunto funcional de componentes de serie o discretos encapsulados juntos.

3.3.7 módulo del software: Construcción que consiste en procedimientos y/o declaraciones de datos que pueden también interactuar con otras construcciones análogas.



NOTA – La electrónica programable se presenta en forma centrada, pero puede colocarse en diversos emplazamientos del PES.

Fig. 2 – Sistema electrónico programable (PES): estructura y terminología



NOTA – El dispositivo E/E/PE se presenta en forma centrada, pero puede colocarse en diversos emplazamientos del E/E/PES.

Fig. 3 – Sistema eléctrico/electrónico/electrónico programable (E/E/PES): estructura y terminología

3.3.8 canal: Elemento o grupo de elementos que ejecuta(n) una función independientemente.

EJEMPLO Una configuración de dos canales (de doble canal) comprende dos canales que realizan independientemente la misma función.

NOTA 1 – Los elementos dentro de un canal podrían incluir módulos de entrada/salida, un sistema lógico (véase apartado 3.4.5), sensores y elementos finales.

NOTA 2 – Se puede usar este término para describir un sistema completo, o una porción de un sistema (por ejemplo sensores o elementos finales).

3.3.9 diversidad: Medios diferentes para realizar una función requerida.

EJEMPLO Se puede lograr la diversidad utilizando medios físicos diferentes u otros enfoques de diseño.

3.3.10 redundancia: Existencia de medios, adicionales a los medios que serían suficientes para que una unidad funcional realizara una función requerida o para representar información mediante datos.

EJEMPLO Son casos de redundancia la utilización de componentes funcionales duplicados y la adición de bits de paridad.

NOTA 1 – La redundancia se usa principalmente para mejorar la fiabilidad o la disponibilidad.

NOTA 2 – La definición en el VEI 191-15-01 es menos completa.

[ISO/CEI 2382-14-01-12]

3.4 Sistemas: aspectos relacionados con la seguridad

3.4.1 sistemas relacionados con la seguridad: Un sistema así designado es un sistema que, simultáneamente

– aplica las funciones de seguridad requeridas necesarias para lograr o mantener un estado de seguridad del EUC o para mantener tal estado; y

– está destinado a alcanzar, por sí mismo o con otros sistemas E/E/PE, sistemas relacionados con la seguridad basados en otras tecnologías o dispositivos externos de reducción de riesgo, el nivel de integridad de seguridad necesario para las funciones de seguridad requeridas.

NOTA 1 – El término se refiere a aquellos sistemas específicos, denominados como relacionados con la seguridad, que están destinados a alcanzar, junto con las dispositivos externos de reducción de riesgo (véase el apartado 3.4.3), la reducción de riesgo necesaria a fin de alcanzar el riesgo tolerable requerido (véase apartado 3.1.6). Véase también el anexo A de la Norma CEI 61508-5.

NOTA 2 – Los sistemas relacionados con la seguridad están diseñados para evitar que el EUC se sitúe en un estado peligroso tomando las medidas apropiadas desde la recepción de las órdenes. El fallo de un sistema relacionado con la seguridad estaría entonces incluido entre los eventos que conducen a fenómeno(s) peligroso(s). Aunque puede haber otros sistemas que posean funciones de seguridad, son los sistemas relacionados con la seguridad los que han sido diseñados para lograr, a su modo, el riesgo tolerable requerido. Los sistemas relacionados con la seguridad se pueden dividir genéricamente en sistemas de control relacionados con la seguridad y en sistemas de protección relacionados con la seguridad, y tienen dos modos de funcionamiento (véase el apartado 3.5.12).

NOTA 3 – Los sistemas relacionados con la seguridad pueden formar parte integrante del sistema de control del EUC o pueden relacionarse en interfaces con el EUC mediante sensores y/o accionadores. Esto significa que se puede lograr la integridad de seguridad requerida aplicando las funciones de seguridad en el sistema de mando del EUC (y posiblemente también por sistemas adicionales separados e independientes) o se pueden aplicar las funciones de seguridad por sistemas separados e independientes dedicados a la seguridad.

NOTA 4 – Un sistema relacionado con la seguridad puede

a) estar diseñado para evitar el evento peligroso (es decir, que no se produzca ningún evento peligroso si el sistema relacionado con la seguridad realiza sus funciones);

b) estar diseñado para mitigar los efectos del evento peligroso, reduciendo así el riesgo al reducir sus consecuencias;

c) estar diseñado para lograr una combinación de a) y b).

NOTA 5 – Una persona puede formar parte de un sistema relacionado con la seguridad (véase el apartado 3.3.1). Por ejemplo una persona podría recibir información de un dispositivo electrónico programable y realizar una acción de seguridad a partir de dicha información a través de un dispositivo electrónico programable;

NOTA 6 – El término incluye todo el hardware, software y dispositivos de soporte (por ejemplo alimentadores de potencia) necesarios para realizar la función de seguridad especificada (los sensores, los otros dispositivos de entrada, los elementos finales (accionadores) y los otros dispositivos de salida están comprendidos por tanto en el sistema relacionado con la seguridad).

NOTA 7 – Un sistema relacionado con la seguridad se puede basar en una amplia gama de tecnologías que incluye las tecnologías eléctrica, electrónica, electrónica programable, hidráulica y neumática.

3.4.2 sistema relacionado con la seguridad basado en otra tecnología: Sistema relacionado con la seguridad basado en una tecnología que no sea eléctrica/electrónica/electrónica programable.

EJEMPLO Una válvula de seguridad es un sistema relacionado con la seguridad basado en otra tecnología.

3.4.3 dispositivos externos de reducción de riesgo: Medidas para reducir o mitigar los riesgos que son separados y distintos de, y que no utilizan, sistemas relacionados con la seguridad E/E/PE o sistemas relacionados con la seguridad basados en otra tecnología.

EJEMPLO Un sistema de drenaje, un cortafuegos y un dique son todos dispositivos externos de reducción de riesgo.

3.4.4 sistema E/E/PE relacionado con la seguridad de baja complejidad: Sistema E/E/PE relacionado con la seguridad (véanse los apartados 3.2.6 y 3.4.1), en el cual

– los modos de fallo de cada componente individual están bien definidos;

– el comportamiento del sistema en condiciones anormales puede ser determinado por completo.

NOTA – Se puede determinar el comportamiento del sistema en condiciones anormales por métodos analíticos y/o de ensayo.

EJEMPLO Un sistema que comprende uno o más interruptores de final de carrera, que funcionan posiblemente a través de relés electromecánicos interpuestos, uno o varios contactores destinados a cortar la alimentación de motores eléctricos es un sistema E/E/PE relacionado con la seguridad de baja complejidad.

3.4.5 sistema lógico: Parte de un sistema que desarrolla una función lógica pero que excluye los sensores y los elementos finales

NOTA – En esta norma se usan los siguientes sistemas lógicos:

- sistemas lógicos eléctricos para la tecnología electromecánica;
- sistemas lógicos electrónicos para la tecnología electrónica;
- sistemas lógicos electrónicos programables para los sistemas electrónicos programables.

3.5 Funciones de seguridad e integridad de seguridad

3.5.1 función de seguridad: Función a realizar por un sistema E/E/PE relacionado con la seguridad, por sistemas relacionados con la seguridad basados en otra tecnología o por un dispositivo externo de reducción de riesgo que está destinado a lograr o mantener un estado de seguridad del EUC con respecto a un evento peligroso específico (véase el apartado 3.4.1).

3.5.2 integridad de seguridad: Probabilidad de que un sistema relacionado con la seguridad ejecute en forma satisfactoria las funciones de seguridad requeridas en todas las condiciones especificadas en un periodo de tiempo especificado.

NOTA 1 – Cuanto más elevado es el nivel de integridad de seguridad de los sistemas relacionados con la seguridad, menor es la probabilidad de que los sistemas relacionados con la seguridad fallen en la ejecución de las funciones de seguridad requeridas.

NOTA 2 – Hay cuatro niveles de integridad de seguridad para los sistemas (véase el apartado 3.5.6).

NOTA 3 – En la determinación de la integridad de seguridad, se deberían incluir todas las causas de fallo (tanto los fallos de hardware aleatorios como los sistemáticos) que conducen a un estado inseguro, por ejemplo los fallos de hardware, los fallos inducidos de software, y los fallos debidos a las perturbaciones eléctricas. Algunos de estos tipos de fallos, en particular los fallos aleatorios de hardware, se pueden cuantificar usando medidas tales como la tasa de fallo en modo de fallo peligroso o la probabilidad de fallo de funcionamiento a la demanda de un sistema relacionado con la seguridad. Sin embargo, la integridad de seguridad de un sistema depende también de muchos factores que no se pueden cuantificar con precisión, sino que sólo se pueden considerar en forma cualitativa.

NOTA 4 – La integridad de seguridad comprende la integridad de seguridad del hardware (véase el apartado 3.5.5) y la integridad de seguridad sistemática (véase el apartado 3.5.4).

NOTA 5 – Esta definición está centrada en la fiabilidad de los sistemas relacionados con la seguridad para realizar funciones de seguridad (véase el VEI 191-12-01 para una definición de fiabilidad).

3.5.3 integridad de seguridad del software: Medida que significa la probabilidad de que el software de un sistema electrónico programable ejecute sus funciones de seguridad en todas las condiciones especificadas dentro de un periodo de tiempo especificado.

3.5.4 integridad de seguridad sistemática: Parte de la integridad de los sistemas relacionados con la seguridad que se refiere a los fallos sistemáticos (véase nota 3 del apartado 3.5.2) en un modo de fallo peligroso.

NOTA 1 – La integridad de seguridad sistemática normalmente no puede ser cuantificada (al contrario de la integridad de seguridad del hardware, que normalmente si puede serlo).

NOTA 2 – Véanse los apartados 3.5.2, 3.5.5 y 3.6.6.

3.5.5 integridad de seguridad del hardware: Parte de la integridad de seguridad de los sistemas relacionados con la seguridad que se refiere a los fallos aleatorios del software en modo de fallo peligroso.

NOTA 1 – Este término se refiere a los fallos en modo peligroso, es decir a los fallos que se presentan en un sistema relacionado con la seguridad y que son susceptibles de perjudicar a su integridad de seguridad. Los dos parámetros a considerar en este contexto son la tasa de fallo peligroso global y la probabilidad de fallo del funcionamiento bajo demanda. El primero de estos dos parámetros de fiabilidad se utiliza cada vez que es necesario mantener un control continuo a fin de garantizar la seguridad; el segundo parámetro de fiabilidad se usa en el contexto de los sistemas de protección relacionados con la seguridad.

NOTA 2 – Véanse los apartados 3.5.2, 3.5.4 y 3.6.5.

3.5.6 nivel de integridad de seguridad (SIL): Nivel discreto (uno entre los cuatro posibles) que permite especificar los requisitos de integridad de seguridad de las funciones de seguridad a asignar a los sistemas E/E/PE relacionados con la seguridad, donde el nivel 4 de integridad de seguridad posee el grado más elevado de integridad de seguridad y el nivel 1 el más bajo.

NOTA – Las medidas objetivo de fallo (véase el apartado 3.5.13) para los cuatro niveles de integridad de seguridad se especifican en las tablas 2 y 3 de la Norma CEI 61508-1.

3.5.7 nivel de integridad de seguridad del software: Nivel discreto (uno entre los cuatro posibles) que permite especificar la integridad de seguridad del software de un sistema relacionado con la seguridad.

NOTA – Véanse los apartados 3.5.3 y 3.5.6.

3.5.8 especificación de requisitos de seguridad: Especificación que contiene todos los requisitos relacionados con las funciones de seguridad que tienen que ser ejecutadas por los sistemas relacionados con la seguridad.

NOTA – La especificación se divide en

- especificación de requisitos de funciones de seguridad (véase el apartado 3.5.9);
- especificación de requisitos de integridad de seguridad (véase el apartado 3.5.10).

3.5.9 especificación de requisitos de funciones de seguridad: Especificación que contiene los requisitos necesarios para las funciones de seguridad que tienen que ser ejecutadas por los sistemas relacionados con la seguridad.

NOTA 1 – Esta especificación constituye una parte (la parte que se refiere a las funciones de seguridad) de la especificación de requisitos de seguridad (véase el apartado 3.5.8) y contiene detalles precisos de las funciones de seguridad que tienen que ser realizadas por los sistemas relacionados con la seguridad.

NOTA 2 – Las especificaciones pueden contener documentos en forma de texto, diagramas de flujo, matrices, diagramas lógicos, etc. que permiten definir claramente las funciones de seguridad.

3.5.10 especificación de requisitos de integridad de seguridad: Especificación que contiene los requisitos relativos a la integridad de seguridad de las funciones de seguridad que tienen que ser ejecutadas por los sistemas relacionados con la seguridad.

NOTA – Esta especificación constituye una parte (la parte que se refiere a la integridad de seguridad) de la especificación de requisitos de seguridad (véase el apartado 3.5.8).

3.5.11 software de seguridad; software relacionado con la seguridad: Software utilizado para ejecutar funciones de seguridad en sistemas relacionados con la seguridad.

3.5.12 modo de funcionamiento: Modo en el que se prevé utilizar un sistema relacionado con la seguridad, con respecto a la frecuencia de las demandas, que puede ser

- **modo de baja demanda:** en el cual la frecuencia de las demandas de funcionamiento realizadas a un sistema relacionado con la seguridad no es superior a una por año ni superior al doble de la frecuencia de ensayos periódicos;
- **modo de alta demanda o modo continuo:** en el cual la frecuencia de las demandas de funcionamiento realizadas a un sistema relacionado con la seguridad es superior a una por año o superior al doble de la frecuencia de ensayos periódicos;

NOTA 1 – El modo de alta demanda o modo continuo cubre los sistemas relacionados con la seguridad que aplican control continuo para mantener la seguridad funcional.

NOTA 2 – Las medidas objetivo de fallo para sistemas relacionados con la seguridad que funcionan en el modo de baja demanda y en el modo de alta demanda o continuo se definen en el apartado 3.5.13.

3.5.13 medida objetivo de fallo: Probabilidad prevista en modo de fallos peligrosos a conseguir con respecto a los requisitos de integridad de seguridad, especificada en términos de:

– probabilidad media de fallo a ejecutar bajo demanda de la función de diseño (para un modo de baja demanda de funcionamiento);

– probabilidad de un fallo peligroso por hora (para un modo de alta demanda o modo continuo de funcionamiento);

NOTA – Los valores numéricos para las medidas objetivo de fallo aparecen en las tablas 2 y 3 de la Norma CEI 61508-1.

3.5.14 reducción de riesgo necesaria: Reducción de riesgo a realizar por el sistema E/E/PE relativo a la seguridad, un sistema relativo a la seguridad basado en otra tecnología y por los dispositivos externos de reducción de riesgo a fin de asegurar que no se excede el riesgo tolerable.

3.6 Anomalía, fallo y error

3.6.1 anomalía: Condición anormal que puede provocar una reducción de capacidad o la pérdida de capacidad de una unidad funcional para cumplir una función requerida.

NOTA – El VEI 191-05-01 define “avería” (en francés "panne" y en inglés "fault") como estado de un elemento caracterizado por la inaptitud para realizar una función requerida, excluyendo la inaptitud debida al mantenimiento preventivo, u otras acciones programadas o a una falta de medios exteriores. El término en inglés "fault" tiene por tanto dos sentidos diferentes designados por dos términos en español diferentes. Véase en la figura 4 una ilustración de ambos puntos de vista.

[ISO/CEI 2382-14-01-10]

3.6.2 prevención de anomalías: Utilización de técnicas y procedimientos destinados a evitar la aparición de anomalías durante cada una de las fases del ciclo de vida de seguridad del sistema relacionado con la seguridad.

3.6.3 tolerancia a las anomalías: Aptitud de una unidad funcional para continuar cumpliendo una función requerida en presencia de anomalías o errores.

NOTA – La definición del término "tolerancia a las averías" en el VEI 191-15-05 sólo se refiere a las averías de los subelementos. Véase la nota del término anomalía en el apartado 3.6.1.

[ISO/CEI 2382-14-04-06]

3.6.4 fallo: Cese de la capacidad de una unidad funcional para continuar cumpliendo una función requerida.

NOTA 1 – La definición en el VEI 191-04-01 es la misma con notas adicionales.

[ISO/CEI 2382-14-01-11]

NOTA 2 – Véase en la figura 4 la relación entre anomalías (averías) y fallos, tanto en la Norma CEI 61508 como en la Norma CEI 60050-191.

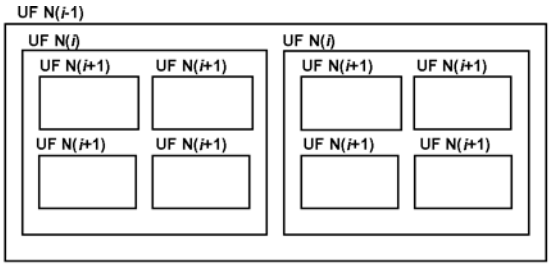
NOTA 3 – El cumplimiento de una función requerida excluye necesariamente determinados comportamientos, y se pueden especificar determinadas funciones en términos de comportamientos a evitar. La presencia de un comportamiento de este tipo constituye un fallo.

NOTA 4 – Los fallos son aleatorios (en el hardware) o sistemáticos (en el hardware o en el software), véanse los apartados 3.6.5 y 3.6.6.

3.6.5 fallos aleatorios del hardware: Fallos que sobrevienen de manera aleatoria y que resultan de diversos mecanismos de degradación del hardware.

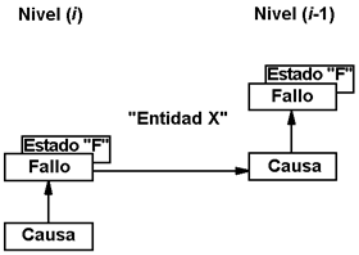
NOTA 1 – Existen muchos mecanismos de degradación que se presentan con diferentes frecuencias en diversos componentes y, dado que las tolerancias de fabricación tienen por consecuencia un fallo de los componentes causado por dichos mecanismos al cabo de tiempos diferentes, los fallos que se producen en un equipo que comprende muchos componentes se presentan con frecuencias previsibles, pero en momentos impredecibles (es decir, aleatorios).

NOTA 2 – Una de las diferencias principales entre los fallos aleatorios del hardware y los fallos sistemáticos (véase el apartado 3.6.6), es que las tasas de fallo del sistema (u otras medidas apropiadas), que surgen de los fallos aleatorios del hardware, se pueden predecir con una precisión razonable, mientras que los fallos sistemáticos, por su propia naturaleza, no se pueden predecir con precisión. Es decir, las tasas de fallo del sistema, que surgen de fallos aleatorios, se pueden cuantificar con precisión razonable, pero las que surgen de fallos sistemáticos no se pueden cuantificar con precisión en forma estadística debido a que los hechos que conducen a los mismos no se pueden predecir con facilidad.

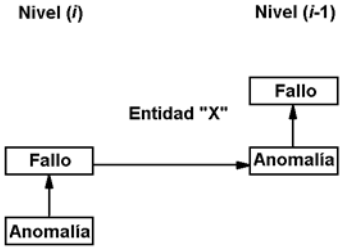


(N = nivel; UF = unidad funcional; *i* = 1, 2, 3, etc)

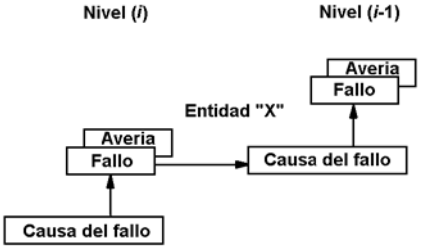
a) Configuración de una unidad funcional



b) Punto de vista general



c) Desde el punto de vista de la Norma CEI 61508 y de la Norma ISO/CEI 2382-14



d) Desde el punto de vista de la Norma CEI 60050(191)

NOTA 1 – Como se muestra en a) una unidad funcional se puede considerar como una composición jerárquica de múltiples niveles, cada uno de los cuales puede a su vez denominarse una unidad funcional. En el nivel (*i*), una "causa" puede manifestarse como un error (una desviación a partir del valor o estado correcto) de una unidad funcional de este nivel (*i*), y si no se corrige o rodea, puede provocar un fallo de esta unidad funcional, como resultado del cual cae a un estado "F" en el que ya no es capaz de cumplir una función requerida (véase el punto b)). Este estado "F" de la unidad funcional del nivel (*i*) puede manifestarse a su vez como un error en la unidad funcional del nivel (*i*-1) y si no fuera corregido o rodeado puede ser causa de un fallo de esta unidad funcional de nivel (*i*-1).

NOTA 2 – En esta cadena de causas y de efectos, la misma cosa ("Entidad X") se puede ver como un estado (estado "F") de la unidad funcional del nivel (*i*) en la que ha caído como consecuencia de su fallo y también como causa del fallo de la unidad funcional del nivel (*i*-1). Esta "Entidad X" combina el concepto de "anomalía" de la Norma CEI 61508 y el de la Norma ISO/CEI 2382-14, que destaca su aspecto de causa, tal como se ilustra en el punto c) y el de avería de la Norma CEI 60050-191, que destaca su aspecto de estado, como se ilustra en el punto d). El estado "F" se denomina avería en la Norma CEI 60050-191, mientras que no se define en la Norma CEI 61508 ni en la Norma ISO/CEI 2382-14.

NOTA 3 – En algunos casos, un fallo o un error puede ser causado por un evento externo, tal como un rayo o una perturbación electrostática, antes que por una anomalía interna. Análogamente, una anomalía (en la Norma ISO/CEI 2382-14) o una avería (en la Norma CEI 60050-191) puede existir sin un fallo previo. Un ejemplo de una anomalía de este tipo es una anomalía de diseño.

Fig. 4 – Modelo de fallo

3.6.6 fallo sistemático: Fallo relacionado de forma determinista a una causa concreta, que sólo se puede eliminar por modificación del diseño o del proceso de fabricación, procedimientos de funcionamiento, documentación u otros factores correspondientes.

NOTA 1 – El mantenimiento correctivo sin modificación no eliminará generalmente la causa del fallo.

NOTA 2 – Se puede inducir un fallo sistemático simulando la causa del fallo.

[VEI 191-04-19]

NOTA 3 – Los ejemplos de causas de fallos sistemáticos incluyen errores humanos en

- la especificación de los requisitos de seguridad;
- el diseño, la fabricación, la instalación, el funcionamiento del hardware;
- el diseño, la aplicación, etc. del software.

NOTA 4 – En esta norma, los fallos en un sistema relacionado con la seguridad se pueden clasificar como fallos aleatorios del hardware o como fallos sistemáticos (véanse los apartados 3.6.4 y 3.6.5).

3.6.7 fallo peligroso: Fallo que tiene la potencialidad de poner al sistema relacionado con la seguridad en estado peligroso o de imposibilidad de ejecutar su función.

NOTA – El hecho de que esta potencialidad se realice o no puede depender de la arquitectura del canal del sistema, en los sistemas con canales múltiples para aumentar la seguridad, es menos probable que un fallo peligroso del hardware provoque el estado peligroso general o la imposibilidad de ejecutar la función.

3.6.8 fallo seguro: Fallo que no tiene la potencialidad de poner al sistema relacionado con la seguridad en estado peligroso o en la imposibilidad de ejecutar su función.

NOTA – El hecho de que esta potencialidad se realice o no puede depender de la arquitectura del canal del sistema, en los sistemas con canales múltiples para aumentar la seguridad, es menos probable que un fallo seguro del hardware provoque una parada errónea.

3.6.9 fallo dependiente: Fallo cuya probabilidad no se puede expresar como simple producto de las probabilidades no condicionadas de los eventos individuales que la han causado.

NOTA – Dos eventos A y B son dependientes únicamente si, siendo $P(z)$ la probabilidad del evento z:

$$P(\text{A y B}) > P(\text{A}) \times P(\text{B})$$

3.6.10 fallo de causa común: Fallo que es el resultado de uno o más eventos, que causan fallos coincidentes de dos o más canales separados en un sistema de canales múltiples, conduciendo al fallo del sistema.

3.6.11 error: Discrepancia entre un valor o una condición calculado, observado o medido y el valor o condición verdadero, especificado o teóricamente correcto.

NOTA – Adaptado del VEI 191-05-24 excluyendo las notas.

3.6.12 error humano: Acción humana o ausencia de intervención, que puede producir un resultado no deseado.

[ISO/CEI 2382-14-01-09]

NOTA – Adaptado del VEI 191-05-24 añadiendo el término “o ausencia de intervención”.

3.7 Actividades ligadas al ciclo de vida

3.7.1 ciclo de vida de seguridad: Actividades necesarias implicadas en la instalación de sistemas relacionados con la seguridad, que se presentan durante un periodo de tiempo que empieza en la fase de diseño conceptual de un proyecto y termina cuando todos los sistemas E/E/PE relacionados con la seguridad, o los sistemas relacionados con la seguridad de otra tecnología e instalaciones de reducción del riesgo externo ya no se encuentran disponibles para su utilización.

NOTA 1 – El término “ciclo de vida de seguridad funcional” es estrictamente más preciso, pero el adjetivo “funcional” no se considera necesario en este caso en el contexto de esta norma.

NOTA 2 – Los modelos de ciclo de vida de seguridad utilizados en esta norma se especifican en las figuras 2, 3 y 4 de la Norma CEI 61508-1.

3.7.2 ciclo de vida del software: Actividades que se desarrollan durante un periodo de tiempo que empieza en la fase de diseño conceptual del software y que termina cuando el software queda permanentemente fuera de uso.

NOTA 1 – Un ciclo de vida de un software incluye típicamente una fase de requisitos, una fase de desarrollo, una fase de ensayo, una fase de instalación y una fase de modificación.

NOTA 2 – El software no es capaz de ser mantenido, sino más bien es modificado.

3.7.3 gestión de la configuración: Disciplina de identificación de los componentes de un sistema en evolución que tiene por objeto controlar los cambios de estos componentes y mantener la continuidad y la trazabilidad a lo largo de todo el ciclo de vida.

NOTA – Para detalles sobre la gestión de la configuración del software, véase el apartado C.5.24 de la Norma CEI 61508-7.

3.7.4 análisis de impacto: Actividad de determinación del efecto que un cambio en una función o componente de un sistema tendrá sobre las otras funciones o componentes de dicho sistema, así como sobre los otros sistemas.

NOTA – En el contexto del software, véase el apartado C.5.23 de la Norma CEI 61508-7.

3.8 Confirmación de las medidas de seguridad

3.8.1 verificación: Confirmación por examen y aportación de pruebas objetivas de que los requisitos se han cumplido.

NOTA 1 – Adaptado de la Norma ISO 8402, excluyendo las notas.

NOTA 2 – En el contexto de esta norma, la verificación es la actividad que consiste en demostrar, para cada fase del ciclo de seguridad correspondiente (general, E/E/PES y software), por análisis y/o ensayos, que para las entradas específicas, las salidas entregadas satisfacen los objetivos y requisitos establecidos para cada fase específica.

EJEMPLO Las actividades de verificación incluyen:

- las revisiones relativas a las salidas de una fase (documentos de todas las fases del ciclo de vida de seguridad) para asegurar el cumplimiento de los objetivos y requisitos de la fase teniendo en cuenta las entradas específicas de dicha fase;
- las revisiones de diseño;
- los ensayos realizados en los productos diseñados para asegurar que funcionan de acuerdo con su especificación;
- los ensayos de integración realizados cuando se ensamblan las diferentes partes de un sistema en forma paso a paso y por ejecución de ensayos medioambientales a fin de asegurar que todas las partes trabajan juntas en la manera especificada.

3.8.2 validación: Confirmación, por examen y aportación de pruebas objetivas, de que se cumplen los requisitos particulares para un fin específico determinado.

NOTA 1 – Adaptado de la Norma ISO 8402, excluyendo las notas.

NOTA 2 – En esta norma, existen tres fases de validación:

- validación de seguridad general, (véase la figura 2 de la Norma CEI 61508-1);
- validación E/E/PE, (véase la figura 3 de la Norma CEI 61508-1);
- validación del software, (véase la figura 4 de la Norma CEI 61508-1).

NOTA 3 – La validación es la actividad de demostrar que el sistema relacionado con la seguridad que se considera, antes o después de la instalación, satisface todos los aspectos de la especificación de requisitos de seguridad para el sistema relacionado con la seguridad. Así, por ejemplo, la validación del software significa confirmar mediante examen y aportación de pruebas objetivas, que el software satisface la especificación de los requisitos de seguridad del software.

3.8.3 evaluación de la seguridad funcional: Investigación, basada en pruebas, para juzgar la seguridad funcional lograda por uno o más sistemas E/E/PE relacionados con la seguridad, sistemas relacionados con la seguridad basados en otras tecnologías o dispositivos externos de reducción de riesgo.

3.8.4 auditoría de la seguridad funcional: Examen sistemático e independiente destinado a determinar si los procedimientos específicos a los requisitos de seguridad funcional a cumplir con las disposiciones proyectadas se han aplicado efectivamente y si son adecuados para lograr los objetivos especificados.

NOTA – Se puede realizar una auditoría de la seguridad funcional como parte de una evaluación de la seguridad funcional.

3.8.5 ensayo periódico: Ensayo periódico realizado para detectar fallos de un sistema relacionado con la seguridad, de forma que, si es necesario, el sistema pueda restablecerse en una condición "como nuevo" o tan próxima a la misma como sea posible.

NOTA – La eficacia de un ensayo periódico depende de hasta que punto se restablece el sistema en una condición "como nuevo". Para que el ensayo periódico sea completamente eficaz, será necesario detectar el 100% de los fallos peligrosos. Aunque en la practica no sea fácil alcanzar el 100% para todo sistema que no sea un sistema E/E/PE relacionado con la seguridad de baja complejidad, conviene conservar este objetivo. Como mínimo, todas las funciones de seguridad que se ejecutan se comprueban de acuerdo con la especificación de requisitos de seguridad del sistema E/E/PES. Si se utilizan canales separados, estos ensayos se realizan por separado para cada uno de los canales.

3.8.6 cobertura del diagnóstico: Fracción que expresa la disminución de la probabilidad de fallos peligrosos del hardware que resultan del funcionamiento de ensayos de diagnóstico automáticos.

NOTA 1 – Se puede representar también la definición en términos de la siguiente ecuación, donde DC es la cobertura de diagnóstico, λ_{DD} es la probabilidad de fallos peligrosos detectados, y $\lambda_{D\ total}$ es la probabilidad de fallos peligrosos totales:

$$DC = \frac{\sum \lambda_{DD}}{\sum \lambda_{D\ total}}$$

NOTA 2 – La cobertura de diagnóstico puede existir para la totalidad de un sistema relacionado con la seguridad o partes del mismo. Puede existir, por ejemplo, cobertura del diagnóstico para los sensores y/o el sistema lógico y/o los elementos finales.

NOTA 3 – El término cobertura del diagnóstico segura, o cobertura del diagnóstico que incluye los fallos seguros, se usa para describir respectivamente la disminución funcional de la probabilidad de un fallo seguro de hardware, o tanto de un fallo seguro como de un fallo peligroso del hardware, que resulta del funcionamiento de los ensayos de diagnóstico automático.

3.8.7 intervalo entre ensayos de diagnóstico: Intervalo entre ensayos en línea para detectar las anomalías de un sistema relacionado con la seguridad que tienen una cobertura del diagnóstico especificada.

3.8.8 detectado; revelado; declarado: Se refiere al hardware y significa detectado por los ensayos de diagnóstico, los ensayos periódicos, la intervención del operador (por ejemplo inspección física y ensayos manuales), o en el curso del funcionamiento normal.

EJEMPLO Estos adjetivos se usan en los casos de anomalía detectada y de fallo detectado.

3.8.9 no detectado; no revelado; no declarado: Se refiere al hardware y significa no detectado por los ensayos de diagnóstico, los ensayos periódicos, la intervención del operador (por ejemplo inspección física y ensayos manuales), o en el curso del funcionamiento normal.

EJEMPLO Estos adjetivos se usan en los casos de anomalía no detectada y de fallo no detectado.

3.8.10 persona independiente: Persona que es separada y distinta de las implicadas en las actividades que tienen lugar durante la fase específica del ciclo de vida de seguridad general de los E/E/PES o del software, que se encarga de la evaluación de la seguridad funcional o de la validación y que no tiene responsabilidad directa en aquellas actividades.

3.8.11 departamento independiente: Departamento que es separado y distinto de los departamentos responsables de las actividades que tienen lugar durante la fase específica del ciclo de vida de seguridad general de los E/E/PES o del software, que se encarga de la evaluación de la seguridad funcional o de la validación.

3.8.12 organización independiente: Organización que es separada y distinta en cuanto a gestión y otros recursos de las organizaciones responsables de las actividades que tienen lugar durante la fase específica del ciclo de vida de seguridad general de los E/E/PES o del software, que se encarga de la seguridad funcional o de la validación.

3.8.13 animación: Operación simulada del sistema de software (o de una porción significativa de dicho sistema) destinada a presentar aspectos significativos del comportamiento del sistema, por ejemplo aplicados a una especificación de requisitos en un formato apropiado o en una representación apropiada de alto nivel del diseño del sistema.

NOTA – La animación puede dar una confianza suplementaria de que el sistema cumple los requisitos reales porque mejora el reconocimiento humano del comportamiento especificado.

3.8.14 ensayo dinámico: Ejecución del software y/o funcionamiento del hardware de manera controlada y sistemática de forma que demuestra la presencia del comportamiento requerido y la ausencia de un comportamiento no deseado.

NOTA – El ensayo dinámico difiere del análisis estático, que no exige la ejecución del software.

3.8.15 simulador de ensayo: Instalación que es capaz de simular (hasta un cierto grado de utilidad) el entorno de funcionamiento del software o del hardware en desarrollo, aplicando casos de ensayo al software y registrando la respuesta.

NOTA – El simulador de ensayo puede comprender también generadores de caso de ensayo e instalaciones para verificar los resultados de ensayo (bien automáticamente por comparación a valores considerados correctos, o bien por análisis manual).

ANEXO A (Informativo)

BIBLIOGRAFÍA

CEI 61131-3:1993 – *Autómatas programables. Parte 3: Lenguajes de programación.*

NOTA – Armonizada como Norma EN 61131-3:1993 (sin ninguna modificación).

CEI 61151:1992 – *Instrumentación nuclear. Amplificadores y preamplificadores utilizados con detectores de radiación ionizante. Procedimientos de ensayo.*

ISO/CEI 2382-1:1993 – *Tecnologías de la información. Vocabulario. Parte 1: Términos fundamentales.*

ISO 9000-3:1991 – *Gestión de la calidad y aseguramiento de la calidad. Parte 3: Directrices para la aplicación de la Norma ISO 9001 al desarrollo, suministro, instalación y mantenimiento de soporte lógico (software).*

NOTA – Armonizada como Norma EN 29000-3:1993 (sin ninguna modificación).

ANSI/ISA S84:1996 – *Aplicación de sistemas de seguridad con instrumentación en industrias de proceso.*

ÍNDICE ALFABÉTICO

ANEXO ZA (Normativo)

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

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

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

Norma Internacional	Fecha	Título	EN/HD	Fecha	Norma UNE correspondiente[1)]
CEI 60050-191	1990	Vocabulario Electrotécnico Internacional (VEI). Capítulo 191: Confiabilidad y calidad de servicio	–	–	UNE 21302-191:1992
CEI 60050-351	1975	Vocabulario Electrotécnico Internacional (VEI). Capítulo 351: Control automático	–	–	UNE 21302-351:1978
CEI 61508-1 + corr. mayo	1998 1999	Seguridad funcional de los sistemas eléctricos/electrónicos/electrónicos programables relacionados con la seguridad. Parte 1: Requisitos generales	EN 61508-1	2001	UNE-EN 61508-1:2003
CEI 61508-2	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 61508-3 + corr. abril	1998 1999	Seguridad funcional de los sistemas eléctricos/electrónicos/electrónicos programables relacionados con la seguridad. Parte 3: Requisitos del software (soporte lógico)	EN 61508-3	2001	UNE-EN 61508-3:2003
CEI 61508-5 + 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)]

(Continúa)

Norma Internacional	Fecha	Título	EN/HD	Fecha	Norma UNE correspondiente[1)]
CEI 61508-7	2000	Seguridad funcional de los sistemas eléctricos/electrónicos/electrónicos programables relacionados con la seguridad. Parte 7: Presentación de técnicas y medidas	EN 61508-7	2001	UNE-EN 61508-7[2)]
Guía CEI 104	1997	Elaboración de las publicaciones de seguridad y utilización de las publicaciones fundamentales de seguridad y de las publicaciones de grupos de seguridad	–	–	–
ISO/CEI 2382-14	1998	Tratamiento de la información. Vocabulario. Parte 14: Fiabilidad, mantenibilidad y disponibilidad	–	–	–
Guía ISO/CEI 51	1990	Directrices para incluir en las normas los aspectos relacionados con la seguridad	–	–	–
ISO 8402	1994	Gestión de la calidad y aseguramiento de la calidad. Vocabulario	EN ISO 8402	1998	UNE-EN ISO 8402:1995

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

ANEXO NACIONAL (Informativo)

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

Norma internacional	Norma UNE
CEI 61131-3:1993	UNE-EN 61131-3:1997

AENOR Asociación Española de Normalización y Certificación

Dirección C Génova, 6
28004 MADRID-España

Teléfono 91 432 60 00

Fax 91 310 40 32