NORMA CUBANA

NC

IEC 61511-1: 2012
(Publicada por la IEC en el 2003)

SEGURIDAD FUNCIONAL — SISTEMAS INSTRUMENTADOS DE SEGURIDAD PARA EL SECTOR DE LAS INDUSTRIAS DE PROCESOS — PARTE 1: MARCO, DEFINICIONES, REQUISITOS, SISTEMAS, EL HARDWARE Y EL SOFWARE. (IEC 61511-1: 2003 + Corr. 2004, IDT)

Functional safety — Safety instrumented systems for the process industry sector — Part 1: Frameworks, definitions, system, hardware and software requirements.

ICS: 13.110; 25.040.01

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 del 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 61511-1: 2003 *Functional safety — Safety instrumented systems for the process industry sector — Part 1: Frameworks, definitions, system, hardware and software requirements* que a su vez adopta de forma idéntica a la Norma Internacional IEC 61511-1: 2003 + Corr. 2004) 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 61511-1

Diciembre 2004

ICS 13.110; 25.040.01

Versión en español

Seguridad funcional
Sistemas instrumentados de seguridad para el sector de las industrias de procesos
Parte 1: Marco, definiciones, requisitos para el sistema, el hardware y el software
(IEC 61511-1:2003 + corrigendum 2004)

Functional safety. Safety instrumented systems for the process industry sector. Part 1: Framework, definitions, system, hardware and software requirements. (IEC 61511-1:2003 + corrigendum 2004).

Sécurité fonctionnelle. Systèmes instrumentés de sécurité pour le secteur des industries de transformation. Partie 1: Cadre, définitions, exigences pour le système, le matériel et le logiciel. (CEI 61511-1:2003 + corrigendum 2004).

Funktionale Sicherheit. Sicherheitstechnische Systeme für die Prozessindustrie. Teil 1: Allgemeines, Begriffe, Anforderungen an Systeme, Software und Hardware. (IEC 61511-1:2003 + Corrigendum 2004).

Esta norma europea ha sido aprobada por CENELEC el 2004-10-01. 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, Chipre, Dinamarca, Eslovaquia, Eslovenia, España, Estonia, Finlandia, Francia, Grecia, Hungría, Irlanda, Islandia, Italia, Letonia, Lituania, Luxemburgo, Malta, Noruega, Países Bajos, Polonia, 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

PRÓLOGO

El texto de la Norma Internacional IEC 61511-1:2003, preparado por el Subcomité SC 65A, *Aspectos de sistemas*, del Comité Técnico TC 65, *Control y medida en procesos industriales*, de IEC, fue sometido al Procedimiento de Aceptación Única (UAP) y fue aprobado por CENELEC como Norma Europea EN 61511-1 el 2004-10-01 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)	2005-10-01
– Fecha límite en la que deben retirarse las normas nacionales divergentes con esta norma	(dow)	2007-10-01

El anexo ZA ha sido añadido por CENELEC.

DECLARACIÓN

El texto de la Norma Internacional IEC 61511-1:2003 + corrigendum noviembre de 2004 fue aprobado por CENELEC como norma europea sin ninguna modificación.

ÍNDICE

Página

COMISIÓN ELECTROTÉCNICA INTERNACIONAL

Seguridad funcional
Sistemas instrumentados de seguridad para el sector de las industrias de procesos
Parte 1: Marco, definiciones, requisitos para el sistema, el hardware y el software

PRÓLOGO

1) IEC (Comisión Electrotécnica Internacional) es una organización mundial para la normalización, que comprende todos los comités electrotécnicos nacionales (Comités Nacionales de IEC). El objetivo de IEC es promover la cooperación internacional sobre todas las cuestiones relativas a la normalización en los campos eléctrico y electrónico. Para este fin y también para otras actividades, IEC publica Normas Internacionales, Especificaciones Técnicas, Informes Técnicos, Especificaciones Disponibles al Público (PAS) y Guías (de aquí en adelante "Publicaciones IEC"). Su elaboración se confía a los comités técnicos; cualquier Comité Nacional de IEC que esté interesado en el tema objeto de la norma puede participar en su elaboración. Organizaciones internacionales gubernamentales y no gubernamentales relacionadas con IEC también participan en la elaboración. IEC colabora estrechamente con la Organización Internacional de Normalización (ISO), de acuerdo con las condiciones determinadas por acuerdo entre ambas.

2) Las decisiones formales o acuerdos de IEC sobre materias técnicas, expresan en la medida de lo posible, un consenso internacional de opinión sobre los temas relativos a cada comité técnico en los que existe representación de todos los Comités Nacionales interesados.

3) Los documentos producidos tienen la forma de recomendaciones para uso internacional y se aceptan en este sentido por los Comités Nacionales mientras se hacen todos los esfuerzos razonables para asegurar que el contenido técnico de las publicaciones IEC es preciso, IEC no puede ser responsable de la manera en que se usan o de cualquier mal interpretación por parte del usuario.

4) Con el fin de promover la unificación internacional, los Comités Nacionales de IEC se comprometen a aplicar de forma transparente las Publicaciones IEC, en la medida de lo posible en sus publicaciones nacionales y regionales. Cualquier divergencia entre la Publicación IEC y la correspondiente publicación nacional o regional debe indicarse de forma clara en esta última.

5) IEC no establece ningún procedimiento de marcado para indicar su aprobación y no se le puede hacer responsable de cualquier equipo declarado conforme con una de sus publicaciones.

6) Todos los usuarios deberían asegurarse de que tienen la última edición de esta publicación.

7) No se debe adjudicar responsabilidad a IEC o sus directores, empleados, auxiliares o agentes, incluyendo expertos individuales y miembros de sus comités técnicos y comités nacionales de IEC por cualquier daño personal, daño a la propiedad u otro daño de cualquier naturaleza, directo o indirecto, o por costes (incluyendo costes legales) y gastos derivados de la publicación, uso o confianza de esta publicación IEC o cualquier otra publicación IEC.

8) Se debe prestar atención a las normas para consulta citadas en esta publicación. La utilización de las publicaciones referenciadas es indispensable para la correcta aplicación de esta publicación.

9) Se debe prestar atención a la posibilidad de que algunos de los elementos de esta Publicación IEC puedan ser objeto de derechos de patente. No se podrá hacer responsable a IEC de identificar alguno o todos esos derechos de patente.

La Norma Internacional IEC 61511-1 ha sido elaborada por el subcomité 65A: Aspectos de sistemas, del comité técnico 65 de IEC: Control y medida en procesos industriales.

Esta versión bilingüe (2003-12) sustituye a la versión inglesa.

El texto de esta norma se basa en los documentos siguientes:

FDIS	Informe de voto
64A/368/FDIS	65A/372/RVD

El informe de voto indicado en la tabla anterior ofrece toda la información sobre la votación para la aprobación de esta norma.

La versión francesa de esta norma no ha sido votada.

Esta norma ha sido elaborada de acuerdo con las Directivas ISO/IEC, Parte 2.

La Norma IEC 61511 consta de las siguientes partes, bajo el título general *Seguridad funcional: Sistemas instrumentados de seguridad para el sector de las industrias de procesos* (véase la figura 1):

Parte 1: Marco, definiciones, requisitos para el sistema, el hardware y el software.

Parte 2: Directrices para la aplicación de la Norma IEC 61511-1.

Parte 3: Guía para la determinación de los niveles requeridos de integridad de seguridad.

El comité ha decidido que el contenido de esta norma permanezca vigente hasta 2007. En esa fecha, la norma será

– confirmada;

– anulada;

– reemplazada por una edición revisada; o

– modificada.

El contenido del corrigendum de noviembre de 2004 se ha incluido en esta edición.

INTRODUCCIÓN

Los sistemas instrumentados de seguridad se han usado durante muchos años para realizar funciones instrumentadas de seguridad en las industrias de procesos. Si la instrumentación se tiene que usar en forma efectiva para las funciones instrumentadas de seguridad, es esencial que esta instrumentación cumpla ciertas normas y niveles de características de funcionamiento mínimos.

Esta norma trata la aplicación de los sistemas instrumentados de seguridad a las industrias de procesos. También requiere la realización de una evaluación de los peligros y riesgos de los procesos para permitir deducir la especificación de los sistemas instrumentados de seguridad. Otros sistemas de seguridad no se consideran más que en la medida en que se pueda tener en cuenta su contribución cuando se consideran los requisitos de características de funcionamiento para los sistemas instrumentados de seguridad. El sistema instrumentado de seguridad incluye todos los componentes y subsistemas necesarios para realizar la función instrumentada de seguridad desde el sensor o sensores hasta el(los) elementos final(es).

Esta norma tiene dos conceptos que son fundamentales en su aplicación; el ciclo de vida de seguridad y los niveles de integridad de seguridad.

Esta norma trata los sistemas instrumentados de seguridad que están basados en el uso de la tecnología eléctrica/electrónica/programable. En los casos en los que se usan otras tecnologías para las unidades lógicas, se deberían aplicar los principios básicos de esta norma. También trata esta norma los sensores de sistemas instrumentados de seguridad y los elementos finales con independencia de la tecnología utilizada. Esta norma es específica de la industria de procesos dentro del marco de la Norma IEC 61508 (véase anexo A).

Esta norma establece un enfoque de las actividades del ciclo de vida de seguridad para cumplir estas normas mínimas. Se ha adoptado este enfoque a fin de usar una política técnica racional y coherente.

En la mayoría de las situaciones, se alcanza mejor la seguridad mediante un diseño de procesos de seguridad inherentes. Si fuera necesario, se puede combinar esto con un sistema o sistemas protectores para tratar cualquier riesgo identificado residual. Los sistemas de seguridad pueden apoyarse en tecnologías diferentes (química, mecánica, hidráulica, neumática, eléctrica, electrónica, electrónica programable). Para facilitar este enfoque, esta norma:

- requiere la realización de una evaluación de los peligros y riesgos para permitir identificar los requisitos generales de seguridad;
- requiere que se efectúe una asignación de los requisitos de seguridad al sistema o sistemas instrumentados de seguridad;
- trabaja dentro de un marco que es aplicable a todos los métodos instrumentados para alcanzar la seguridad funcional;
- detalla el uso de determinadas actividades, tales como la gestión de seguridad, que pueden ser aplicables a todos los métodos de alcanzar la seguridad funcional.

Esta norma sobre los sistemas instrumentados de seguridad para las industrias de procesos

- trata todas las fases del ciclo de vida de seguridad desde el concepto inicial, diseño, realización, funcionamiento y mantenimiento hasta la retirada del servicio;
- permite que se armonicen las normas específicas de cada país relativas a industrias de procesos existentes o nuevas con esta norma.

Esta norma internacional está destinada a conducir a un alto nivel de coherencia (por ejemplo, de principios subyacentes, terminología, información) dentro de las industrias de procesos. Esto debería producir beneficios tanto de seguridad como económicos.

En jurisdicciones en las que las autoridades gobernantes (por ejemplo, nacionales, federales, estaduales, provinciales, de condado, municipales) hayan establecido requisitos relativos al diseño de seguridad de procesos, diseño de seguridad, gestión de seguridad de procesos u otros, éstos prevalecerán sobre los requisitos definidos en esta norma.

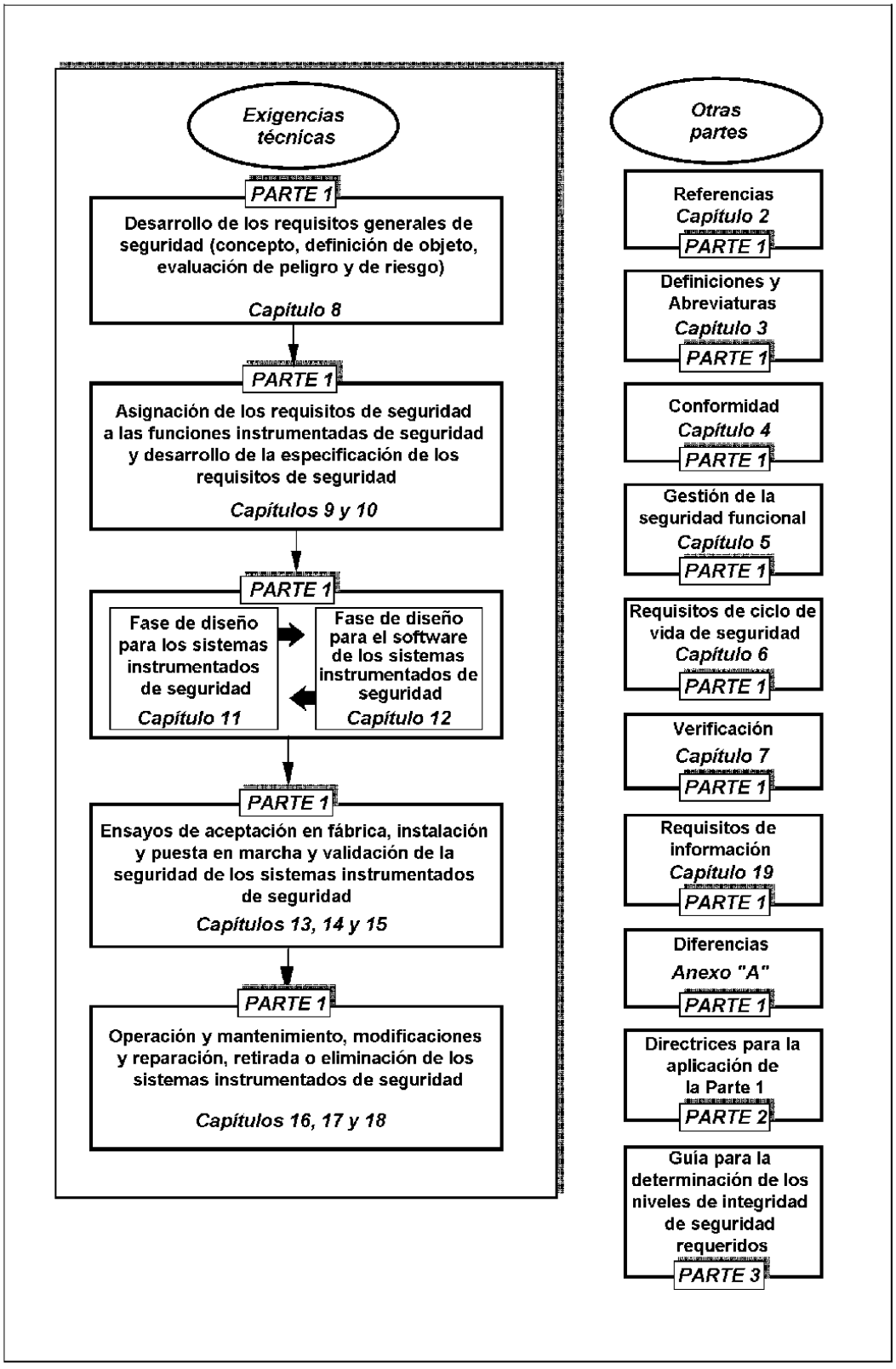


Fig. 1 – Cuadro general de esta norma

Seguridad funcional
Sistemas instrumentados de seguridad para el sector de las industrias de procesos
Parte 1: Marco, definiciones, requisitos para el sistema, el hardware y el software

1 OBJETO Y CAMPO DE APLICACIÓN

Esta norma internacional establece los requisitos para la especificación, diseño, instalación, funcionamiento y mantenimiento de un sistema de seguridad, de manera que se le pueda encomendar con toda confianza el establecimiento y/o el mantenimiento del proceso en una condición segura. Esta norma ha sido realizada como una aplicación al sector de las industrias de procesos de la Norma IEC 61508.

En particular, esta norma:

a) especifica los requisitos para lograr la seguridad funcional, pero no especifica quien es responsable de implantar los requisitos (por ejemplo, diseñadores, suministradores, propietario/empresa operadora, contratista); esta responsabilidad será asignada a las diferentes partes según la planificación de la seguridad y las reglamentaciones nacionales;

b) se aplica cuando un equipo que satisface los requisitos de la Norma IEC 61508, o del apartado 11.5 de la Norma IEC 61511-1 está integrado en un sistema general que se va a usar en una aplicación del sector de procesos, pero no es aplicable a los fabricantes que deseen reivindicar que los dispositivos son adecuados para sus uso en sistemas instrumentados de seguridad para el sector de procesos (véanse las Normas IEC 61508-2 y IEC 61508-3);

c) define la relación entre las Normas IEC 61511 y IEC 61508 (véanse figuras 2 y 3);

d) es aplicable cuando se ha desarrollado un software de aplicación para sistemas que tienen programas con una variabilidad limitada o fijos, pero no es aplicable a los fabricantes, diseñadores de sistemas instrumentados de seguridad, integradores y usuarios que desarrollan sistemas de software integrado (software de sistema) o usan lenguajes de variabilidad plena (véase la Norma IEC 61508-3);

e) es aplicable a una amplia variedad de industrias dentro del sector de procesos que incluye las de productos químicos, refino de petróleo, producción de petróleo y gas, pasta y papel, generación eléctrica no nuclear, etc.;

NOTA – Dentro del sector de procesos, algunas aplicaciones, (por ejemplo, de tipo "costero" o "en el mar"), pueden tener requisitos adicionales a satisfacer.

f) define la relación entre las funciones instrumentadas de seguridad y otras funciones (figura 4);

g) da lugar a la identificación de los requisitos funcionales y los requisitos de integridad de seguridad para la(s) función(es) instrumentadas de seguridad(s) tomando en cuenta la reducción de riesgo lograda por otros medios;

h) especifica los requisitos para la arquitectura del sistema y la configuración de su hardware, software de aplicación e integración del sistema;

i) especifica los requisitos para el software de aplicación para usuarios e integradores de sistemas instrumentados de seguridad (capítulo 12). En particular, se especifican los requisitos para los siguientes aspectos:

- las fases del ciclo de vida y actividades que hay que aplicar durante el diseño y desarrollo del software de aplicación (modelo del ciclo de vida de seguridad del software). Estos requisitos incluyen la aplicación de medidas y técnicas que están destinadas a evitar fallos del software y a controlar los fallos que pudieran producirse;

- la información relativa a la validación de la seguridad del software a efectuar por parte de los organismos que realicen la integración del SIS;

- la preparación de la información y procedimientos relativos al software que necesita el usuario para el funcionamiento y mantenimiento del SIS;

- los procedimientos y las especificaciones a satisfacer por el organismo que realice modificaciones del software de seguridad;

j) es aplicable cuando se alcanza la seguridad funcional usando una o más funciones instrumentadas de seguridad para la protección del personal, protección del público en general o protección del medio ambiente;

k) se puede usar en aplicaciones no de seguridad, tales como la protección de bienes;

l) define requisitos para aplicar funciones instrumentados de seguridad como parte de las disposiciones generales para alcanzar la seguridad funcional;

m) usa un ciclo de vida de seguridad (figura 8) y define una lista de actividades que son necesarias para determinar los requisitos funcionales y los requisitos de integridad de seguridad para los sistemas instrumentados de seguridad;

n) exige la realización de una evaluación de peligro y de riesgo para definir los requisitos de seguridad funcional y los niveles de integridad de seguridad de cada función instrumentadas de seguridad;

NOTA – Véase la figura 9 para tener una visión de conjunto de los métodos de reducción de riesgo.

o) establece objetivos numéricos para la probabilidad media de fallo en caso de demanda y la frecuencia de los fallos peligrosos por hora para los niveles de integridad de seguridad;

p) especifica los requisitos mínimos para las tolerancias de defectos de hardware;

q) especifica las técnicas/medidas necesarias para alcanzar los niveles de seguridad especificados;

r) define un nivel máximo de características de funcionamiento (SIL 4) que se puede alcanzar para una función instrumentada de seguridad realizada según esta norma;

s) define un nivel mínimo de características de funcionamiento (SIL 1) por debajo del cual esta norma no se aplica;

t) proporciona un marco para el establecimiento de niveles de integridad de seguridad pero no especifica los niveles de integridad de seguridad requeridos para aplicaciones específicas (que se deberían establecer en base al conocimiento de la aplicación concreta);

u) especifica los requisitos para todas las partes del sistema instrumentado de seguridad, desde el sensor hasta el(los) elemento(s) final(es);

v) define la información que se necesita durante el ciclo de vida de seguridad;

w) requiere que el diseño de una función instrumentada de seguridad tenga en cuenta los factores humanos;

x) no establece ningún requisito directo respecto al operador o personal de mantenimiento.

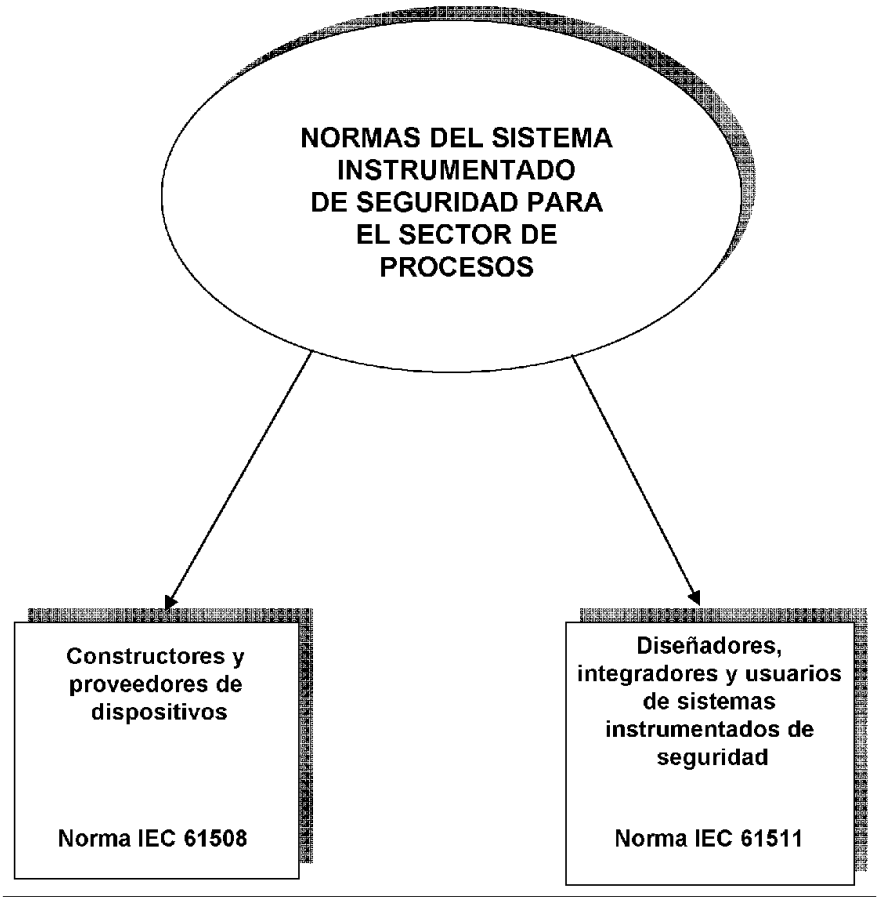


Fig. 2 – Relación entre las Normas IEC 61511 y IEC 61508

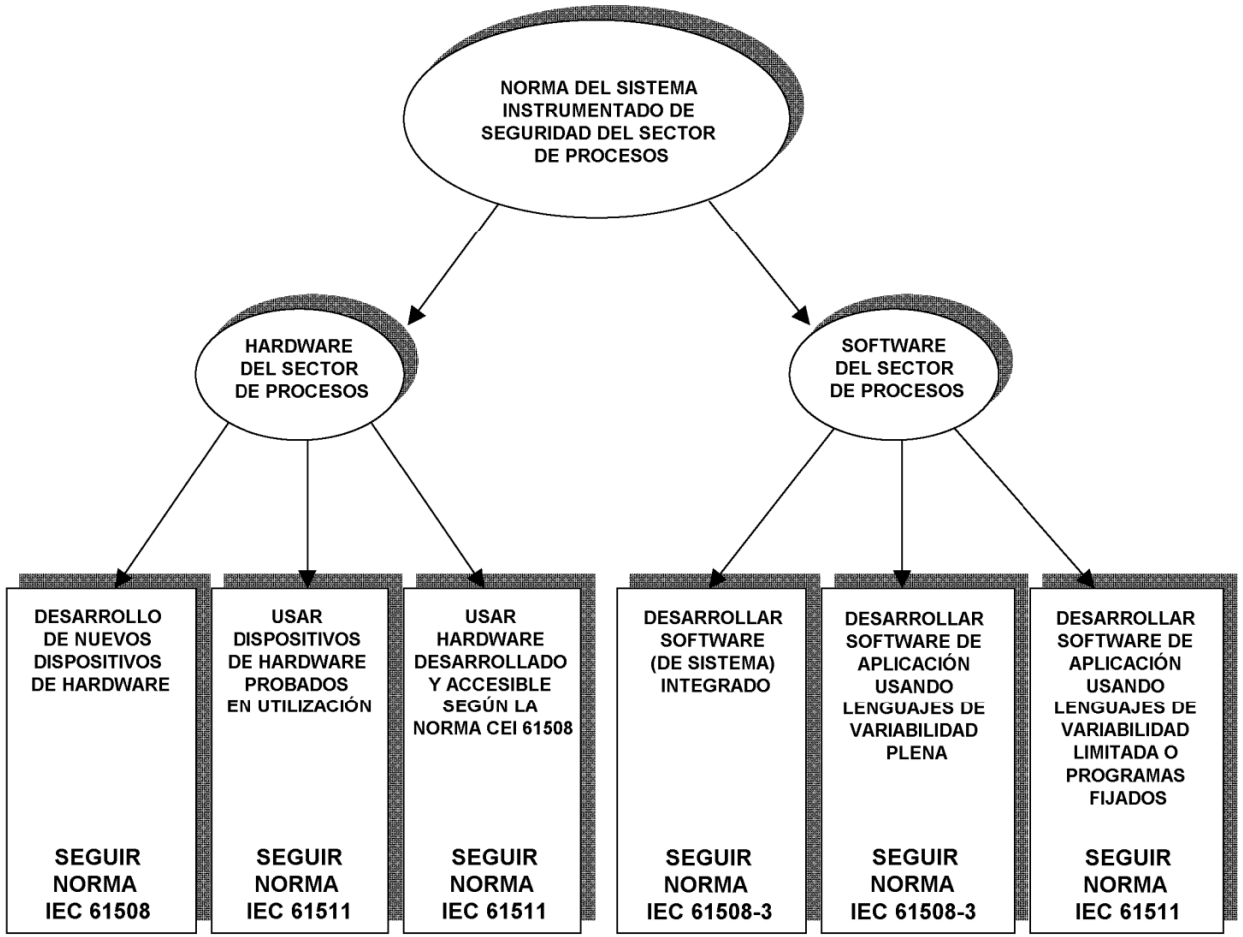


Fig. 3 – Relación entre las Normas IEC 61511 y IEC 61508 (véase capítulo 1)

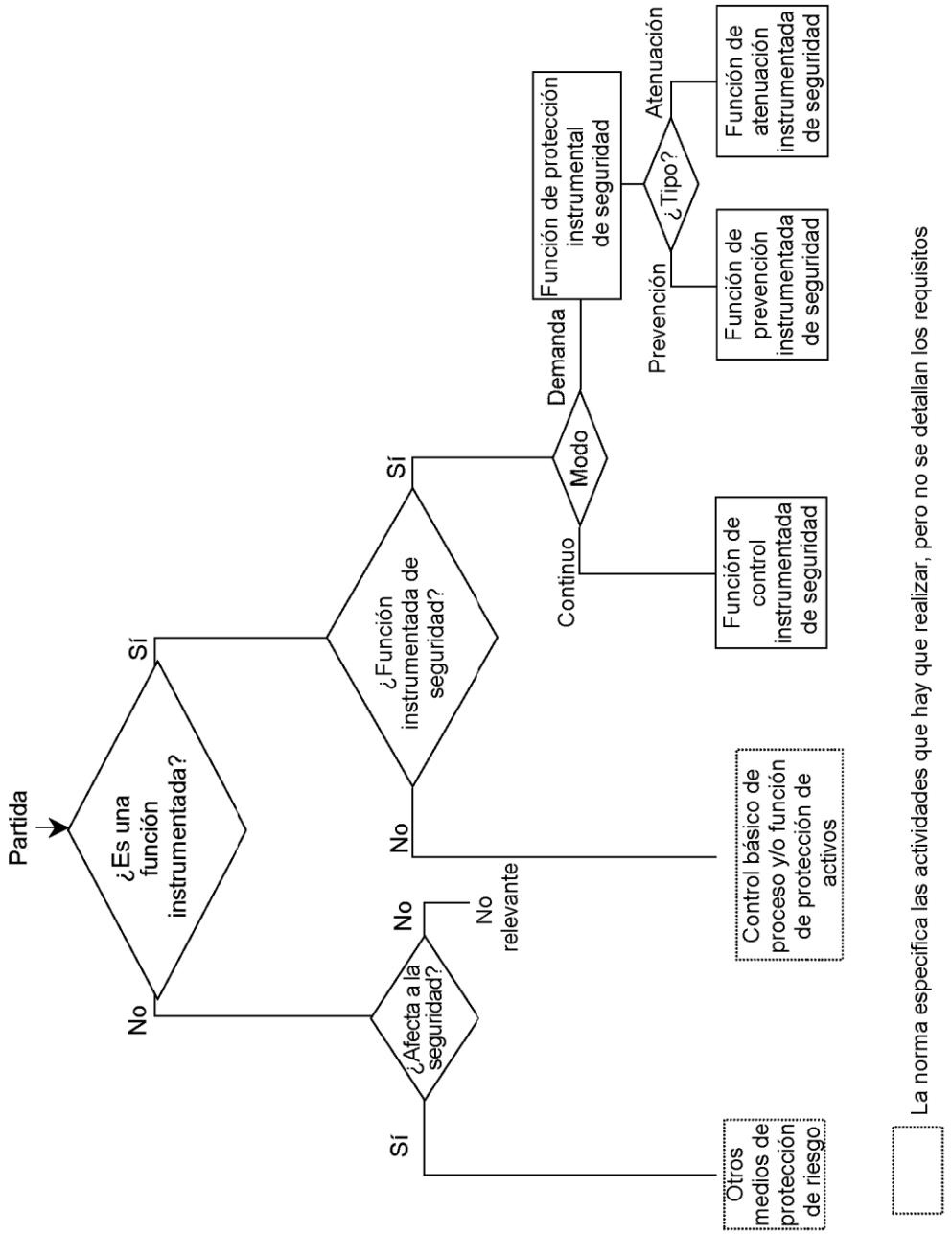


Fig. 4 – Relación entre las funciones instrumentadas de seguridad y otras funciones

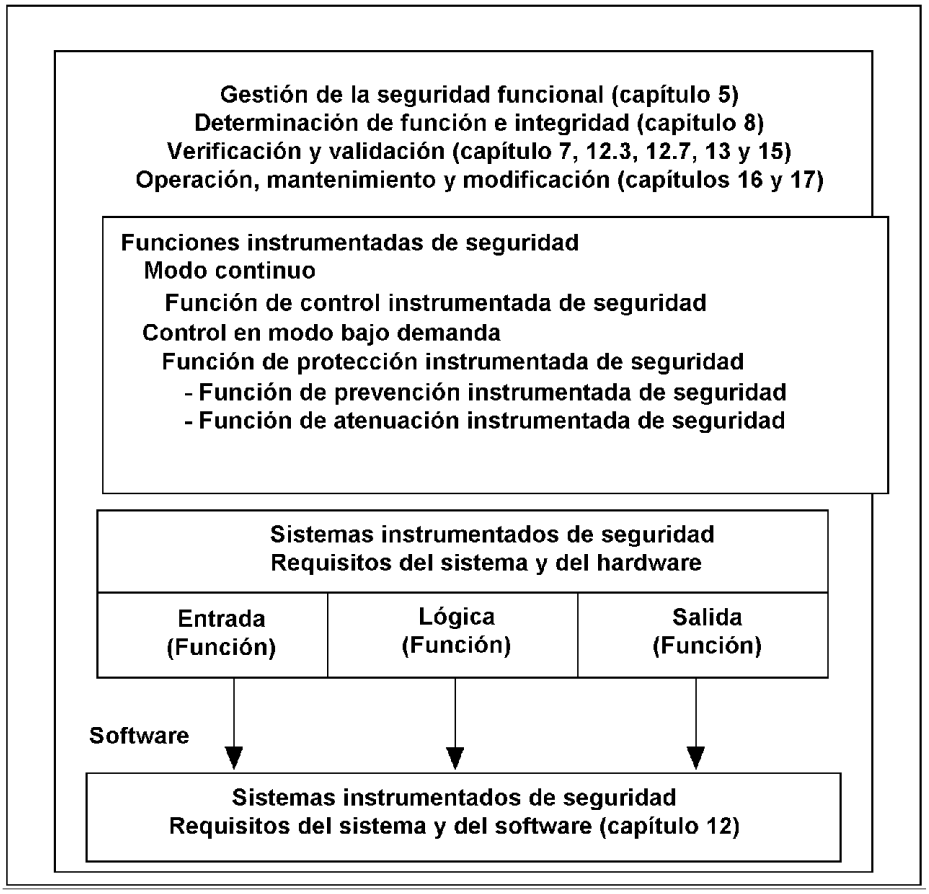


Fig. 5 – Relación entre el sistema, el hardware y el software en la Norma IEC 61511-1

2 NORMAS PARA CONSULTA

Las normas que a continuación se indican son indispensables para la aplicación de esta norma. Para las referencias con fecha, sólo se aplica la edición citada. Para las referencias sin fecha se aplica la última edición de la norma (incluyendo cualquier modificación de ésta).

IEC 60654-1:1993 – *Condiciones de funcionamiento* de los equipos de medida y control de los procesos industriales. Parte 1: Condiciones climáticas.

IEC 60654-3:1998 – *Condiciones de funcionamiento de los equipos de medida y control de los procesos industriales. Parte 3: Influencias mecánicas.*

IEC 61326-1 – *Material eléctrico para medida, control y uso en laboratorio. Requisitos de compatibilidad electromagnética (CEM). Parte 1: Requisitos generales.*

IEC 61508-2 – *Seguridad funcional de los sistemas eléctricos/electrónicos/electrónicos programables relacionados con la seguridad. Parte 2: Requisitos para los sistemas eléctricos/electrónicos/electrónicos programables relacionados con la seguridad.*

IEC 61508-3 – *Seguridad funcional de los sistemas eléctricos/electrónicos/electrónicos programables relacionados con la seguridad. Parte 3: Requisitos del software (soporte lógico).*

IEC 61511-2 – *Seguridad funcional. Sistemas instrumentados de seguridad para el sector de las industrias transformadoras. Parte 2. Directrices para la aplicación de la Norma IEC 61511-1.*

3 ABREVIATURAS Y DEFINICIONES

3.1 Abreviaturas

En la tabla 1 se dan las abreviaturas usadas en toda la Norma IEC 61511.

Tabla 1
Abreviaturas usadas en la Norma IEC 61511

Abreviatura	Expresión completa
ALARP	Tan bajo como sea razonablemente posible
ANSI	Instituto de Normalización Nacional de los EEUU
BPCS	Sistema básico de control de proceso
c.a./c.c.	Corriente alterna/corriente continua
CEM	Compatibilidad electromagnética
DC	Cobertura del diagnóstico
E/E/PE	Eléctrico/Electrónico/Electrónico programable
E/E/PES	Sistema eléctrico/electrónico/electrónico programable
FAT	Ensayos de aceptación en fábrica
FPL	Lenguaje de programa fijado
FTA	Análisis por árbol de defectos
FVL	Lenguaje de variabilidad plena
HFT	Tolerancia a los defectos del hardware

HMI	Interfaz hombre máquina
H&RA	Evaluación de peligro y de riesgo
HRA	Análisis de fiabilidad humana
H/W	Hardware
IEC	Comisión Electrotécnica Internacional
IEV (VEI)	Vocabulario Electrotécnico Internacional (VEI)
ISA	Sociedad de Instrumentación, Sistemas y Automatización
ISO	Organización Internacional de Normalización
LVL	Lenguaje de variabilidad limitada
MooN	"M" canales entre "N" (véase el apartado 3.2.45)
NP	No programable
PE	Electrónica programable
PES	Sistema electrónico programable
PFD	Probabilidad de fallo en demanda
PFD_{avg}	Probabilidad media de fallo en demanda
PLC	Controlador lógico programable (autómata programable)
SAT	Ensayo de aceptación en el sitio
SFF	Proporción de fallos seguros
SIF	Función instrumentada de seguridad
SIL	Nivel de integridad de seguridad
SIS	Sistema instrumentado de seguridad
SRS	Especificación de requisitos de seguridad
S/W	Software

3.2.4 canal: Elemento o grupo de elementos que realiza(n) independientemente una función.

NOTA 1 – Los elementos dentro de un canal podrían incluir módulos de entrada/salida (I/O), sistemas lógicos (véase apartado 3.2.40), sensores, elementos finales.

NOTA 2 – Una configuración de canal doble (es decir, con dos canales) es aquella con dos canales que realizan independientemente la misma función.

NOTA 3 – Se puede usar el término para describir un sistema completo o una parte de un sistema (por ejemplo, sensores o elementos finales).

3.2.5 codificación: Véase "programación".

3.2.6

3.2.6.1 fallo de causa común: Fallo que es el resultado de uno o más acontecimientos, que causan fallos de dos o más canales separados en un sistema de canales múltiples, dando lugar al fallo del sistema.

3.2.6.2 fallo de modo común: Fallo de dos o más canales del mismo modo, que causan el mismo resultado erróneo.

3.2.7 componente: Una de las partes de un sistema, subsistema o dispositivo que realiza una función específica.

3.2.8 configuración: Véase "arquitectura".

3.2.9 gestión de la configuración: Disciplina de identificar los componentes de un sistema en evolución (hardware y software) para los fines de controlar los cambios de esos componentes y de mantener la continuidad y trazabilidad a través de todo el ciclo de vida.

3.2.10 sistema de control: Sistema que responde a señales de entrada del proceso y/o del operador y genera señales de salida que causan que el proceso funcione de la manera deseada.

NOTA – El sistema de control incluye dispositivos de entrada y elementos finales y puede ser un BPCS o un SIS o una combinación de ambos.

3.2.11 fallo peligroso: Fallo que tiene el potencial de poner el sistema instrumentado de seguridad en un estado peligroso o en la imposibilidad de ejecutar su función.

NOTA – El hecho de que el potencial se realice o no puede depender de la arquitectura de canales del sistema. En sistemas con canales múltiples para mejorar la seguridad, es menos probable un fallo peligroso que conduzca a un estado general de fallo o de imposibilidad de ejecutar su función.

3.2.12 fallo dependiente: Fallo cuya probabilidad no se puede expresar como el producto simple de las probabilidades incondicionales de los acontecimientos que lo causaron.

NOTA 1 – Dos acontecimientos A y B son dependientes, siendo $P(z)$ la probabilidad del acontecimiento *z,* sólo si $P(\text{A y B}) > P(\text{A}) \times P(\text{B})$.

NOTA 2 – Véase el apartado 9.5 como ejemplo de consideración de fallo dependiente entre capas de protección.

NOTA 3 – El fallo dependiente incluye la causa común (véase apartado 3.2.6).

3.2.13 detectado; revelado; declarado: En relación a fallos de hardware o a fallos de software, detectados por los ensayos de diagnóstico o a lo largo del funcionamiento normal.

3.2.14 dispositivo: Unidad funcional de hardware o de software, o de ambos, capaz de cumplir una finalidad especificada (por ejemplo, dispositivos de campo, equipo conectado al lado de campo de los bornes I/O del SIS: este equipo incluye cableado de campo, sensores, elementos finales, unidades lógicas y aquellos dispositivos de interfaz de operador conectados por hilos a los bornes I/O del SIS).

3.2.15 cobertura del diagnóstico (DC): Relación de la tasa de fallos detectados a la tasa de fallos total del componente o subsistema tal como se ha detectado en los ensayos de diagnóstico. La cobertura del diagnóstico no incluye ninguno de los defectos detectados por los ensayos periódicos.

NOTA 1 – La cobertura de diagnóstico se usa para calcular las tasas de fallos detectados (λ_D) y no detectados (λ_N) a partir de la tasa de fallos totales (λ_T) de la manera siguiente: $\lambda_D = DC \times \lambda_T$ y $\lambda_N = (1 - DC) \times \lambda_T$.

NOTA 2 – La cobertura del diagnóstico se aplica a los componentes o a los subsistemas de un sistema instrumentado de seguridad. Por ejemplo, la cobertura del diagnóstico se determina típicamente para un sensor, elemento final o unidad lógica.

NOTA 3 – Para aplicaciones de seguridad, la cobertura del diagnóstico se aplica típicamente a los fallos seguros y peligrosos de un componente o subsistema. Por ejemplo, la cobertura del diagnóstico para los fallos peligrosos de un componente o subsistema es $DC = \lambda_{DD} / \lambda_{DT}$, donde λ_{DD} es la tasa de fallos peligrosos detectada y λ_{DT} es la tasa de fallos peligrosos total.

3.2.16 diversidad: Existencia de diferentes medios para realizar una función requerida.

NOTA – Se puede lograr la diversidad por diferentes métodos físicos o diferentes enfoques de diseño.

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

NOTA – El término pretende cubrir el conjunto de los dispositivos o sistemas que funcionan en base a principios eléctricos y que incluirían:

- dispositivos electromecánicos (eléctricos);
- dispositivos electrónicos de estado sólido no programables (electrónicos);
- dispositivos electrónicos basados en la tecnología informática (electrónicos programables) (véase apartado 3.2.55).

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

NOTA – Adaptada de VEI 191-05-24, excluyendo las notas.

3.2.19 instalaciones externas de reducción de riesgo: Medidas para reducir o mitigar los riesgos, que son separadas y distintas del SIS.

NOTA 1 – Los ejemplos incluyen un sistema de drenaje, cortafuegos, un muro (dique).

NOTA 2 – El término se desvía de la definición dada por la Norma IEC 61508-4 para reflejar las diferencias de la terminología del sector de procesos.

3.2.20 fallos: Terminación de la capacidad de una unidad funcional para realizar una función requerida.

NOTA 1 – Esta definición, excluyendo estas notas, corresponde con la de la Norma ISO/IEC 2382-14-01-09:1997.

NOTA 2 – Para más información, véase la Norma IEC 61508-4.

NOTA 3 – La realización de las funciones requeridas excluye necesariamente determinados comportamientos, y algunas funciones pueden ser especificadas en términos de los comportamientos a evitar. Si se produce un comportamiento de este tipo, se tiene un fallo.

NOTA 4 – Los fallos son aleatorios o sistemáticos (véanse los apartados 3.2.62 y 3.2.85).

3.2.21 defecto: Condición anormal que puede causar una reducción en la capacidad de una unidad funcional para realizar una función requerida o la pérdida de la misma.

NOTA – El VEI 191.06-01 define “defecto” como la incapacidad de realizar una función requerida, excluyendo la incapacidad durante el mantenimiento preventivo u otras acciones planificadas, o debida a la falta de recursos externos. [ISO/IEC 2382-14-01-09]

3.2.22 evitación de defectos: Uso de técnicas o procedimientos tendentes a evitar la introducción de defectos durante cualquier fase del ciclo de seguridad del sistema instrumentado de seguridad.

3.2.23 tolerancia de defectos: Capacidad de una unidad funcional para continuar desarrollando una función requerida en presencia de defectos o errores.

NOTA – La definición VEI 191-15-05 se refiere sólo al subtérmino defectos. Véase la nota sobre el término defecto en el apartado 3.2.21.

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

3.2.24 elemento final: Parte de un sistema instrumentado de seguridad que realiza la acción física necesaria para lograr un estado seguro.

NOTA – Son ejemplos las válvulas, aparamenta, motores, incluyendo sus elementos auxiliares, por ejemplo, una válvula solenoide y un actuador si están implicados en la función instrumentada de seguridad.

3.2.25 seguridad funcional: Parte de la seguridad general relativa al proceso y al BPCS que depende del funcionamiento correcto del SIS y de otras capas de protección.

NOTA – El término se desvía de la definición dada por la Norma IEC 61508-4 para reflejar las diferencias de la terminología del sector de procesos.

3.2.26 evaluación de la seguridad funcional: Investigación, basada en pruebas, de la seguridad funcional alcanzada por una o más capas de protección.

NOTA – El término se desvía de la definición dada por la Norma IEC 61508-4 para reflejar las diferencias de la terminología del sector de procesos.

3.2.27 auditoría de la seguridad funcional: Examen sistemático e independiente para determinar si los procedimientos específicos de los requisitos de seguridad funcional cumplen con las disposiciones planificadas, se realizan efectivamente y son adecuados para lograr los objetivos específicos.

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

3.2.28 unidad funcional: Entidad de hardware o de software, o ambos, capaz de cumplir una finalidad especificada.

NOTA 1 – En VEI 191-01-01, se usa el término más general “elemento” en lugar de unidad funcional. Un elemento puede incluir a veces personas.

NOTA 2 – Esta es la definición dada en la Norma ISO/IEC 2382-14-01-01.

3.2.29 integridad de seguridad de hardware: Parte de la integridad de seguridad o de la función de seguridad instrumentada que se refiere a los fallos aleatorios del hardware en un modo peligroso de fallo.

NOTA 1 – El término se refiere a fallos en un modo peligroso. Es decir, aquellos fallos de una función instrumentada de seguridad que perjudicarían la integridad de la seguridad. Los dos parámetros que son relevantes en este contexto son la tasa de fallos peligrosos general y la probabilidad de fallo para funcionar bajo demanda.

NOTA 2 – Véase el apartado 3.2.86.

NOTA 3 – Este término se desvía de la definición dada por la Norma IEC 61508-4 para reflejar las diferencias de la terminología del sector de procesos.

3.2.30 daño: Heridas físicas o daños a la salud de las personas, bien directamente o indirectamente, como consecuencia de daños a la propiedad o al medio ambiente.

NOTA – Esta definición corresponde a la Guía ISO/IEC 51.

3.2.31 peligro: Fuente potencial de daño.

NOTA 1 – Esta definición, sin notas, corresponde al apartado 3.4 de la Guía ISO/IEC 51.

NOTA 2 – El término incluye el peligro para las personas que surge al cabo de un tiempo corto (por ejemplo, fuego y explosión) y también los que afectan a la salud de las personas al cabo de un tiempo largo (por ejemplo, el escape de sustancias tóxicas).

3.2.32 error humano; falta: Acción o inacción humana que produce un resultado no intencionado.

NOTA – Esta es la definición de la Norma ISO/IEC 2382-14-02-03 y se desvía de la dada en VEI 191-05-25 por la adición de “o inacción”.

3.2.33 análisis de impacto: Actividad de determinar el efecto que tendrá un cambio en una función o componente en las otras funciones o componentes de ese sistema, así como en los otros sistemas.

3.2.34 departamento independiente: Departamento que es separado y distinto, por gestión y otros recursos, del departamento responsable de las actividades que tienen lugar durante la fase específica del ciclo de vida de seguridad sometido a la evaluación o validación de la seguridad funcional.

3.2.35 organización independiente: Organización que es separada y distinta, por gestión y otros recursos, de las organizaciones responsables de las actividades que tienen lugar durante la fase específica del ciclo de vida de seguridad sometido a la evaluación o validación de la seguridad funcional.

3.2.36 persona independiente: Persona que es separada y distinta de las actividades que tienen lugar durante la fase específica del ciclo de vida de seguridad sometido a la evaluación o validación de la seguridad funcional, y que no tiene responsabilidad directa en esas actividades.

3.2.37 función de entrada: Función que supervisa el proceso y el equipo asociado a fin de proporcionar información de entrada para la unidad lógica.

NOTA – Una función de entrada podría ser una función manual.

3.2.38 instrumento: Aparato utilizado para efectuar una acción (encontrado habitualmente en los sistemas instrumentados).

NOTA – Los sistemas instrumentados en el sector de procesos se componen generalmente de sensores (por ejemplo, transmisores de presión, caudal, temperatura), unidades lógicas o sistemas de control (por ejemplo, controladores programables, sistemas de control distribuido), y elementos finales (por ejemplo, válvulas de control). En casos especiales, los sistemas instrumentados pueden ser sistemas instrumentados de seguridad (véase el apartado 3.2.72).

3.2.39 función lógica: Función que realiza las transformaciones entre la información de entrada (proporcionada por una o más funciones de entrada) y la información de salida (usada por una o más funciones de salida); las funciones lógicas proporcionan la transformación de una o más funciones de entrada en una o más funciones de salida.

NOTA – Para guía adicional, véanse las Normas IEC 61131-3 y IEC 60617-12.

3.2.40 unidad lógica: Aquella parte de un BPCS o de un SIS que realiza una o más funciones lógicas.

NOTA 1 – En la Norma IEC 61511 se usan los términos siguientes para los sistemas lógicos:

- sistemas lógicos eléctricos para tecnología electromecánica;
- sistemas lógicos electrónicos para tecnología electrónica;
- sistemas lógicos PE para tecnología electrónica programable.

NOTA 2 – Son ejemplos los sistemas eléctricos, los sistemas electrónicos, los sistemas electrónicos programables, los sistemas neumáticos, los sistemas hidráulicos. Los sensores y los elementos finales no forman porte de la unidad lógica.

3.2.40.1 unidad lógica configurada para la seguridad: Unidad lógica PE de grado industrial para uso general que ha sido específicamente configurada para su uso en las aplicaciones de seguridad de acuerdo con el apartado 11.5.

3.2.41 interfaz de mantenimiento/ingeniería: La interfaz de mantenimiento/ingeniería es el hardware y software proporcionado para permitir un mantenimiento o modificación adecuados del SIS. Puede incluir instrucciones y diagnósticos que se pueden encontrar en el software, los terminales de programación con los protocolos de comunicación adecuados, herramientas de diagnóstico, dispositivos de desvío, dispositivos de ensayo y dispositivos de calibración.

3.2.42 atenuación: Acción que reduce las consecuencias de un acontecimiento peligroso.

NOTA – Los ejemplos incluyen la despresurización de emergencia a la detección de un incendio confirmado o de una fuga de gas.

3.2.43 modo de funcionamiento: Manera en que opera una función instrumentada.

3.2.43.1 función instrumentada de seguridad en modo bajo demanda: Cuando se toma una acción especificada (por ejemplo, el cierre de una válvula) en respuesta a condiciones de proceso u otras solicitaciones. En el caso de un fallo peligroso de la función instrumentada de seguridad sólo se produce un peligro potencial en el caso de un fallo en el proceso o en el BPCS.

3.2.43.2 función instrumentada de seguridad en modo continuo: Cuando si se produce un fallo peligroso de la función instrumentada de seguridad, se produce un peligro potencial sin necesidad de un fallo adicional a menos que se tome una acción para evitarlo.

NOTA 1 – El modo continuo cubre aquellas funciones instrumentadas de seguridad que efectúan un control continuo para mantener la seguridad funcional.

NOTA 2 – En las aplicaciones en modo bajo demanda en las que la tasa de demanda sea más frecuente que una vez al año, la tasa de peligro no será superior a la tasa de fallo peligroso de la función instrumentada de seguridad. En tal caso, será normalmente apropiado usar criterios de modo continuo.

NOTA 3 – En las tablas 3 y 4 se definen las medidas de fallo objetivo para las funciones de seguridad instrumentada que operan en modo bajo demanda y en modo continuo.

NOTA 4 – Este término se desvía de la definición dada por la Norma IEC 61508-4 para reflejar las diferencias de la terminología del sector de procesos.

3.2.44 módulo: Conjunto autocontenido de componentes de hardware que realiza una función de hardware específica (es decir, módulo de entrada digital, módulo de salida analógica), o programa de aplicación reutilizable (puede ser interno a un programa o un conjunto de programas) que dan soporte a una función específica, por ejemplo, parte de un programa informático que realiza una función específica.

NOTA 1 – En el contexto de la Norma IEC 61131-3, un módulo de software es una función o bloque de funciones.

NOTA 2 – Este término se desvía de la definición dada por la Norma IEC 61508-4 para reflejar las diferencias de la terminología del sector de procesos.

3.2.45 MooN: Sistema instrumentado de seguridad o parte de éste compuesta por "**N**" canales independientes, que están conectados de tal manera que "**M**" canales son suficientes para ejecutar la función instrumentada de seguridad.

3.2.46 reducción de riesgo necesaria: Reducción de riesgo necesaria para asegurarse de que se reduce el riesgo a un nivel tolerable.

3.2.47 sistema no programable (NP): Sistema basado en tecnologías no informáticas (es decir un sistema no basado en la electrónica programable (PE) o software).

NOTA – Los ejemplos incluirían los sistemas eléctricos o electrónicos cableados, los sistemas mecánicos, hidráulicos, o neumáticos.

3.2.48 interfaz de operador: Medios por los cuales se comunica información entre un(os) operador(es) humano(s) y el SIS (por ejemplo, monitores de rayos catódicos, luces indicadoras, pulsadores, bocinas, alarmas); a veces se hace referencia a la interfaz de operador como la interfaz hombre-máquina (HMI).

3.2.49 sistemas relacionados con la seguridad basados en otra tecnología: Sistemas relacionados con la seguridad que se basan en otra tecnología distinta de la eléctrica, electrónica, o electrónica programable.

NOTA – Una válvula de seguridad es un "sistema relacionado con la seguridad basado en otra tecnología". Los "sistemas relacionados con la seguridad basados en otra tecnología" pueden incluir sistemas hidráulicos y neumáticos.

3.2.50 función de salida: Función que controla el proceso y su equipo asociado según las informaciones del accionador final, a partir de una función lógica.

3.2.51 fase: Periodo dentro del ciclo de seguridad en el que tienen lugar las actividades descritas en esta norma.

3.2.52 prevención: Acción que reduce la frecuencia con la que ocurre un acontecimiento peligroso.

3.2.53 uso anterior: Véase “probado en uso” (véase apartado 3.2.60).

3.2.54 riesgo de proceso: Riesgo que surge de las condiciones de proceso causadas por acontecimientos anormales (incluyendo un mal funcionamiento del BPCS).

NOTA 1 – El riesgo en este contexto es el asociado con el acontecimiento peligroso específico en el cual los SIS se van a usar para proporcionar la reducción de riesgo necesaria (es decir, el riesgo asociado con la seguridad funcional).

NOTA 2 – En la Norma IEC 61511-3 se describe el análisis de riesgo de proceso. El principal objetivo de determinar el riesgo de proceso es establecer un punto de referencia para el riesgo sin tener en cuenta las capas de protección.

NOTA 3 – La evaluación de este riesgo debería incluir los aspectos relativos al factor humano asociado.

NOTA 4 – Este término es equivalente al "riesgo EUC" de la Norma IEC 61508-4.

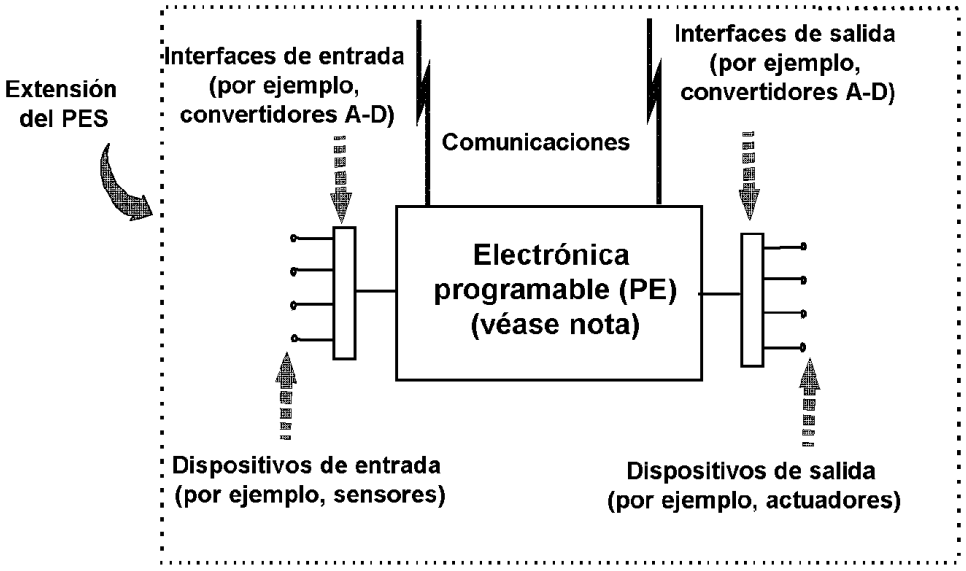
3.2.55 electrónico programable (PE): Componente o dispositivo electrónico que forma parte de un PES y basado en tecnología informática. El término engloba tanto hardware como software y tanto unidades de entrada como de salida.

NOTA 1 – Este término cubre los dispositivos microelectrónicos basados en una o más unidades centrales de proceso (CPU) junto con memorias asociadas. Los ejemplos de electrónica programable en el sector de procesos incluyen:

- sensores y elementos terminales inteligentes;
- unidades lógicas electrónicas programables, que incluyen:
  - controladores programables;
  - controladores lógicos programables;
  - controladores de bucle.

NOTA 2 – Este término difiere de la definición de la Norma IEC 61508-4 para reflejar las diferencias en la terminología del sector de procesos.

3.2.56 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 fuentes de alimentación, sensores y otros dispositivos de entrada, autopistas de datos y otras vías de comunicación, actuadores y otros dispositivos de salida (véase figura 6).



Estructura básica de un PES

NOTA La electrónica programable se presenta localizada centralmente pero podría existir en diversos lugares del PES

Fig. 6 – Sistema electrónico programable (PES): estructura y terminología

3.2.57 programación: Proceso consistente en diseñar, escribir y ensayar un conjunto de instrucciones para resolver un problema o procesar datos.

NOTA – En esta norma, la programación está básicamente asociada a los PE.

3.2.58 ensayo periódico: Ensayo realizado para revelar defectos no detectados de un sistema instrumentado de seguridad de manera que, si fuera necesario, se pueda restaurar el sistema en su funcionalidad de diseño.

3.2.59 capa de protección: Cualquier mecanismo independiente que reduce el riesgo por control, prevención o atenuación.

NOTA – Podría ser un mecanismo de ingeniería de procesos, tal como el tamaño de los recipientes que contienen productos químicos peligrosos, un dispositivo de ingeniería mecánica, tal como un sistema instrumentado de válvula de seguridad, o un procedimiento administrativo, tal como un plan de emergencia contra un peligro inminente. Estas respuestas pueden ser automatizadas o iniciadas por acciones humanas (véase figura 9).

3.2.60 probado en uso: Cuando una evaluación documentada ha mostrado que existe evidencia apropiada, en base al previo uso de un componente, de que el componente es adecuado en un sistema instrumentado de seguridad (véase "uso previo" en el apartado 11.5).

NOTA – Este término se desvía de la Norma IEC 61508 para reflejar las diferencias en la terminología del sector de procesos.

3.2.61 calidad: Totalidad de las características de una entidad que influyen en su capacidad para satisfacer las necesidades establecidas e implicadas.

NOTA – Véanse más detalles en la Norma ISO 9000.

3.2.62 fallo aleatorio del hardware: Fallo que se produce en un momento aleatorio, que resulta de una variedad de mecanismos de degradación del hardware.

NOTA 1 – Existen muchos mecanismos de degradación que se producen a diferentes tasas en diferentes componentes y puesto que las tolerancias de fabricación hacen que sus componentes fallen debido a estos mecanismos después de un tiempo de funcionamiento, los fallos de un equipo total que comprende muchos componentes ocurren a tasas predecibles pero en momentos impredecibles (es decir, aleatorios).

NOTA 2 – Una característica distintiva principal entre los fallos aleatorios del hardware y los fallos sistemáticos (véase el apartado 3.2.85) es que las tasas de fallo del sistema (u otras medidas apropiadas), que surgen de los fallos aleatorios del hardware, se pueden predecir, pero los fallos sistemáticos, por su propia naturaleza, no se pueden predecir. Esto es, las tasas de fallos del sistema que surgen de los fallos aleatorios del hardware pueden ser cuantificadas, pero las que surgen de los fallos sistemáticos no se pueden cuantificar estadísticamente porque los acontecimientos que dan lugar a las mismas no se pueden predecir fácilmente.

3.2.63 redundancia: Uso de elementos o sistemas múltiples para realizar la misma función; la redundancia puede realizarse por elementos idénticos (redundancia idéntica) o por elementos diversos (redundancia diversa).

NOTA 1 – Son ejemplos el uso de componentes funcionales duplicados y la adición de bits de paridad.

NOTA 2 – La redundancia se usa principalmente para mejorar la fiabilidad o la disponibilidad.

NOTA 3 – La definición VEI 191-15-01 es menos completa (ISO/IEC 2382-14-01-11).

NOTA 4 – Este término se desvía de la Norma IEC 61508-4 para reflejar las diferencias en la terminología del sector de procesos.

3.2.64 riesgo: Combinación de la probabilidad de que se produzca un daño y de la gravedad de este último.

NOTA – Véase en el capítulo 8 comentarios adicionales sobre este concepto.

3.2.65 fallo seguro: Fallo que no tiene el potencial de poner en estado peligroso el sistema instrumentado de seguridad o de ponerlo en estado de fallo de funcionamiento.

NOTA 1 – Que se realice el potencial o no puede depender de la arquitectura de canales del sistema.

NOTA 2 – Otras denominaciones usadas para fallo seguro son fallo intempestivo, desencadenamiento parasitario de fallo, falso desencadenamiento de fallo o fallo fuera de la seguridad.

3.2.65.1 proporción de fallos seguros: Proporción de la tasa de fallos aleatorios de hardware de un dispositivo que da lugar a un fallo seguro o a un fallo peligroso detectado.

3.2.66 estado seguro: Estado del proceso cuando se alcanza la seguridad.

NOTA 1 – Al ir de un estado potencialmente peligroso al estado final seguro, el proceso puede tener que pasar por un número de estados seguros intermedios. Para algunas situaciones, sólo existe un estado seguro en tanto se controla continuamente el proceso. Tal control continuo del proceso puede ser por un periodo de tiempo corto o indefinido.

NOTA 2 – Este término se desvía de la Norma IEC 61508-4 para reflejar las diferencias en la terminología del sector de procesos.

3.2.67 seguridad: Ausencia de riesgo inaceptable.

NOTA – Esta definición está de acuerdo con la Guía ISO/IEC 51.

3.2.68 función de seguridad: Función a realizar por un SIS, otro sistema relacionado con la seguridad o instalaciones externas de reducción de riesgo, que está destinada a alcanzar o mantener un estado seguro para el proceso, con respecto a un acontecimiento peligroso específico.

NOTA – Este término se desvía de la Norma IEC 61508-4 para reflejar las diferencias en la terminología del sector de procesos.

3.2.69 función instrumentada de control de seguridad: Función instrumentada de seguridad con un SIL funcionando en modo continuo que es necesaria para evitar que surja una condición peligrosa y/o para atenuar sus consecuencias.

3.2.70 sistema instrumentado de control de seguridad: Sistema instrumentado usado para realizar una o más funciones instrumentadas de control de seguridad.

NOTA – Los sistemas instrumentados de control de seguridad son raros dentro de las industrias de procesos. En los casos en los que se identifican estos sistemas, necesitarán ser tratados como un caso especial y diseñados en base individual. Deberían aplicarse los requisitos de esta norma, pero puede ser necesario un análisis adicional para demostrar que el sistema es capaz de alcanzar los requisitos de seguridad.

3.2.71 función instrumentada de seguridad (SIF): Función de seguridad con un nivel de integridad de seguridad especificado que es necesaria para alcanzar una condición de seguridad funcional y que puede ser una función instrumentada de protección de seguridad o una función instrumentada de control de seguridad.

3.2.72 sistema instrumentado de seguridad (SIS): Sistema instrumentado usado para realizar una o más funciones instrumentadas de seguridad. Un SIS se compone de cualquier combinación de cualquier combinación de sensor(es), unidad(es) lógica(s), y elemento(s) final(es) (por ejemplo, véase la figura 7).

NOTA 1 – Esto puede incluir funciones instrumentadas de control de seguridad o funciones instrumentadas de protección de seguridad o ambas.

NOTA 2 – Los fabricantes y proveedores de dispositivos SIS deberían referirse al capítulo 1 puntos a) a d) inclusive.

NOTA 3 – Un SIS puede incluir software o no.

NOTA 4 – Véase capítulo A.2.

NOTA 5 – Cuando una acción humana forma parte de un SIS, se debe especificar en el SRS la disponibilidad de la acción del operador e incluirla en los cálculos de las características de funcionamiento para el SIS. Véase la Norma IEC 61511-2 para guía sobre como incluir la disponibilidad y la fiabilidad del operador en los cálculos del SIL.

Arquitectura del SIS y ejemplo de función instrumentada de seguridad mostrando diferentes dispositivos

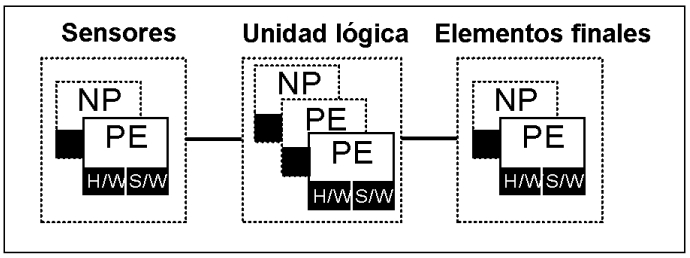


Fig. 7 – Ejemplo de arquitectura de un SIS

3.2.73 integridad de seguridad: Probabilidad media de que un sistema instrumentado de seguridad realice satisfactoriamente las funciones instrumentadas de seguridad en todas las condiciones establecidas dentro de un periodo de tiempo establecido.

NOTA 1 – Cuanto más elevado es el nivel de integridad de seguridad, más alta es la probabilidad de que la función instrumentada de seguridad (SIF) se realice.

NOTA 2 – Existen cuatro niveles de integridad de seguridad para funciones instrumentadas de seguridad.

NOTA 3 – Para la determinación de la integridad de seguridad, se deberían incluir todas las causas de fallos (tanto fallos aleatorios del hardware como fallos sistemáticos) que den lugar a un estado inseguro; por ejemplo, los fallos de hardware, los fallos inducidos por el software y los fallos debidos a interferencias eléctricas. Algunos de estos tipos de fallos, en particular los fallos aleatorios de hardware, se pueden cuantificar usando medidas tales como la tasa de fallos en el modo peligroso de fallo o la probabilidad de que una función instrumentada de seguridad falle en su funcionamiento a solicitud. Sin embargo, la integridad de seguridad de una SIF depende también de muchos factores, los cuales no se pueden cuantificar con precisión, sino que sólo se pueden considerar cualitativamente.

NOTA 4 – La integridad de seguridad comprende la integridad de seguridad del hardware y la integridad de seguridad sistemática.

3.2.74 nivel de integridad de seguridad (SIL): Nivel discreto (uno de cuatro) para especificar los requisitos de integridad de seguridad de las funciones instrumentadas de seguridad a asignar a los sistemas instrumentados de seguridad. La integridad de seguridad de nivel 4 tiene el nivel más elevado de integridad de seguridad; la integridad de seguridad de nivel 1 tiene el más bajo.

NOTA 1 – En las tablas 3 y 4 se especifican las medidas de fallo objetivo para los niveles de integridad de seguridad.

NOTA 2 – Es posible utilizar varios sistemas de nivel de integridad de seguridad inferior para satisfacer las necesidades de una función de nivel más elevado (por ejemplo, utilizando un sistema a la vez de SIL 2 y de SIL 1 para satisfacer las necesidades de una función de SIL 3).

NOTA 3 – Este término difiere de la definición de la Norma IEC 61508-4 para reflejar las diferencias en la terminología del sector de procesos.

3.2.75 especificación de los requisitos relativos a la integridad de seguridad: Especificación que contiene los requisitos relativos a la integridad de las funciones instrumentadas de seguridad que deben ser ejecutadas por el(los) sistema(s) instrumentado(s) de seguridad.

NOTA 1 – Esta especificación constituye una parte (parte relativa a la integridad de seguridad) de la especificación de los requisitos concernientes a la seguridad (véase el apartado 3.2.78)

NOTA 2 – Este término difiere de la definición de la Norma IEC 61508-4 para reflejar las diferencias en la terminología del sector de procesos.

3.2.76 ciclo de vida de seguridad: Actividades necesarias para la realización de la(s) función(es) instrumentada(s) de seguridad que se desarrollan a lo largo de un periodo de tiempo, que comienza en la fase de diseño de un proyecto y termina cuando todas las funciones instrumentadas de seguridad 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 como necesario en este caso, es decir, en el contexto de esta norma.

NOTA 2 – En la figura 8 se da el modelo de ciclo de vida utilizado en la Norma IEC 61511.

3.2.77 manual de seguridad: Un manual de seguridad define como se puede usar sin riesgo el dispositivo, el subsistema o el sistema.

NOTA – Éste puede ser un documento autónomo, un manual de instrucciones, un manual de programación, un documento normalizado, o estar incluido en un(os) documento(s) de usuario que defina limitaciones de aplicación.

3.2.78 especificación de las exigencias relativas a la seguridad: Especificación que contiene todas las exigencias relativas a funciones instrumentadas de seguridad que se deben ejecutar por los sistemas instrumentados de seguridad.

3.2.79 software de seguridad: Software de un sistema instrumentado de seguridad con una funcionalidad de software de aplicación, integrado o utilitario.

3.2.80 sensor: Dispositivo o combinación de dispositivos que miden el estado del proceso (por ejemplo, transmisores, transductores, interruptores de proceso, interruptores de posición).

3.2.81 software: Creación intelectual que comprende los programas, procedimientos, datos, reglas y cualquier documentación correspondiente al funcionamiento de un sistema de proceso de datos.

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

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

3.2.81.1 lenguajes de software en los subsistemas de un SIS

3.2.81.1.1 lenguaje de programa fijado (FPL): En este tipo de lenguaje, el usuario se limita al ajuste de algunos parámetros (por ejemplo, rango de un transmisor de presión, umbrales de alarma, direcciones de la red).

NOTA – Son ejemplos representativos de los dispositivos con FPL: sensor inteligente (por ejemplo, transmisor de presión), válvula inteligente, secuencia de controlador de acontecimientos, caja de alarma inteligente, pequeños sistemas de registro de datos.

3.2.81.1.2 lenguaje de variabilidad limitada (LVL): Este tipo de lenguaje está diseñado para ser comprensible por los usuarios del campo de procesos y proporciona la posibilidad de combinar funciones de biblioteca, predefinidas, específicas de una aplicación, para aplicar las especificaciones de las exigencias relativas a la seguridad. Un LVL proporciona una correspondencia funcional próxima con las funciones necesarias para realizar la aplicación.

NOTA 1 – En la Norma IEC 61131-3 se dan ejemplos típicos de LVL: comprenden el diagrama de escalera, el lenguaje de bloques funcionales y el diagrama funcional en secuencia.

NOTA 2 – Son ejemplos típicos de sistemas que utilizan el LVL: un PLC normal (por ejemplo, autómata programable para la gestión de un quemador).

3.2.81.1.3 lenguaje de variabilidad total (FVL): Este tipo de lenguaje está diseñado para ser comprensible por los informáticos (programadores) y proporciona la posibilidad de aplicar una amplia gama de funciones y de aplicaciones.

NOTA 1 – Un ejemplo típico de sistema que utiliza el FVL son los ordenadores de uso general.

NOTA 2 – En el campo de los procesos, el FVL se encuentra en el software integrado y raramente en el software de aplicación.

NOTA 3 – Entre los ejemplos de FVL se puede citar: el Ada, el C, el Pascal, Instruction List, los lenguajes de ensamblaje, el C++, el Java, el SQL.

3.2.81.2 tipo de programa de software

3.2.81.2.1 software de aplicación: Software específico de la aplicación de usuario. En general, contiene secuencias lógicas, exoneraciones, términos y expresiones lógicas que controlan la entrada, la salida y los cálculos apropiados, las decisiones necesarias para satisfacer las exigencias funcionales instrumentadas de seguridad. Véase el lenguaje fijado y el lenguaje de variabilidad limitada.

3.2.81.2.2 software integrado: Software que forma parte del sistema proporcionado por el constructor y que no es accesible para modificaciones por parte del usuario final. El software integrado se denomina igualmente microsoftware o software de sistema. Véase el apartado 3.2.81.1.3, lenguaje de variabilidad total.

3.2.81.2.3 software utilitario: Herramientas de software para la creación, modificación, y documentación de los programas de aplicación. Estas herramientas no son necesarias para la explotación del SIS.

3.2.82 ciclo de vida del software: Actividades que se desarrollan en el curso de un periodo de tiempo que va desde la fase en la cual se diseña el software hasta el momento en el que ya no se utiliza el software definitivamente.

NOTA 1 – El ciclo de vida del software incluye típicamente una fase de prescripción, una fase de desarrollo, una fase de ensayo, una fase de integración, una fase de instalación y una fase de modificación.

NOTA 2 – El software no se puede mantener, pero es modificable.

3.2.83 subsistema: Véase “sistema”.

3.2.84 sistema: Conjunto de elementos que interactúan según un diseño; un elemento de un sistema puede ser otro sistema, llamado subsistema, pudiendo ser este último un sistema de control, o un sistema controlado, y puede estar compuesto de hardware, de software e interacciones con personas.

NOTA 1 – Una persona puede formar parte de un sistema.

NOTA 2 – Esta definición difiere de la VEI 351-01-01.

NOTA 3 – Un sistema incluye sensores, unidades lógicas, elementos finales, equipos de comunicación y auxiliares que pertenecen al SIS (por ejemplo cables, tuberías, alimentación de energía).

3.2.85 fallo sistemático: Fallo unido de forma determinista a una causa determinada, que no puede ser eliminada más que por una modificación del diseño o del proceso de fabricación, de los procedimientos de operación, de la documentación o de otros factores apropiados.

NOTA 1 – El mantenimiento correctivo sin modificación no elimina, habitualmente, la causa del fallo.

NOTA 2 – Un fallo sistemático puede ser inducido simulando la causa del fallo.

NOTA 3 – Esta definición (hasta la nota 2) corresponde a la VEI 191-04-19.

NOTA 4 – Ejemplos de las causas sistemáticas de fallo comprenden el error humano en:

- la especificación de los requisitos relativos a la seguridad;
- el diseño, la fabricación, la instalación y la explotación del hardware;
- el diseño y/o la instalación del software.

3.2.86 integridad de seguridad sistemática: Parte de la integridad de seguridad de las funciones instrumentadas de seguridad que se refiere a los fallos sistemáticos (véase la nota 3 del apartado 3.2.73) en un modo de fallo peligroso.

NOTA 1 – La integridad de seguridad sistemática no puede ser cuantificada normalmente (a diferencia de la integridad de seguridad del hardware).

NOTA 2 – Véase también el apartado 3.2.29.

3.2.87 medida objetivo de fallos: Probabilidad prevista de fallos de modo peligroso a alcanzar respecto a los requisitos de integridad de seguridad, especificada en términos bien de probabilidad media de fallo para ejecutar la función para la cual ha sido diseñado bajo demanda (en modo de funcionamiento bajo demanda) o bien de frecuencia de un fallo peligroso, por hora, cuando se ejecuta la SIF (para un modo de funcionamiento en continuo).

NOTA – En las tablas 3 y 4 se dan los valores numéricos de las medidas de fallo objetivo.

3.2.88 plantilla; plantilla de software: Parte no especificada y estructurada de software de aplicación que se puede cambiar con facilidad para dar soporte a funciones específicas, conservando la estructura original; por ejemplo, una plantilla interactiva de pantalla controla el encadenamiento de pantallas de la aplicación, pero no es específica de los datos presentados; un programador puede tomar la plantilla genérica y hacer modificaciones para producir una nueva pantalla destinada a los usuarios.

NOTA – A veces se usa el término conexo “plantilla de software”. Típicamente, se refiere a un algoritmo o a un conjunto de algoritmos que han sido programados para ejecutar una función o un conjunto de funciones deseadas, y está constituido de tal manera que puede ser utilizado en numerosos casos diferentes. En el contexto de la Norma IEC 61131-3, es un programa que puede ser escogido para su utilización en numerosas aplicaciones.

3.2.89 riesgo tolerable: Riesgo aceptado en un contexto determinado y fundado en los valores actuales de la sociedad.

NOTA – Véase la Norma IEC 61511-3.

[Guía ISO/IEC 51]

3.2.90 no detectado; no revelado; no declarado: Se refiere a los defectos de hardware y de software, no detectadas por los ensayos de diagnóstico o en el curso de una operación normal.

NOTA – Este término difiere de la definición de la Norma IEC 61508-4 para reflejar las diferencias en la terminología del sector de procesos.

3.2.91 validación: Actividad que consiste en demostrar que la(s) función(es) instrumentada(s) de seguridad y el(los) sistema(s) instrumentado(s) de seguridad en cuestión, después de la instalación, satisfacen en todos los puntos la especificación de los requisitos relativos a la seguridad.

3.2.92 verificación: Actividad que consiste, para cada fase del ciclo de vida de seguridad correspondiente, en demostrar por análisis y/o por ensayos, que para las entradas específicas, las salidas satisfacen, en todos los puntos, los objetivos y los requisitos fijados para la fase específica.

NOTA – Se citan como ejemplos de actividades de verificación:

- las revisiones relativas a las salidas de una fase (documentos relativos a todas las fases del ciclo de vida de seguridad), destinadas a asegurar la conformidad con los objetivos y exigencias de la fase, y tomando en cuenta las entradas especificadas en esta fase;
- las revisiones de diseño;
- los ensayos realizados en los productos instalados, a fin de asegurarse de que su funcionamiento es conforme a su especificación;
- los ensayos de integración realizados en el ensamblaje de las diferentes partes de un sistema, elemento por elemento, a fin de asegurar que todas las partes funcionan las unas con las otras, en conformidad con lo especificado.

3.2.93 perro guardián: Combinación de diagnósticos y de un dispositivo de salida (típicamente un interruptor) para efectuar la supervisión del buen funcionamiento del dispositivo electrónico programable (PE) y emprender una acción cuando se produce la detección de un funcionamiento incorrecto.

NOTA 1 – El perro guardián confirma que el sistema de software funciona correctamente reiniciando regularmente un dispositivo externo (por ejemplo, temporizador electrónico de perro guardián de hardware), por un dispositivo de salida controlado por el software.

NOTA 2 – Se puede usar el perro guardián para desactivar un grupo de salidas de seguridad cuando se detectan fallos peligrosos a fin de poner el proceso en estado seguro. Se usa el perro guardián para aumentar la cobertura de diagnóstico en línea de la unidad lógica PE (véanse los apartados 3.2.15 y 3.2.40).

4 CONFORMIDAD CON ESTA NORMA INTERNACIONAL

Para satisfacer esta norma internacional, se debe demostrar que se ha satisfecho cada uno de los requisitos descritos en los capítulos 5 al 19 según los criterios definidos y por tanto se ha(n) satisfecho el(los) objetivo(s) del capítulo.

5 GESTIÓN DE LA SEGURIDAD FUNCIONAL

5.1 Objetivo

El objetivo de los requisitos de este capítulo es identificar las actividades de gestión que son necesarias para asegurar que se cumplen los objetivos de la seguridad funcional.

NOTA – Este capítulo pretende únicamente alcanzar y mantener la seguridad funcional de los sistemas instrumentados de seguridad y es independiente y distinta de las medidas de salud y seguridad necesarias para el logro de la seguridad en el lugar de trabajo.

5.2 Requisitos

5.2.1 Generalidades

5.2.1.1 La política y la estrategia para alcanzar la seguridad deben ser identificadas conjuntamente con los medios para evaluar su logro y deben ser comunicadas dentro de la organización.

5.2.1.2 Se debe instaurar un sistema de gestión de la seguridad de forma que se asegure que en los casos en los que se usen sistemas instrumentados de seguridad, tengan la capacidad de situar y/o mantener el proceso en un estado seguro.

5.2.2 Organización y recursos

5.2.2.1 Las personas, departamentos, organizaciones u otras unidades que sean responsables de realizar y revisar cada una de las fases del ciclo de vida de seguridad deben ser identificadas y deben ser informadas de las responsabilidades asignadas a ellas (incluyendo, en los casos en los que sea relevante, las autoridades que otorgan los permisos o los organismos reguladores de la seguridad).

5.2.2.2 Las personas, departamentos u organismos implicados en actividades del ciclo de vida de seguridad deben ser competentes para realizar las actividades de las que son responsables.

NOTA – Como mínimo, se deberían tratar los aspectos siguientes cuando se considere la competencia de las personas, departamentos, organismos u otras unidades implicados en las actividades del ciclo de vida de seguridad

a) conocimientos de ingeniería, formación y experiencia apropiados para la aplicación de proceso;

b) conocimientos de ingeniería, formación y experiencia apropiados para la tecnología de la aplicación usada (por ejemplo, eléctrica, electrónica o electrónica programable);

c) conocimientos de ingeniería, formación y experiencia apropiados para los sensores y elementos finales;

d) conocimientos de ingeniería de seguridad (por ejemplo, análisis de seguridad de procesos);

e) conocimientos de los requisitos de las reglamentaciones legales y de seguridad;

f) gestión adecuada y habilidades de liderazgo adecuadas para su papel en las actividades del ciclo de vida de seguridad;

g) entendimiento de las consecuencias potenciales de un acontecimiento;

h) el nivel de integridad de seguridad de las funciones instrumentadas;

i) la innovación y complejidad de la aplicación y de la tecnología.

5.2.3 Evaluación y gestión de los riesgos. Se deben identificar los peligros, evaluar los riesgos y determinar la reducción de riesgo necesaria como se define en el capítulo 8.

NOTA – Puede ser beneficioso considerar también las pérdidas de capital potenciales, por razones económicas.

5.2.4 Planificación. Se debe instaurar la planificación de la seguridad para definir las actividades que se requiere realizar junto con las personas, departamentos, organismos u otras unidades responsables de realizar estas actividades. Se debe actualizar esta planificación en la forma necesaria a lo largo de todo el ciclo de vida de seguridad (véase el capítulo 6).

NOTA – La planificación de la seguridad puede ser incorporada en

- una sección del plan de calidad titulada "plan de seguridad"; o
- un documento independiente titulado "plan de seguridad"; o
- varios documentos que pueden incluir procedimientos de empresa o prácticas de trabajo.

5.2.5 Aplicación y supervisión

5.2.5.1 Se deben aplicar los procedimientos para asegurarse de su pronto seguimiento y satisfactoria resolución de las recomendaciones correspondientes al sistema instrumentado de seguridad procedentes de:

a) análisis de peligros y evaluación de riesgos;

b) actividades de evaluación y auditoría;

c) actividades de verificación;

d) actividades de validación;

e) actividades post-incidente y post-accidente.

5.2.5.2 Cualquier proveedor, que suministre productos o servicios a una organización, teniendo responsabilidad general de una o más fases del ciclo de vida de seguridad, debe proporcionar productos o servicios como hayan sido especificados por esa organización y debe tener un sistema de gestión de la calidad. Se deben instaurar procedimientos para establecer la adecuación del sistema de gestión de la calidad.

5.2.5.3 Se deben aplicar procedimientos para evaluar las características de funcionamiento del sistema instrumentado de seguridad en función de sus requisitos de seguridad, incluyendo procedimientos para

- identificación y prevención de los fallos sistemáticos que pudieran perjudicar la seguridad;
- evaluar si las tasas de fallos peligrosos del sistema instrumentado de seguridad están de acuerdo con las asumidas durante el diseño;

  NOTA 1 – Los fallos peligrosos se revelan por medio de ensayos periódicos, diagnósticos o fallos para funcionar bajo demanda.

  NOTA 2 – Se deberían considerar procedimientos que definan la acción correctiva necesaria a tomar si las tasas de fallo son mayores de lo asumido durante el diseño.

- evaluar la tasa de demanda de las funciones instrumentadas de seguridad durante el funcionamiento real para verificar los supuestos realizados durante la evaluación de riesgo cuando se determinaron los requisitos de nivel de integridad.

5.2.6 Evaluación, auditorías y revisiones

5.2.6.1 Evaluación de la seguridad funcional

5.2.6.1.1 Se debe definir y ejecutar un procedimiento para una evaluación de seguridad funcional de tal manera que se pueda emitir un juicio respecto a la seguridad funcional y la integridad de seguridad lograda por el sistema instrumentado de seguridad. El procedimiento debe requerir que se nombre un equipo evaluador que incluya la experiencia técnica, de aplicaciones y de explotación necesarias para la instalación concreta.

5.2.6.1.2 Los integrantes del equipo evaluador deben incluir al menos una persona experimentada competente no implicada en el equipo de diseño del proyecto.

NOTA 1 – Cuando el equipo de evaluación es grande, se debería dar consideración a disponer de más de una persona competente con experiencia que sea independiente del equipo del proyecto.

NOTA 2 – Se deberían considerar los aspectos siguientes cuando se planifica una evaluación de la seguridad funcional:

- el objeto de la evaluación de la seguridad funcional;
- quién va a participar en la evaluación de la seguridad funcional;
- las experiencias, responsabilidades y autoridades del equipo de evaluación de la seguridad funcional;
- la información que se generará como resultado de la actividad de evaluación de la seguridad funcional;
- la identidad de cualesquiera otros organismos de seguridad implicados en la evaluación;
- los recursos requeridos para completar la actividad de evaluación de la seguridad funcional;
- el nivel de independencia del equipo de evaluación;
- los medios por los cuales se revalidará la evaluación de la seguridad funcional después de las modificaciones.

5.2.6.1.3 Las etapas del ciclo de seguridad en las cuales se tienen que llevar a cabo las actividades de evaluación de la seguridad funcional se deben identificar durante la planificación de la seguridad.

NOTA 1 – Puede ser necesario introducir actividades adicionales de evaluación de la seguridad conforme se identifican nuevos peligros, después de las modificaciones y a intervalos periódicos durante el funcionamiento.

NOTA 2 – Se debería dar consideración a la realización de actividades de evaluación de la seguridad funcional en las etapas siguientes (véase la fiugura 8).

- Etapa 1 – Después de haber llevado a cabo la evaluación de peligros y riesgos, de haber identificado las capas de protección requeridas y de haber realizado la especificación de los requisitos de seguridad.
- Etapa 2 – Después de haber diseñado el sistema instrumentado de seguridad.
- Etapa 3 – Después de haber completado la instalación, recepción previa y validación final del sistema instrumentado y de haber redactado los procedimientos de operación y el mantenimiento.
- Etapa 4 – Después de adquirir experiencia en la operación y el mantenimiento.
- Etapa 5 – Después de la modificación y antes de la retirada de servicio de un sistema instrumentado de seguridad.

NOTA 3 – El número, tamaño y objeto de las actividades de evaluación de la seguridad funcional debería depender de las circunstancias específicas. Los factores para esta decisión podrían incluir:

- el tamaño del proyecto;
- el grado de complejidad;
- el nivel de integridad de seguridad;
- la duración del proyecto;
- las consecuencias en caso de fallo;
- el grado de normalización de las características de diseño;
- los requisitos de los reglamentos de seguridad;
- la experiencia previa con un diseño similar.

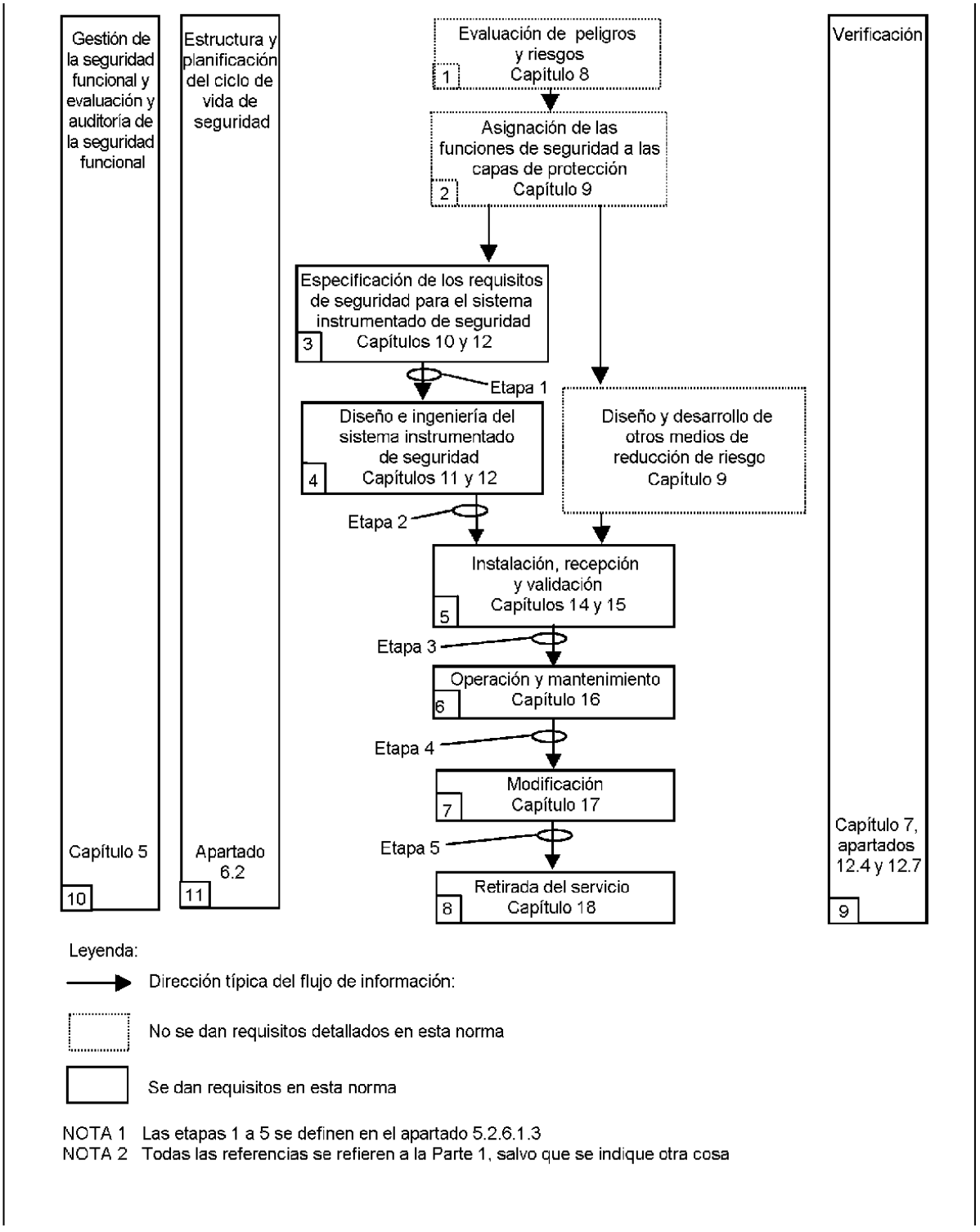


Fig. 8 – Fases del ciclo de vida de seguridad y etapas de evaluación de seguridad funcional

5.2.6.1.4 Se debe realizar al menos una evaluación de seguridad funcional. Esta evaluación de seguridad funcional se debe realizar para asegurar que los peligros que surgen de un proceso y de sus equipos asociados son controlados adecuadamente. Como mínimo, se debe realizar una evaluación antes de que se presenten los peligros identificados (es decir, la etapa 3). El equipo de evaluación debe confirmar, antes de que se presenten los peligros identificados que:

- se ha realizado la evaluación de peligros y riesgos (véase el apartado 8.1);
- se han realizado o resuelto las recomendaciones que surgen de la evaluación de peligros y riesgos que son aplicables al sistema instrumentado de seguridad;
- se han efectuado los procedimientos de cambio de diseño de proyecto y han sido aplicados correctamente;
- se han resuelto las recomendaciones que surgen de la evaluación de seguridad funcional previa;
- el sistema instrumentado de seguridad está diseñado, construido e instalado de acuerdo con la especificación de requisitos de seguridad, habiendo sido identificadas y resueltas cualesquiera diferencias;
- se efectúan los procedimientos de seguridad, funcionamiento, mantenimiento y emergencia correspondientes al sistema instrumentado de seguridad;
- la planificación de la validación del sistema instrumentado de seguridad es apropiada y se han completado las actividades de validación;
- se ha completado la formación de los empleados y se ha proporcionado información apropiada sobre el sistema instrumentado de seguridad al personal de mantenimiento y operación;
- se aplican planes y estrategias para realizar evaluaciones adicionales de seguridad funcional.

5.2.6.1.5 En los casos en los que se usan herramientas de desarrollo y producción para cualquier actividad del ciclo de vida de seguridad, se debe someter a las mismas a una evaluación de la seguridad funcional.

NOTA 1 – El grado según el cual tienen que tratarse dichas herramientas dependerá de su impacto en la seguridad a lograr.

NOTA 2 – Ejemplos de herramientas de desarrollo y producción incluyen herramientas de simulación y modelización, equipos de medición, equipos de ensayo, equipos usados durante las actividades de mantenimiento y las herramientas de gestión de la configuración.

NOTA 3 – La evaluación de la seguridad funcional de las herramientas incluye la trazabilidad de las normas de calibración, la historia de funcionamiento y la lista de defectos, pero no se limita a estos aspectos.

5.2.6.1.6 Los resultados de la evaluación de la seguridad funcional deben estar disponibles junto con cualquier recomendación que proceda de esta evaluación.

5.2.6.1.7 Se debe hacer disponible toda información relevante al equipo de evaluación de la seguridad funcional a su solicitud.

5.2.6.2 Auditoría y revisión

5.2.6.2.1 Se deben definir y ejecutar los procedimientos para auditar la conformidad con los requisitos, comprendiendo:

- la frecuencia de las actividades de auditoría;
- el grado de independencia entre las personas, departamentos, organismos u otras unidades que realicen el trabajo y los que realizan las actividades de auditoría;
- las actividades de registro y seguimiento.

5.2.6.2.2 La gestión de los procedimientos de modificación debe efectuarse para iniciar, documentar, revisar, aplicar y aprobar los cambios en el sistema instrumentado de seguridad que no sean la sustitución en tipo (es decir, por otro elemento idéntico).

5.2.7 Gestión de la configuración del SIS

5.2.7.1 Requisitos

5.2.7.1.1 Deben hallarse disponibles los procedimientos para la gestión de la configuración del SIS durante todas las fases del ciclo de vida de seguridad del SIS y del software. En particular, se debería especificar los puntos siguientes:

- la etapa en la cual se debe realizar el control de la configuración formal;
- los procedimientos a usar para identificar de manera unívoca todas las partes constitutivas de un elemento (hardware y software);
- los procedimientos para impedir que entren en servicio elementos no autorizados.

6 REQUISITOS RELATIVOS AL CICLO DE VIDA DE SEGURIDAD

6.1 Objetivos

Los objetivos de este capítulo son:

- definir las fases y establecer los requisitos de las actividades del ciclo de vida de seguridad;
- organizar las actividades técnicas en un ciclo de vida de seguridad;
- asegurar que existe (o se desarrolla) una planificación adecuada que permite tener la certeza de que el sistema instrumentado de seguridad satisfará todos los requisitos de seguridad.

NOTA – En las figuras 8, 10 y 11 se muestra el enfoque general de esta norma. Debería destacarse que este enfoque es con fines ilustrativos y sólo pretende indicar las actividades típicas del ciclo de vida de seguridad desde el diseño inicial hasta la retirada del servicio.

6.2 Requisitos

6.2.1 Durante la planificación de la seguridad se debe definir un ciclo de vida de seguridad que incorpore los requisitos de esta norma.

6.2.2 Se debe definir cada fase del ciclo de vida de seguridad en términos de entradas, salidas y actividades de verificación (véase la tabla 2).

Tabla 2
Vista de conjunto del ciclo de vida de seguridad de un SIS

Fase o actividad del ciclo de vida de seguridad		Objetivos	Requisitos Capítulo o apartado	Entradas	Salidas
Número de caja de la figura 8	Título				
1	Evaluación de peligro y riesgo	Determinar los peligros y acontecimientos peligrosos del proceso y de los equipos asociados, la secuencia de acontecimientos que lleva al acontecimiento peligroso, los riesgos de proceso asociados con el acontecimiento peligroso, los requisitos para la reducción del riesgo y las funciones de seguridad requeridas para lograr la reducción de riesgo necesaria	8	Diseño de proceso, disposición, los equipos de personal, objetivos de seguridad	Una descripción de los peligros, de la(s) función(es) de seguridad requerida(s) y de la reducción de riesgos asociada
2	Asignación de las funciones de seguridad a las capas de protección	Asignación de las funciones de seguridad a las capas de protección y para cada función instrumentada de seguridad, el nivel de integridad de seguridad asociado	9	Una descripción de la(s) función(es) instrumentada(s) de seguridad y de los requisitos de integridad de seguridad asociados	Descripción de los requisitos de asignación de seguridad (Véase capítulo 9)
3	Especificación de los requisitos de seguridad del SIS	Especificar los requisitos para cada SIS en términos de las funciones instrumentadas de seguridad requeridas y de su integridad de seguridad asociada a fin de alcanzar la seguridad funcional requerida	10	Descripción de la asignación de requisitos de seguridad (véase el capítulo 9)	Requisitos de seguridad del SIS; requisitos de seguridad del software
4	Diseño e ingeniería del SIS	Diseñar el SIS para satisfacer los requisitos correspondientes de las funciones instrumentadas de seguridad y de la integridad de seguridad	11 y 12.4	Requisitos de seguridad del SIS Requisitos de seguridad del software	Diseño del SIS en conformidad con los requisitos de seguridad del SIS; planificación para el ensayo de integración del SIS
5	Instalación, recepción y validación del SIS	Integrar y ensayar el SIS Validar que el SIS satisface en todos los aspectos los requisitos de seguridad en términos de las funciones instrumentadas de seguridad y de integridad de seguridad requeridas	12.3, 14, 15	Diseño del SIS Plan de ensayo de integración del SIS Requisitos de seguridad del SIS Plan para la validación de seguridad del SIS	SIS funcionando completamente de acuerdo con los resultados de diseño del SIS en los ensayos de integración del SIS Resultados de las actividades de instalación, recepción y validación

(Continúa)

Tabla 2 *(Fin)*
Vista de conjunto del ciclo de vida de seguridad de un SIS

Fase o actividad del ciclo de vida de seguridad		Objetivos	Requisitos	Entradas	Salidas
Número de caja de la figura 8	Título		Capítulo o apartado		
6	Operación y mantenimiento del SIS	Asegurar que se mantiene la seguridad funcional del SIS durante la operación y el mantenimiento	16	Requisitos del SIS Diseño del SIS Plan para la operación y el mantenimiento del SIS	Resultados de las actividades de operación y mantenimiento
7	Modificación del SIS	Hacer correcciones, mejoras o adaptaciones del SIS, asegurándose de que se alcanza y mantiene el nivel de integridad de seguridad requerido	17	Requisitos de seguridad del SIS revisados	Resultados de la modificación del SIS
8	Retirada del servicio	Asegurarse una revisión y organización del sector apropiadas y asegurarse que la SIF sigue siendo apropiada	18	Requisitos de seguridad "tal como se construyó" e información de proceso	SIF puesta fuera de servicio
9	Verificación del SIS	Ensayar y evaluar las salidas de una fase dada para asegurarse de la veracidad y la coherencia con respecto a los productos y a las normas dadas como entrada en esa fase	7, 12.7	Plan para la verificación del SIS para cada fase	Resultados de la verificación del SIS para cada fase
10	Evaluación de la seguridad funcional del SIS	Investigar y llegar a un juicio sobre la seguridad funcional alcanzada por el SIS	5	Planificación de la evaluación de la seguridad funcional del SIS Requisitos de seguridad del SIS	Resultados de la evaluación de seguridad funcional del SIS

6.2.3 Para todas las fases del ciclo de vida de seguridad, debe tener lugar una planificación de seguridad que defina los criterios, técnicas, medidas y procedimientos para:

- asegurar que se cumplen los requisitos de seguridad del SIS para todos los modos relevantes del proceso; esto incluye requisitos tanto funcionales como de integridad de seguridad;
- asegurar una instalación y recepción apropiadas del sistema instrumentado de seguridad;
- asegurar la integridad de seguridad de las funciones instrumentadas de seguridad después de la instalación;
- mantener la integridad de seguridad durante el funcionamiento (por ejemplo, ensayos periódicos, análisis de fallos);
- gestionar los peligros de proceso durante las actividades de mantenimiento en el sistema instrumentado de seguridad.

7 VERIFICACIÓN

7.1 Objetivo

El objetivo de este capítulo es demostrar por revisión, análisis y/o ensayo que las salidas requeridas satisfacen los requisitos definidos para las fases apropiadas (figura 8) del ciclo de vida de seguridad identificado por la planificación de seguridad.

7.1.1 Requisitos. La planificación de verificación debe definir todas las actividades requeridas para la fase apropiada (figura 8) del ciclo de vida de seguridad. Debe cumplir esta norma proporcionando los siguientes elementos:

- las actividades de verificación;
- los procedimientos, medidas y técnicas a usar para la verificación, incluyendo la aplicación y resolución de las recomendaciones resultantes;
- cuándo tendrán lugar estas actividades;
- las personas, departamentos y organismos responsables de estas actividades, incluyendo los niveles de independencia;
- la identificación de los elementos a verificar;
- la identificación de la información contra la que se efectúa la verificación;
- como tratar las no conformidades;
- herramientas y análisis de soporte.

7.1.1.1 La verificación se debe realizar según la planificación de la verificación.

7.1.1.2 Se deben hacer disponibles los resultados del proceso de verificación.

NOTA 1 – La selección de las técnicas y medidas para el proceso de verificación y el grado de independencia depende de un número de factores que incluyen el grado de complejidad, la novedad del diseño, la novedad de la tecnología y el nivel de integridad de seguridad requerido.

NOTA 2 – Ejemplos de algunas actividades de verificación incluyen revisiones de diseño, uso de herramientas y técnicas incluyendo herramientas de verificación del software y herramientas de CAD.

8 EVALUACIÓN DE PELIGROS Y RIESGOS DE PROCESO

8.1 Objetivo

El objetivo de los requisitos de este capítulo son:

- determinar los peligros y acontecimientos peligrosos del proceso y equipos asociados;
- determinar la secuencia de acontecimientos que da lugar al acontecimiento peligroso;
- determinar los riesgos de proceso asociados al acontecimiento peligroso;
- determinar cualquier requisito para la reducción del riesgo;
- determinar las funciones de seguridad requeridas para lograr la reducción de riesgo necesaria;
- determinar si alguna de las funciones de seguridad son funciones de seguridad instrumentadas (véase el capítulo 9).

NOTA 1 – El capítulo 8 de esta norma se dirige a los ingenieros de procesos, especialistas en peligros y riesgos, gestores de la seguridad así como a ingenieros de instrumentación. La finalidad es reconocer el enfoque multidisciplinario requerido típicamente para la determinación de las funciones instrumentadas de seguridad.

NOTA 2 – En los casos en los que sea razonablemente factible, se deberían diseñar los procesos para que fueran intrínsecamente seguros. Cuando esto no es práctico, se puede necesitar añadir al diseño métodos de reducción de riesgo como sistemas de protección mecánica y sistemas instrumentados de seguridad. Estos sistemas pueden actuar solos o en combinación entre sí.

NOTA 3 – En la figura 9 se indican métodos de reducción de riesgo típicos que se encuentran en plantas de procesos (sin implicar jerarquía).

8.2 Requisitos

8.2.1 Se debe realizar una evaluación de peligros y riesgos en el proceso y sus equipos asociados (por ejemplo, un BPCS). Debe dar lugar a

- una descripción de cada acontecimiento peligroso identificado y de los factores que contribuyen a ello (incluyendo errores humanos);
- una descripción de las consecuencias y probabilidad del acontecimiento;
- una consideración de condiciones tales como funcionamiento normal, arranque, parada, mantenimiento, pérdida de control del proceso, parada de emergencia;
- la determinación de los requisitos para la reducción adicional del riesgo necesaria a fin de lograr la seguridad requerida;
- una descripción de las medidas tomadas para reducir o eliminar los peligros y el riesgo, o referencias a la información sobre las mismas;
- una descripción detallada de los supuestos hechos durante el análisis de los riesgos, incluyendo las tasa de demanda probables y las tasas de fallo de los equipos, y cualquier toma en cuenta de limitaciones operacionales o de la intervención humana;
- la asignación de las funciones de seguridad a las capas de protección (véase el capítulo 9) teniendo en cuenta la reducción potencial en la protección efectiva debida a fallos de causa común entre las capas de seguridad y entre las capas de seguridad y el BPCS (véase la nota 1);
- identificación de aquella(s) función(es) aplicada(s) como función(es) instrumentada(s) (véase el capítulo 9).

NOTA 1 – En la determinación de los requisitos de integridad de seguridad, será necesario tener en cuenta los efectos de causa común entre los sistemas que crean las demandas y los sistemas de protección que se diseñan para responder a esas demandas. Un ejemplo en este sentido sería el caso en que las demandas surjan por fallo del sistema de control y el equipo usado dentro de los sistemas de protección sea similar o idéntico al equipo que se usa en el sistema de control. En tales casos, una demanda causada por un fallo en el sistema de control puede no ser respondida eficazmente si una causa común ha hecho que el equipo similar del sistema de protección sea ineficaz. Puede no ser posible reconocer problemas de causa común durante la identificación inicial del peligro y el análisis del riesgo porque en una etapa tan temprana no se habrá completado necesariamente el diseño del sistema de protección. En tales casos, será necesario reconsiderar los requisitos para la integridad de seguridad y para las funciones instrumentadas de seguridad una vez se ha completado el sistema instrumentado de seguridad y las otras capas de protección. Para determinar si el diseño general del sistema instrumentado de seguridad y de las capas de protección satisface los requisitos, será necesario considerar los fallos de causa común.

NOTA 2 – En la Norma IEC 61511-3 se ilustran ejemplos de técnicas que se pueden usar para establecer el SIL requerido de las funciones instrumentadas de seguridad.

8.2.2 La tasa de fallos peligrosos de un BPCS (que no satisface la Norma IEC 61511) que realiza una demanda en una capa de protección, no debe ser estimada en un valor mejor que 10^{-5} por hora.

8.2.3 Se debe registrar la evaluación de peligro y riesgo de tal modo que la relación entre los elementos anteriores sea clara y trazable.

NOTA 1 – Los objetivos anteriores no obligan a que los objetivos de riesgo y de reducción de riesgo tengan que recibir un valor numérico. También se pueden usar enfoques gráficos (véase la Norma IEC 61511-3).

NOTA 2 – La extensión de la reducción de riesgo necesaria debería variar dependiendo de la aplicación y de los requisitos legales nacionales. Un principio aceptado en muchos países es que se deberían aplicar medidas adicionales de reducción de riesgo hasta que el costo incurrido llegue a hacerse desproporcionado respecto a la reducción de riesgo alcanzada.

9 ASIGNACIÓN DE LAS FUNCIONES DE SEGURIDAD A LAS CAPAS DE PROTECCIÓN

9.1 Objetivos

Los objetivos de los requisitos de este capítulo son:

- asignar las funciones de seguridad a las capas de protección;
- determinar las funciones instrumentadas de seguridad requeridas;
- determinar, para cada función instrumentada de seguridad, el nivel de integridad de seguridad asociado.

NOTA – Se debería tener en cuenta, durante el proceso de asignación, otras normas o códigos de la industria.

9.2 Requisitos del proceso de asignación

9.2.1 El proceso de asignación debe dar como resultado

- la asignación de funciones de seguridad a capas de protección específicas para fines de prevención, control o atenuación de los peligros del proceso y sus equipos asociados;
- la asignación de objetivos de reducción de riesgo a las funciones instrumentadas de seguridad.

NOTA – Los requisitos legislativos u otros códigos de la industria pueden determinar prioridades en el proceso de asignación.

9.2.2 Se debe deducir el nivel de integridad de seguridad requerido de una función instrumentada de seguridad teniendo en cuenta la reducción de riesgo requerida que se va a proporcionar mediante esa función.

NOTA – Véase guía en la Norma IEC 61511-3.

9.2.3 Para cada función instrumentada de seguridad que opere en modo de demanda, se debe especificar el SIL requerido de acuerdo con la tabla 3 ó la tabla 4. Si se usa la tabla 4, no se deben usar ni el intervalo entre ensayos periódicos ni la tasa de demanda para la determinación del nivel de integridad de seguridad.

9.2.4 Para cada función instrumentada de seguridad que opere en modo continuo de funcionamiento, se debe especificar el SIL requerido de acuerdo con la tabla 4.

Tabla 3
Niveles de integridad de seguridad: probabilidad de fallo bajo demanda

FUNCIONAMIENTO EN MODO BAJO DEMANDA		
Nivel de integridad de seguridad (SIL)	**Probabilidad de fallo media objetivo de fallo bajo demanda**	**Reducción de riesgo objetivo**
4	$\geq 10^{-5}$ a $<10^{-4}$	>10 000 a ≤100 000
3	$\geq 10^{-4}$ a $<10^{-3}$	>1 000 a ≤10 000
2	$\geq 10^{-3}$ a $<10^{-2}$	>100 a ≤1 000
1	$\geq 10^{-2}$ a $<10^{-1}$	>10 a ≤100

Tabla 4
Niveles de integridad de seguridad: probabilidad de fallos peligrosos de las SIF

FUNCIONAMIENTO EN MODO CONTINUO	
Nivel de integridad de seguridad (SIL)	**Probabilidad objetivo de fallos peligrosos para realizar la función instrumentada de seguridad (por hora)**
4	$\geq 10^{-9}$ a $<10^{-8}$
3	$\geq 10^{-8}$ a $<10^{-7}$
2	$\geq 10^{-7}$ a $<10^{-6}$
1	$\geq 10^{-6}$ a $<10^{-5}$

NOTA 1 – Véase el apartado 3.2.43 para explicaciones adicionales.

NOTA 2 – El nivel de integridad de seguridad se define numéricamente de forma que constituya un objetivo para comparar diseños y soluciones alternativos. Sin embargo se reconoce que, en el actual estado de los conocimientos, muchas causas sistemáticas de fallos sólo se pueden evaluar cualitativamente.

NOTA 3 – La frecuencia requerida de fallos peligrosos para una función instrumentada de seguridad en modo continuo se determina considerando el riesgo (en términos de tasa de peligro) causado por un fallo de la función instrumentada de seguridad que actúa en modo continuo junto con la tasa de fallo de otros equipos que conduzcan al mismo riesgo, teniendo en cuenta las contribuciones de otras capas de protección.

NOTA 4 – Es posible usar varios sistemas de una función de seguridad inferior para satisfacer la necesidad de un nivel de integridad de seguridad más elevado (por ejemplo, usando un sistema con SIL 2 y con SIL 1 juntos para satisfacer la necesidad de una función de SIL 3).

9.3 Requisitos adicionales para satisfacer el nivel 4 de integridad de seguridad

9.3.1 No se debe asignar a un sistema instrumentado de seguridad ninguna función instrumentada de seguridad con un nivel de integridad de seguridad superior que el asociado a un nivel 4. Son raras en la industria de procesos las aplicaciones que requieren el uso de una única función instrumentada de seguridad de nivel 4 de integridad de seguridad. Se debe evitar tales aplicaciones en los casos en los que sea razonablemente factible debido a la dificultad de alcanzar y mantener niveles tan altos de características de funcionamiento a lo largo del ciclo de vida de seguridad. En los casos en los que se especifiquen tales sistemas, requerirán niveles elevados de competencia por parte de todos los implicados a lo largo del ciclo de vida de seguridad.

Si el análisis da lugar a que se asigne un nivel 4 de integridad de seguridad a una función instrumentada, se debe dar consideración a cambios en el diseño del proceso de tal manera que se haga más inherentemente seguro o a añadir capas adicionales de protección. Estas mejoras podrían quizá reducir los requisitos de nivel de integridad de seguridad para la función instrumentada de seguridad.

9.3.2 Se debe permitir una función instrumentada de seguridad de nivel 4 de integridad de seguridad sólo si se satisfacen los criterios de a) o tanto de b) como de c) indicados a continuación.

a) Ha habido una demostración explícita por combinación de métodos analíticos apropiados y ensayos, de que se ha satisfecho la medida de fallos de integridad de seguridad objetivo.

b) Ha habido experiencia amplia de operación con los componentes usados como parte de la función instrumentada de seguridad.

   NOTA – Se debería haber adquirido tal experiencia en entornos similares y, como mínimo, se deberían haber utilizado los componentes en un sistema de nivel de complejidad comparable.

c) Existen suficientes datos de fallo del hardware, obtenidos de componentes usados como parte de la función instrumentada de seguridad, para otorgar una confianza suficiente sobre la medida objetivo de fallos de integridad de seguridad del hardware que se va a reivindicar.

NOTA – Los datos deberían ser correspondientes al entorno, aplicación y nivel de complejidad propuestos.

9.4 Requisitos relativos al sistema de control de procesos básico como capa de protección

9.4.1 El sistema de control de procesos básico puede ser identificado como una capa de protección, tal como se muestra en la figura 9.

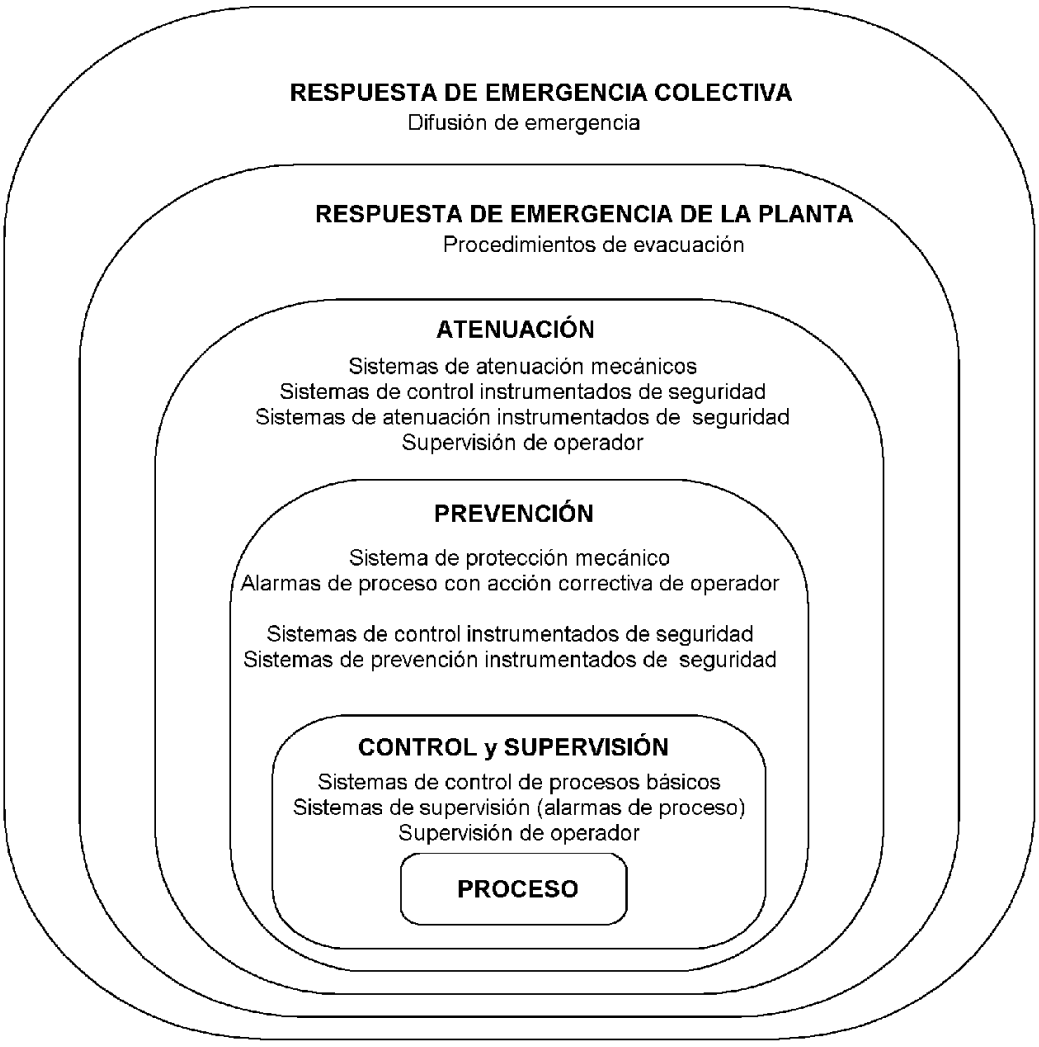


Fig. 9 – Métodos típicos de reducción de riesgo que se encuentran en las plantas de proceso

9.4.2 El factor de reducción de riesgo para un BPCS (que no satisface las Normas IEC 61511 o IEC 61508) usado como capa de protección debe estar por debajo de 10.

NOTA – Cuando se considera cuánto crédito otorgar a un BPCS en lo que se refiere a reducción de riesgo, se debería dar consideración al hecho de que una parte del BPCS puede ser también una fuente iniciadora de un acontecimiento.

9.4.3 Si se reivindica para un BPCS un factor de reducción superior a 10, se debe diseñar según los requisitos de esta norma.

9.5 Requisitos para evitar los fallos de causa común, de modo común y dependientes

9.5.1 Se debe evaluar el diseño de las capas de protección para asegurar que la probabilidad de fallos de causa común, de modo común y dependientes entre las capas de protección y entre las capas de protección y el BPCS es suficientemente baja en comparación con los requisitos generales de integridad de seguridad de las capas de protección. La evaluación puede ser cualitativa o cuantitativa.

NOTA – Véase el aparatado 3.2.12 para una definición de fallo dependiente.

9.5.2 La evaluación debe considerar los siguientes aspectos:

- la independencia entre las capas de protección;
- la diversidad entre las capas de protección;
- la separación física entre las diferentes capas de protección;
- los fallos de causa común entre las capas de protección y entre las capas de protección y el BPCS (por ejemplo, ¿pueden las válvulas de seguridad causar los mismos problemas que la obturación de los sensores en un SIS?).

10 ESPECIFICACIÓN DE LOS REQUISITOS DE SEGURIDAD DE UN SIS

10.1 Objetivo

El objetivo de este capítulo es especificar los requisitos para la(s) función(es) de seguridad instrumentada

10.2 Requisitos generales

10.2.1 Los requisitos de seguridad se deben deducir de la asignación de las funciones instrumentadas de seguridad y de los requisitos identificados durante la planificación de seguridad.

NOTA – Los requisitos del SIS deberían ser expresados y estructurados de tal manera que sean:

- claros, precisos, verificables, mantenibles y factibles; y
- escritos para ayudar a la comprensión por parte de aquellos que probablemente utilicen la información en cualquier fase del ciclo de vida.

10.3 Requisitos de seguridad del SIS

10.3.1 Estos requisitos deben ser suficientes para diseñar el SIS y deben incluir los puntos siguientes:

- una descripción de todas las funciones instrumentadas de seguridad necesarias para alcanzar la seguridad funcional requerida;
- los requisitos para identificar y tener en cuenta los fallos de causa común;
- una definición del estado seguro del proceso para cada función instrumentada de seguridad identificada;
- una definición de cada uno de los estados individualmente seguros del proceso que, cuando se producen en forma concurrente, crean un peligro distinto (por ejemplo, la sobrecarga del almacenamiento de emergencia, alivio de gases a un sistema de antorcha);
- las fuentes supuestas de demanda y la tasa de demanda respecto a la función instrumentada de seguridad;
- los requisitos de los intervalos de ensayos periódicos;

- los requisitos de tiempo de respuesta para que el SIS lleve el proceso a un estado seguro;
- el nivel de integridad de seguridad y el modo de funcionamiento (bajo demanda/continuo) para cada función instrumentada de seguridad;
- una descripción de las mediciones de proceso del SIS y sus puntos de disparo;
- una descripción de las acciones de salida de proceso del SIS y los criterios de funcionamiento satisfactorio, por ejemplo, requisitos para válvulas de cierre estanco;
- la relación funcional entre las entradas y las salidas de proceso, incluyendo las funciones lógicas, matemáticas y cualesquiera tolerancias requeridas;
- los requisitos para la parada manual;
- los requisitos relativos a la conexión y a la desconexión en el disparo;
- los requisitos para reiniciar el SIS después de una parada;
- la tasa de disparos parásitos máxima admisible;
- los modos de fallo y respuesta deseada del SIS (por ejemplo, alarmas, parada automática);
- cualesquiera requisitos relativos a los procedimientos para arrancar y volver a arrancar el SIS;
- todas las interfaces entre el SIS y cualquier otro sistema (incluyendo el BPCS y los operadores);
- una descripción de los modos de funcionamiento de la planta e identificación de las funciones instrumentadas de seguridad que se requieren para funcionar dentro de cada modo;
- los requisitos de seguridad del software de aplicación tal como se enumeran en el apartado 12.2.2;
- los requisitos para las prioridades / las inhibiciones / los desvíos, incluyendo la forma en que se desactivarán;
- la especificación de cualquier acción necesaria para alcanzar o mantener un estado seguro en el caso de que se declare un fallo o fallos en el SIS. Cualquier acción de este tipo se debe determinar tomando en cuenta todos los factores humanos relevantes;
- el tiempo medio de reparación que sea factible para el SIS, teniendo en cuenta el tiempo de desplazamiento, el lugar, el stock de repuestos, los contratos de servicio, las limitaciones ambientales;
- la identificación de las combinaciones peligrosas de estados de salida del SIS que es necesario evitar;
- se deben identificar los valores extremos de todas las condiciones ambientales que son susceptibles de ser encontradas por el SIS. Esto puede requerir la consideración de los siguientes puntos: temperatura, humedad, contaminantes, puesta a tierra, interferencias electromagnéticas / interferencias de radiofrecuencia (EM/RFI), choques / vibraciones, descargas electrostáticas, clasificación de zonas eléctricas, inundaciones, rayos y otros factores relacionados;
- la identificación de modos normales y anormales para la planta en su conjunto (por ejemplo, arranque de la planta) y procedimientos de funcionamiento individuales de la planta (por ejemplo, mantenimiento de equipos, calibración y/o reparación de sensores). Pueden ser necesarias funciones instrumentadas de seguridad adicionales para dar soporte a estos modos de funcionamiento.

- la definición de los requisitos para cualquier función instrumentada de seguridad necesaria para superar un acontecimiento accidental importante, por ejemplo, el tiempo requerido para que una válvula siga siendo operativa en caso de incendio.

NOTA – El SIS puede realizar funciones instrumentadas que no sean de seguridad para asegurar una parada ordenada o un arranque más rápido. Éstas deberían ser independientes de las funciones instrumentadas de seguridad.

10.3.2 La especificación de los requisitos de seguridad del software debe deducirse de la especificación de los requisitos de seguridad y de la arquitectura escogida para el SIS.

11 DISEÑO E INGENIERÍA DEL SIS

11.1 Objetivo

El objetivo de los requisitos de este capítulo es diseñar un SIS o varios para proporcionar la(s) función(es) instrumentada(s) de seguridad y satisfacer el(los) nivel(es) de integridad de seguridad especificado(s).

11.2 Requisitos generales

11.2.1 El diseño del SIS debe estar de acuerdo con las especificaciones de los requisitos de seguridad del SIS, teniendo en cuenta todos los requisitos de este capítulo.

11.2.2 En los casos en los que el SIS tenga que realizar función(es) instrumentadas tanto de seguridad como de no seguridad, todo el hardware y el software que puedan afectar negativamente a cualquier SIF en condiciones tanto normales como de defecto, se deben tratar como parte del SIS y cumplir con los requisitos del SIL más elevado.

NOTA 1 – En los casos en que sea factible, las funciones instrumentadas de seguridad deberían ser independientes de las funciones instrumentadas que no sean de seguridad.

NOTA 2 – Independencia adecuada significa que ni el fallo de las funciones que no sean de seguridad ni el acceso de programación a las funciones de software que no sean de seguridad sean capaces de causar un fallo peligroso de las funciones instrumentadas de seguridad.

11.2.3 En los casos en los que el SIS ha de realizar funciones instrumentadas de seguridad de diferentes niveles de integridad de seguridad, el hardware y el software comunes compartidos deben satisfacer el nivel de integridad de seguridad más alto a menos que se pueda demostrar que las funciones instrumentadas de seguridad de nivel de integridad de seguridad más bajo no pueden afectar negativamente a las funciones instrumentadas de seguridad de nivel de integridad de seguridad más alto.

11.2.4 Si se pretende no calificar el sistema básico de control de proceso según esta norma, el sistema básico de control de proceso se debe diseñar en forma distinta e independiente de tal manera que no se comprometa la integridad funcional del sistema instrumentado de seguridad.

NOTA 1 – Se puede intercambiar información de funcionamiento pero no debería comprometer la seguridad funcional del SIS.

NOTA 2 – Se pueden usar también dispositivos del SIS para funciones del sistema básico de control de proceso si se puede demostrar que un fallo del sistema básico de control de proceso no compromete las funciones instrumentadas de seguridad del sistema instrumentado de seguridad.

11.2.5 Se deben considerar los requisitos de operatividad, susceptibilidad de mantenimiento y de ensayo durante el diseño del SIS a fin de facilitar la aplicación de requisitos de ergonomía desde el diseño (por ejemplo, dispositivos de desvío para permitir el ensayo y la alarma en línea cuando está activado el desvío).

NOTA – Las instalaciones de mantenimiento y ensayo deberían diseñarse para reducir al mínimo, en la medida de lo posible, la probabilidad de fallos peligrosos que surjan de su uso.

11.2.6 El diseño del SIS debe tener en cuenta las capacidades y limitaciones humanas para la tarea asignada a los operadores y equipo de mantenimiento. El diseño de todas las interfaces hombre-máquina debe seguir la buena práctica ergonómica y debe adaptarse al nivel probable de formación o de sensibilización que deberían recibir los operadores.

11.2.7 El SIS debe ser diseñado de tal manera que una vez se ha colocado el proceso en un estado seguro, debe permanecer en el estado seguro hasta que se inicie una restauración, salvo que se indique otra cosa en las especificaciones de los requisitos de seguridad.

11.2.8 Se deben disponer medios manuales (por ejemplo, un pulsador de parada de emergencia), independientes de la unidad lógica, para accionar los elementos finales del SIS, salvo que se indique otra cosa en las especificaciones de los requisitos de seguridad.

11.2.9 El diseño del SIS debe tener en cuenta todos los aspectos de independencia y dependencia entre el SIS y el BPCS, y entre el SIS y otras capas de protección.

11.2.10 Un dispositivo utilizado para realizar parte de una función instrumentada de seguridad no se debe usar para fines de control de proceso básico, en los casos en los que un fallo de ese dispositivo dé lugar a un fallo de la función de control de proceso básico, lo cual causa una demanda en la función instrumentada de seguridad, salvo que se haya realizado un análisis para confirmar que el riesgo global es aceptable.

NOTA – Cuando una parte del SIS se use también para fines de control de proceso y un fallo del equipo común cause una demanda en la función realizada por el SIS, se introduce un nuevo riesgo. El riesgo adicional depende de la tasa de fallos peligrosos del equipo común, porque si falla el componente compartido, se crearía inmediatamente una demanda a la que el SIS no sería capaz de responder. Por esa razón, será necesario un análisis adicional para asegurarse de que la tasa de fallos peligrosos del equipo compartido es suficientemente baja. Los sensores y válvulas son ejemplos en los que se considera frecuentemente compartir equipo con el BPCS.

11.2.11 Para los subsistemas que en el caso de pérdida de potencia no pasen al estado seguro, se deben satisfacer todos los requisitos siguientes y se debe tomar una acción de acuerdo con el apartado 11.3:

- se detecta la pérdida de integridad de circuito (por ejemplo, supervisión del extremo de línea).
- se asegura la integridad de la alimentación de energía usando una fuente de alimentación auxiliar (por ejemplo, respaldo de batería, fuentes de alimentación ininterrumpida);
- se detecta la pérdida de alimentación de energía al subsistema.

11.3 Requisitos relativos al comportamiento del sistema a la detección de un defecto

11.3.1 La detección de una defecto peligrosa (por ensayos de diagnóstico, ensayos periódicos o por cualquier otro medio) en cualquier subsistema que pueda tolerar una única defecto de hardware debe dar lugar a una de las dos consecuencias indicadas a continuación:

a) una acción especificada para alcanzar o mantener un estado seguro (véase nota); o

b) un funcionamiento seguro continuado del proceso mientras se repara la parte defectuosa. Si la reparación de la parte defectuosa no se completa dentro del tiempo medio de restauración (MTTR) asumido en el cálculo de la probabilidad de fallos aleatorios del hardware, se debe ejecutar una acción especificada para alcanzar o mantener un estado seguro (véase nota).

En los casos en los que las acciones anteriores dependen de que un operador ejecute acciones específicas en respuesta a una alarma (por ejemplo, abrir o cerrar una válvula), la alarma se debe considerar parte del sistema instrumentado de seguridad (es decir, independiente del BPCS).

En los casos en los que las acciones anteriores dependen de que un operador notifique a mantenimiento para reparar un sistema defectuoso en respuesta a una alarma de diagnóstico, la alarma de diagnóstico puede ser una parte del BPCS pero debe ser sometida a los ensayos periódicos apropiados y a la gestión de cambio junto con el resto del SIS.

NOTA – La acción especificada (reacción al defecto) requerida para lograr o mantener un estado seguro debería ser especificada en los requisitos de seguridad (véase el apartado 10.3).Puede consistir, por ejemplo, en la parada segura del proceso o de aquella parte del proceso que se apoya, para la reducción de riesgo, en el subsistema defectuoso u otra planificación de atenuación especificada.

11.3.2 La detección de un defecto peligroso (por ensayo diagnóstico, ensayos periódicos o por cualquier otro medio) en cualquier subsistema que no tenga redundancia y en el cual una función instrumentada de seguridad sea enteramente dependiente (véase nota 1), en el caso en el que el subsistema se use sólo por funcionamiento con función(es) instrumentada(s) de seguridad en el modo por demanda, debe dar lugar a una de las dos consecuencias indicadas a continuación:

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

b) la reparación del subsistema defectuoso dentro del tiempo medio de restauración (MTTR) asumido en el cálculo de la probabilidad de fallos aleatorios del hardware. Durante este tiempo se debe asegurar la seguridad continuada del proceso por medidas y limitaciones adicionales. La reducción de riesgo proporcionada por estas medidas y limitaciones debe ser al menos igual a la reducción de riesgo proporcionada por el sistema instrumentado de seguridad en ausencia de cualesquiera defectos. Las medidas y limitaciones adicionales deben ser especificadas en los procedimientos de operación y mantenimiento del SIS. Si no se efectúa la reparación dentro del tiempo medio de restauración (MTTR) especificado se debe ejecutar una acción especificada para alcanzar o mantener un estado seguro (véase nota 2).

En los casos en los que las acciones anteriores dependen de que un operador ejecute acciones específicas en respuesta a una alarma (por ejemplo, abrir o cerrar una válvula), la alarma se debe considerar parte del sistema instrumentado de seguridad (es decir, independiente del BPCS).

En los casos en los que las acciones anteriores dependen de que un operador notifique a mantenimiento para reparar un sistema defectuoso en respuesta a una alarma de diagnóstico, la alarma de diagnóstico puede ser una parte del BPCS pero debe ser sometida a los ensayos periódicos apropiados y a la gestión de cambio junto con el resto del SIS.

NOTA 1 – Una función instrumentada de seguridad se considera enteramente dependiente de un subsistema si un fallo de este subsistema da lugar a un fallo de la función instrumentada de seguridad en el sistema instrumentado de seguridad que se considera, y la función instrumentada de seguridad no ha sido también asignada a otra capa de protección (véase el capítulo 9).

NOTA 2 – La acción especificada (reacción al defecto) requerida para lograr o mantener un estado seguro debería ser especificada en los requisitos de seguridad (véase el apartado 10.3). Puede consistir, por ejemplo, en la parada segura del proceso o de aquella parte del proceso que se apoya, para la reducción de riesgo, en el subsistema defectuoso u otra planificación de atenuación especificada.

11.3.3 La detección de un defecto peligroso (por ensayo diagnóstico, ensayos periódicos o por cualquier otro medio) en cualquier subsistema que no tenga redundancia y en el cual una función instrumentada de seguridad sea enteramente dependiente (véase nota 1), en el caso de un subsistema que está aplicando cualquier función o funciones instrumentadas de seguridad funcionando en modo continuo (véase nota 2), debe dar lugar a una acción especificada para lograr o mantener un estado seguro.

La acción especificada (reacción al defecto) requerida para lograr o mantener un estado seguro debería ser indicada en la especificación de los requisitos de seguridad. Puede consistir, por ejemplo, en la parada segura del proceso o de aquella parte del proceso que se apoya, para la reducción de riesgo, en el subsistema defectuoso u otra planificación de atenuación especificada. El tiempo total para detectar el defecto y para ejecutar la acción debe ser menor que el tiempo para que se produzca el acontecimiento peligroso.

En los casos en los que las acciones anteriores dependen de que un operador ejecute acciones específicas en respuesta a una alarma (por ejemplo, abrir o cerrar una válvula), la alarma se debe considerar parte del sistema instrumentado de seguridad (es decir, independiente del BPCS).

En los casos en los que las acciones anteriores dependen de que un operador notifique a mantenimiento para reparar un sistema defectuoso en respuesta a una alarma de diagnóstico, la alarma de diagnóstico puede ser una parte del BPCS pero debe ser sometida a los ensayos periódicos apropiados y a la gestión de cambio junto con el resto del SIS.

NOTA 1 – Una función instrumentada de seguridad se considera enteramente dependiente de un subsistema si un fallo de este subsistema da lugar a un fallo de la función instrumentada de seguridad en el sistema instrumentado de seguridad que se considera, y la función instrumentada de seguridad no ha sido también asignada a otra capa de protección.

NOTA 2 – En los casos en los que existe alguna posibilidad de que alguna combinación de estados de salida de un subsistema pueda causar directamente un acontecimiento peligroso, debería ser necesario ver la detección de defectos peligrosos en el subsistema como una función instrumentada de seguridad que funciona en modo continuo.

11.4 Requisitos relativos a la tolerancia a los defectos de hardware

11.4.1 Para las funciones instrumentadas de seguridad, los sensores, unidades lógicas y elementos finales deben tener una tolerancia mínima a los defectos de hardware.

NOTA 1 – La tolerancia a los defectos de hardware es la capacidad de un componente o subsistema para continuar siendo capaz de ejecutar la función instrumentada de seguridad requerida en presencia de una o más defectos peligrosos en el hardware. Una tolerancia a los defectos del hardware de 1 significa que hay, por ejemplo, dos dispositivos y la arquitectura es tal que el fallo peligroso de uno de los dos componentes o subsistemas no impide que se produzca la acción de seguridad.

NOTA 2 – Se ha definido la tolerancia mínima a los defectos del hardware para aliviar imperfecciones potenciales en el diseño de la SIF que pueden dar lugar al número de supuestos realizados en el diseño de la SIF, junto con la incertidumbre en la tasa de fallos de los componentes o subsistemas utilizados en diversas aplicaciones de proceso.

NOTA 3 – Es importante observar que los requisitos relativos a la tolerancia a los defectos del hardware representan la redundancia mínima del componente o subsistema. Dependiendo de la aplicación, la tasa de fallos del componente y del intervalo entre ensayos periódicos, puede ser necesaria una redundancia adicional para satisfacer el SIL de la SIF según el apartado 11.9.

11.4.2 Para unidades lógicas PE, la tolerancia mínima a los defectos del hardware debe ser la mostrada en la tabla 5.

Tabla 5
Tolerancia mínima a los defectos de hardware de las unidades lógicas de electrónica programable (PE)

SIL	Tolerancia mínima a los defectos de hardware		
	SFF < 60%	SFF 60% a 90%	SFF > 90%
1	1	0	0
2	2	1	0
3	3	2	1
4	Se aplican requisitos especiales (véase la Norma IEC 61508)		

11.4.3 Para todos los subsistemas (por ejemplos sensores, elementos finales y unidades lógicas que no sean de PE) excepto las unidades lógicas de PE, la tolerancia mínima a los defectos de hardware debe ser como se muestra en la tabla 6, siempre que el modo de fallo dominante sea el correspondiente al estado seguro o se detecten los fallos peligrosos (véase el apartado 11.3); de otra forma se debe aumentar la tolerancia a los defectos en uno.

NOTA – Para establecer si el modo de fallo dominante es el correspondiente al estado seguro, es necesario considerar cada uno de los siguientes aspectos:

- la conexión de proceso del dispositivo;
- el uso de la información de diagnóstico del dispositivo para validar la señal de proceso;
- el uso del comportamiento de seguridad intrínseca inherente al dispositivo (por ejemplo, ausencia de señal activa, pérdida de alimentación de energía que da lugar a un estado seguro).

11.4.4 Para todos los subsistemas (por ejemplos sensores, elementos finales y unidades lógicas que no sean de PE) excepto las unidades lógicas de PE, la tolerancia mínima a los defectos de hardware especificada en la tabla 6 se puede reducir en uno si los dispositivos usados cumplen con todos los aspectos siguientes:.

- el hardware del dispositivo se selecciona en base a la utilización previa (véase apartado 11.5.3);
- el dispositivo permite sólo el ajuste de los parámetros relativos al proceso; por ejemplo, el intervalo de medida, el sentido del fallo, ascendente o descendente;
- el ajuste de los parámetros relativos al proceso está protegido, por ejemplo mediante barrera de salto, contraseña;
- la función tiene un requisito de SIL inferior a 4.

Tabla 6
Tolerancia mínima a los defectos de hardware de los sensores y elementos finales y de las unidades lógicas distintas de las PE

SIL	Tolerancia mínima a los defectos de hardware (véanse apartados 11.4.3 y 11.4.4)
1	0
2	1
3	2
4	Se aplican requisitos especiales (véase la Norma IEC 61508)

11.4.5 Se pueden usar requisitos alternativos de tolerancia a los defectos con tal de que se haga una evaluación de acuerdo con los requisitos de la Norma IEC 61508-2, tablas 2 y 3.

11.5 Requisitos relativos a la selección de componentes y subsistemas

11.5.1 Objetivos

11.5.1.1 El primer objetivo de este capítulo es especificar los requisitos para la selección de componentes o subsistemas que se van a utilizar como parte de un sistema instrumentado de seguridad.

11.5.1.2 El segundo objetivo de este capítulo es especificar los requisitos para la selección de componentes o subsistemas para permitir a un componente ser integrado en la arquitectura de un SIS.

11.5.1.3 El tercer objetivo de este capítulo es especificar los criterios de aceptación para los componentes y subsistemas en términos de funciones instrumentadas de seguridad y de integridad de seguridad.

11.5.2 Requisitos generales

11.5.2.1 Los componentes y subsistemas seleccionados para su utilización como parte de un sistema instrumentado de seguridad destinado a aplicaciones de SIL 1 a SIL 5 deben estar de acuerdo con las Normas IEC 61508-2 y IEC 61508-3, según proceda, o en otro caso debe cumplir con los apartados 11.4 y 11.5.3 a 11.5.6, según proceda.

11.5.2.2 Los componentes y subsistemas seleccionados para su utilización como parte de un sistema instrumentado de seguridad destinado a aplicaciones de SIL 4 deben estar de acuerdo con las Normas IEC 61508-2 y IEC 61508-3, según proceda.

11.5.2.3 Se debe demostrar la adecuación de los componentes seleccionados mediante la consideración de

- la documentación del fabricante para el hardware y el software integrado;
- si fuera aplicable, la selección de un lenguaje de aplicación y unas herramientas apropiadas (véase el apartado 12.4.4).

11.5.2.4 Los componentes y subsistemas deben ser coherentes con las especificaciones de los requisitos de seguridad del SIS.

NOTA – Para la selección de componentes y subsistemas, siguen aplicándose todos los demás aspectos aplicables de esta norma, incluyendo las limitaciones de arquitectura, la integridad del hardware, el comportamiento en caso de detección de una defecto y el software de aplicación.

11.5.3 Requisitos para la selección de componentes y subsistemas basados en la utilización previa

11.5.3.1 Se debe disponer de evidencias apropiadas de que los componentes y subsistemas son adecuados para su uso en el sistema instrumentado de seguridad.

NOTA 1 – En el caso de elementos de campo, puede haber una amplia experiencia de funcionamiento en aplicaciones de seguridad o no. Se puede usar ésta como base para la evidencia.

NOTA 2 – El nivel de detalle de la evidencia debería estar de acuerdo con la complejidad del componente o subsistema que se considera y con la probabilidad de fallo necesaria para alcanzar el nivel de integridad de seguridad requerido de la(s) función(es) instrumentada(s) de seguridad.

11.5.3.2 Las evidencias de adecuación deben incluir los puntos siguientes:

- consideración de los sistemas del fabricante relativos a calidad, gestión y gestión de la configuración;
- identificación y especificación adecuadas de los componentes o subsistemas;
- demostración de las características de funcionamiento de los componentes o subsistemas en perfiles de funcionamiento y entornos físicos análogos;

  NOTA – En el caso de dispositivos de campo (por ejemplo, sensores y elementos finales) que cumplen una función determinada, esta función es habitualmente idéntica en las aplicaciones de seguridad y en las que no son de seguridad, lo cual significa que el dispositivo actuará de forma similar en ambos tipos de aplicaciones. Por tanto, se debería juzgar también las características de funcionamiento de tales dispositivos en aplicaciones que no sean de seguridad para satisfacer este requisito.

- el volumen de la experiencia de funcionamiento.

  NOTA – En el caso de dispositivos de campo la información relativa a la experiencia en funcionamiento se registra principalmente en la lista del usuario de equipo aprobado para uso en sus instalaciones, basada en un amplio historial de características de funcionamiento satisfactorias en aplicaciones de seguridad y no de seguridad, y en la eliminación de equipos que no den resultados satisfactorios. La lista de dispositivos de campo se puede usar como soporte de declaraciones de experiencia en funcionamiento, siempre que

  - se actualice y supervise la lista regularmente;
  - se añadan los dispositivos de campo únicamente cuando se haya obtenido una experiencia de funcionamiento suficiente;
  - se retiren los dispositivos de campo cuando muestren un historial de características de funcionamiento no satisfactorio;
  - se incluya la aplicación de proceso en la lista en los casos en que sea relevante.

11.5.4 Requisitos para la selección de los componentes y subsistemas programables FPL (por ejemplo, dispositivos de campo) basados en la utilización previa

11.5.4.1 Se aplican los requisitos de los apartados 11.5.2 y 11.5.3.

11.5.4.2 Se deben identificar las características no utilizadas de los componentes y subsistemas en la evidencia de adecuación, y se debe establecer que no son susceptibles de perjudicar las funciones instrumentadas de seguridad.

11.5.4.3 Para la configuración específica y perfil operacional del hardware y del software, la prueba de adecuación debe considerar

- las características de las señales de entrada y salida;
- los modos de utilización;
- las funciones y configuraciones utilizadas;
- el uso previo en aplicaciones y entornos físicos similares.

11.5.4.4 Para las aplicaciones de SIL 3, se debe realizar una evaluación formal (de acuerdo con el apartado 5.2.6.1) del dispositivo FPL para demostrar que

- el dispositivo de FPL es capaz tanto de realizar las funciones requeridas como que el uso previo ha demostrado que existe una baja probabilidad de que falle de una manera que pudiera conducir a un acontecimiento peligroso cuando se use como parte de un sistema instrumentado de seguridad, debido a fallos aleatorios del hardware o a defectos sistemáticos del hardware o del software;

- se han aplicado normas apropiadas para el hardware y el software;

- se ha usado o ensayado el dispositivo FPL en configuraciones representativas de los perfiles operacionales a los que se destina.

11.5.4.5 Para las aplicaciones de SIL 3, se debe disponer de un manual de seguridad que incluya las limitaciones de operación, mantenimiento y detección de defectos, cubriendo las configuraciones típicas del dispositivo FPL y los perfiles operacionales a los que se destina.

11.5.5 Requisitos para la selección de los componentes y subsistemas programables LVL (por ejemplo, unidades lógicas) basados en la utilización previa

11.5.5.1 Sólo se pueden aplicar los requisitos siguientes a las unidades lógicas PE usadas en sistemas instrumentados de seguridad que realizan funciones instrumentadas de seguridad SIL 1 ó SIL 2.

11.5.5.2 Se aplican los requisitos del apartado 11.5.4.

11.5.5.3 En los casos en los que exista cualquier diferencia entre los perfiles operacionales y los entornos físicos de un componente o subsistema experimentado previamente, y el perfil operacional y el entorno físico del componente o subsistema cuando se usa dentro del sistema instrumentado de seguridad, se deben identificar cualesquiera diferencias de este tipo y se debe realizar una evaluación basada en análisis y ensayos, según sea apropiado, para demostrar que la probabilidad de defectos sistemáticos cuando se use en el sistema instrumentado de seguridad es suficientemente baja.

11.5.5.4 Se debe determinar la experiencia en funcionamiento considerada necesaria para justificar la adecuación teniendo en cuenta:

- el SIL de la función instrumentada de seguridad;

- la complejidad y funcionalidad del componente o subsistema.

NOTA – Véase la Norma IEC 61511-2 para guía adicional.

11.5.5.5 Para las aplicaciones de SIL 1 ó 2, se puede usar una unidad lógica de PE configurada para la seguridad siempre que se satisfagan las disposiciones adicionales siguientes:

- comprensión de los modos de fallo peligrosos;

- uso de técnicas para configuración de seguridad que traten los modos de fallo identificados;

- software integrado que tenga un buen historial de uso en aplicaciones de seguridad;

- protección contra modificaciones no autorizadas o fortuitas.

NOTA – Una unidad lógica de PE configurada para la seguridad es una unidad lógica de grado PE para uso industrial general que esté específicamente configurada para su uso en aplicaciones de seguridad.

11.5.5.6 Se debe realizar una evaluación formal (de acuerdo con el apartado 5.2.6.1) para cualquier unidad lógica usada en una aplicación de SIL 2, a fin de demostrar que

- es capaz de realizar las funciones requeridas y en uso previo ha demostrado que existe una probabilidad suficientemente baja de que falle de una manera que pueda provocar un acontecimiento peligroso cuando se use como parte de un sistema instrumentado de seguridad, debido bien a fallos aleatorios del hardware o bien a defectos sistemáticos del hardware o del software;

- se aplican medidas para detectar defectos durante la ejecución del programa e iniciar la reacción apropiada; estas medidas deben comprender todos los puntos siguientes:

  – supervisión de la secuencia del programa;

  – protección por código contra las modificaciones o detección de fallos por supervisión en línea;

  – programación por afirmación o diversidad;

  – verificación del intervalo de las variables o verificación de la verosimilitud de los valores;

  – enfoque modular;

  – se han utilizado las normas de codificación apropiadas para el software integrado y utilitario;

  – se ha ensayado en configuraciones típicas, con casos de ensayo representativos de los perfiles operacionales previstos;

  – se han usado módulos de software y componente verificados de confianza;

  – el sistema ha experimentado análisis y ensayos dinámicos;

  – el sistema no usa inteligencia artificial ni reconfiguración dinámica;

  – se ha realizado ensayos de inserción de defectos documentados.

11.5.5.7 Se debe disponer, para las aplicaciones de SIL 2, de un manual de seguridad que incluya las limitaciones de operación, mantenimiento y detección de defectos cubriendo las configuraciones típicas de la unidad lógica de PE y los perfiles operacionales a que se destina.

11.5.6 Requisitos para la selección de los componentes y subsistemas programables FVL (por ejemplo, unidades lógicas)

11.5.6.1 Cuando se programan las aplicaciones usando un FVL, la unidad lógica PE debe estar de acuerdo con la Norma IEC 61508-2 y IEC 61508-3.

11.6 Dispositivos de campo

11.6.1 Se debe seleccionar e instalar los dispositivos de campo de forma que se reduzcan al mínimo los fallos que pudieran dar lugar a información imprecisa debido a las condiciones que surgen del proceso y a las condiciones ambientales. Las condiciones que se deberían considerar incluyen la corrosión, la congelación de los materiales de las tuberías, los sólidos en suspensión, la polimerización, la cocción, los valores extremos de temperatura y presión, la condensación en los tramos secos de las líneas de impulso y la condensación insuficiente en los tramos húmedos de las líneas de impulso.

11.6.2 La excitación para el disparo en circuitos de entrada/salida discretos debe aplicar un método para asegurarse de la integridad del circuito y de la alimentación de potencia;

NOTA – Un ejemplo de un método de este tipo es un monitor de extremo de línea, en el que se monitoriza continuamente una corriente piloto para asegurar la continuidad del circuito y en el que la corriente piloto no es de suficiente magnitud para afectar el funcionamiento de I/O.

11.6.3 Cada dispositivo de campo individual debe tener su propio cableado dedicado a la entrada/salida del sistema, excepto en los casos siguientes.

- Varios sensores discretos se conectan en serie a una única entrada y todos los sensores supervisan el mismo estado del proceso (por ejemplo, las sobrecargas del motor).
- Se conectan varios elementos finales a una única salida.

  NOTA – Para dos válvulas conectadas a una salida, se requiere que ambas válvulas cambien de estado a la vez para todas las funciones instrumentadas de seguridad que usan ambas válvulas.

- Una comunicación por bus digital con características de seguridad globales que satisface los requisitos de integridad de la SIF a la que da servicio.

11.6.4 Los sensores inteligentes deben ser protegidos en escritura para evitar la modificación inadvertida desde un emplazamiento remoto, salvo que una revisión de seguridad apropiada permita el uso de la lectura/escritura. La revisión debería tener en cuenta factores humanos tales como los fallos en la trazabilidad de los procedimientos.

11.7 Interfaces

Las interfaces hombre máquina y de comunicación con el SIS pueden incluir, sin limitarse a ellas:

- la interfaz o interfaces de operador;
- la interfaz o interfaces de mantenimiento de ingeniería;
- la interfaz o interfaces de comunicación.

11.7.1 Requisitos relativos a la interfaz de operador

11.7.1.1 En los casos en los que la interfaz de operador del SIS se hace a través de la interfaz de operador del BPCS, se deben tener en cuenta los fallos previsibles que pueden producirse en la interfaz de operador del BPCS.

11.7.1.2 El diseño del SIS debe reducir al mínimo la necesidad de que el operador seleccione opciones y la necesidad de desviar el sistema mientras la unidad se encuentre en marcha. Si el diseño no requiere el uso de acciones del operador, el diseño debería incluir instalaciones para la protección contra errores de operador.

NOTA – Si el operador tiene que seleccionar una opción determinada debería haber una etapa de confirmación por repetición.

11.7.1.3 Se deben proteger los interruptores de desvío mediante enclavamientos con candados o contraseñas para impedir el uso no autorizado.

11.7.1.4 La información sobre el estado del SIS que sea crítica para el mantenimiento del SIS debe encontrarse disponible como parte de la interfaz de operador. Esta información puede incluir:

- donde está el proceso en su secuencia;
- la indicación de que ha tenido lugar una acción de protección del SIS;
- la indicación de que ha sido desviada una función de protección;
- la indicación de que ha tenido lugar una acción(es) automática(s) tal como la degradación del voto mayoritario y/o el tratamiento de el defecto;
- el estado de los sensores y elementos finales;
- la pérdida de energía en los casos en los que las pérdidas de energía tienen un impacto en la seguridad;

- los resultados de los diagnósticos;
- el fallo de los equipos de acondicionamiento ambiental que sean necesarios para dar soporte al SIS.

11.7.1.5 El diseño de la interfaz de operador del SIS debe ser tal que impida los cambios del software de aplicación del SIS. En los casos en los que se necesite transmitir la información de seguridad desde el BPCS al SIS se deberían usar sistemas que puedan permitir selectivamente escribir desde el BPCS a variables específicas del SIS. Se deberían aplicar equipos o procedimientos para confirmar que se ha transmitido la selección apropiada y ha sido recibida por el SIS y no compromete la funcionalidad de seguridad del SIS.

NOTA 1 – Si se seleccionan opciones o desvíos en el BPCS y se descargan en el SIS, los fallos del BPCS pueden interferir la capacidad del SIS para funcionar bajo demanda. Si puede ocurrir esto, el BPCS se convertirá en un sistema relacionado con la seguridad.

NOTA 2 – En los procesos discontinuos se puede usar un SIS para seleccionar diferentes puntos de ajuste o funciones lógicas dependiendo de la fórmula que se use. En estos casos se puede usar la interfaz de operador para efectuar la selección requerida.

NOTA 3 – La entrega de información incorrecta procedente del BPCS al SIS no debe comprometer la seguridad.

11.7.2 Requisitos relativos a la interfaz de mantenimiento / ingeniería

11.7.2.1 El diseño de la interfaz de mantenimiento / ingeniería del SIS de PE debe asegurar que cualquier fallo de esta interfaz no debe afectar adversamente a la capacidad del SIS para llevar el proceso a un estado seguro. Esto puede requerir desconectar las interfaces de mantenimiento / ingeniería, tales como paneles de programación, durante el funcionamiento normal del SIS.

11.7.2.2 La interfaz de mantenimiento / ingeniería debe proporcionar las funciones siguientes con protección de seguridad de acceso a cada una

- modo de funcionamiento del SIS, datos, medios de desactivar la comunicación de alarma, ensayo, desvío, mantenimiento;
- diagnóstico del SIS, servicios de voto y tratamiento de defectos;
- añadir, borrar o modificar el software de aplicación;
- datos necesarios para solucionar averías del SIS;
- en los casos en los que se requieren desvíos, se deberían instalar de tal modo que no se desactiven las alarmas ni los dispositivos manuales de parada.

NOTA – Los aspectos referentes al software son sólo aplicables a los SIS que usen tecnología PE.

11.7.2.3 La interfaz de mantenimiento / ingeniería no se debe usar como interfaz de operador.

11.7.2.4 La activación y la desactivación del acceso a la lectura / escritura sólo se deben realizar mediante una configuración o un proceso de programación que use la interfaz de mantenimiento/ingeniería con la documentación y las medidas de seguridad apropiadas.

11.7.3 Requisitos relativos a la interfaz de comunicación

11.7.3.1 El diseño de la interfaz de comunicación del SIS debe asegurar que cualquier fallo de la interfaz de comunicación no debe afectar adversamente la capacidad del SIS para llevar el proceso a un estado seguro.

11.7.3.2 El SIS debe ser capaz de comunicarse con el BPCS y los periféricos sin impacto en la SIF.

11.7.3.3 La interfaz de comunicación debe ser suficientemente robusta para resistir las interferencias electromagnéticas, incluyendo las sobretensiones, sin causar un fallo peligroso de la SIF.

11.7.3.4 La interfaz de comunicación debe ser adecuada para la comunicación entre los dispositivos referenciados a diferentes potenciales eléctricos de puesta a tierra.

NOTA – Puede ser necesario un medio alternativo (por ejemplo, fibra óptica).

11.8 Requisitos relativos al mantenimiento o al diseño de los ensayos

11.8.1 El diseño debe permitir el ensayo del SIS en su conjunto o por partes. En los casos en los que el intervalo entre paradas de proceso programadas sea mayor que el intervalo entre los ensayos periódicos se requieren instalaciones de ensayo en línea.

NOTA – El término "en su conjunto" significa desde el fluido de proceso en el extremo del sensor al fluido de proceso en el extremo de actuación.

11.8.2 En los casos en los que se requieran ensayos en línea, las instalaciones de ensayo deben ser una parte integrante del diseño del SIS para ensayar los fallos no detectados.

11.8.3 Cuando se incluyan instalaciones de ensayo y/o desvío en el SIS, deben satisfacer los puntos siguientes:

- Se debe diseñar el SIS de acuerdo con los requisitos de mantenimiento y ensayos definidos en las especificaciones de los requisitos de seguridad.

- Se debe alertar al operador ante el desvío de cualquier parte del SIS mediante una alarma y/o un procedimiento operacional.

11.8.4 No se debe usar el forzado de entradas y salidas de un SIS de PE como parte de

- un software de aplicación;

- procedimiento(s) operacional(es);

- mantenimiento, excepto lo abajo indicado.

El forzado de entradas y salidas sin retirar de servicio el SIS no se debe permitir a menos que vaya acompañado de procedimientos y una seguridad de acceso. Cualquier forzado de este tipo debe ser anunciado o ser objeto de una alarma, según proceda.

11.9 Probabilidad de fallo de la SIF

11.9.1 La probabilidad de fallo por demanda de cada función instrumentada de seguridad debe ser igual o menor que la medida de fallos objetivo como se indica en las especificaciones de los requisitos de seguridad. Esto se debe verificar por cálculo.

NOTA 1 – En el caso de funciones instrumentadas de seguridad que funcionen en el modo por demanda, la medida de fallos objetivo se debería expresar en términos de la probabilidad media de fallos para realizar la función de diseño por demanda, como se determina por el nivel de integridad de seguridad de la función instrumentada de seguridad (véase la tabla 3).

NOTA 2 – En el caso de una función instrumentada de seguridad que funcione en el modo continuo, la medida de fallos objetivo se debería expresar en términos de la frecuencia de un fallo peligroso por hora, como se determina por el nivel de integridad de seguridad de la función instrumentada de seguridad (véase la tabla 4).

NOTA 3 – Es necesario cuantificar la probabilidad de fallos separadamente para cada función instrumentada de seguridad porque podrían ser aplicables modos de fallo de componentes diferentes y la arquitectura del SIS (en términos de redundancia) puede variar también.

NOTA 4 – La medida objetivo de fallos puede ser un valor especificado de probabilidad media de fallos por demanda o tasa de fallos peligrosos deducida de un análisis cuantitativo o el intervalo especificado asociado con el SIL si ha sido determinado por métodos cualitativos.

11.9.2 La probabilidad calculada de fallos de cada función instrumentada de seguridad debida a fallos del hardware debe tener en cuenta

a) la arquitectura del SIS en cuanto se refiere a cada función instrumentada de seguridad que se considera;

b) la tasa de fallos estimada de cada subsistema, debida a los defectos aleatorias del hardware, en cualquier modo, que causarían un fallo peligroso del SIS pero que no son detectados por los ensayos de diagnóstico;

c) la tasa de fallos estimada de cada subsistema, debida a los defectos aleatorias del hardware, en cualquier modo, que causarían un fallo peligroso del SIS que son detectados por los ensayos de diagnóstico;

NOTA – Las tasas estimadas de fallos de un subsistema se pueden determinar por un análisis de modos de fallo cuantificado usando datos de fallos de un componente o subsistema procedentes de una fuente reconocida de la industria o de la experiencia del uso previo del subsistema en el mismo entorno que para la aplicación a la que se destina, y en el cual la experiencia es suficiente para demostrar el tiempo medio hasta el fallo que se declara sobre una base estadística con un límite inferior de confianza monolateral del 70% como mínimo.

d) la susceptibilidad del SIS a los fallos de causa común;

e) la cobertura de diagnóstico de cualesquiera ensayos periódicos de diagnóstico (determinada según la Norma IEC 61511-2), el intervalo de los ensayos de diagnóstico asociado y la fiabilidad de las instalaciones de diagnóstico;

f) los intervalos a los cuales se realizan los ensayos periódicos;

g) los tiempos de reparación para los fallos detectados;

h) la tasa estimada de fallos peligrosos de cualquier proceso de comunicación en cualesquiera modos que causaría un fallo peligroso del SIS (tanto detectado como no detectado por los ensayos de diagnóstico);

i) la tasa estimada de fallos peligrosos de cualquier respuesta humana en cualesquiera modos que causaría un fallo peligroso del SIS (tanto detectados como no detectados por los ensayos de diagnóstico);

j) la susceptibilidad a las perturbaciones electromagnéticas (por ejemplo, según la Norma IEC 61326-1);

k) la susceptibilidad a las condiciones climáticas y mecánicas (por ejemplo, según las Normas IEC 60654-1 e IEC 60654-3);

NOTA 1 – Se dispone de métodos de modelización y corresponde al analista determinar el método más apropiado, que debería depender de las circunstancias. Los métodos disponibles incluyen (véase la Norma IEC 61508-6, anexo B)

- la simulación;
- el análisis causa-efecto;
- el análisis del árbol de defectos;
- los modelos de Markov;
- los diagramas de bloques de fiabilidad.

NOTA 2 – El intervalo entre ensayos diagnósticos, así como el tiempo de reparación subsiguiente constituyen el tiempo medio para restauración (véase VEI 191-13-08) que se debería considerar en el modelo de fiabilidad.

12 REQUISITOS RELATIVOS AL SOFTWARE DE APLICACIÓN, INCLUYENDO LOS CRITERIOS DE SELECCIÓN PARA EL SOFTWARE UTILITARIO

Este capítulo reconoce

– tres tipos de software:

  • software de aplicación;

  • software utilitario, es decir, las herramientas de software para desarrollar y verificar el software de aplicación;

  • software integrado, es decir, el software suministrado como parte del PE;

– tres tipos de lenguaje de desarrollo de software:

  • lenguajes de desarrollo fijado (FPL);

  • lenguajes de variabilidad limitada (LVL);

  • lenguajes de variabilidad total (FVL).

Esta norma se limita al software de aplicación desarrollado usando FPL o LVL. Los siguientes requisitos son adecuados para el desarrollo y la modificación del software de aplicación hasta el SIL 3. Por tanto esta norma no diferencia entre SIL 1, 2 y 3.

El desarrollo y modificación del software de aplicación que usa FPL o LVL hasta SIL 3 debe cumplir con esta norma. El desarrollo y modificación del software de aplicación SIL 4 debe cumplir con la Norma IEC 61508. El desarrollo y modificación del software de aplicación que usa FVL debe cumplir con la Norma IEC 61508.

El software utilitario (junto con el manual de seguridad del fabricante que define cómo se puede aplicar el sistema PE con seguridad) se debe seleccionar y aplicar en conformidad con los requisitos del apartado 12.4.4. La selección del software integrado debe cumplir con el apartado 11.5.

12.1 Requisitos de ciclo de vida de seguridad del software de aplicación

12.1.1 Objetivos

12.1.1.1 Los objetivos de este capítulo son:

• definir las actividades requeridas para desarrollar el software de aplicación para cada subsistema SIS programado;

• definir como seleccionar, controlar, y aplicar el software de utilización usado para desarrollar el software de aplicación;

• asegurar que existe una planificación adecuada de forma que se cumplen los objetivos de seguridad asignados a la aplicación.

NOTA – La figura 10 ilustra el objeto del capítulo 12 dentro del ciclo de vida de seguridad.

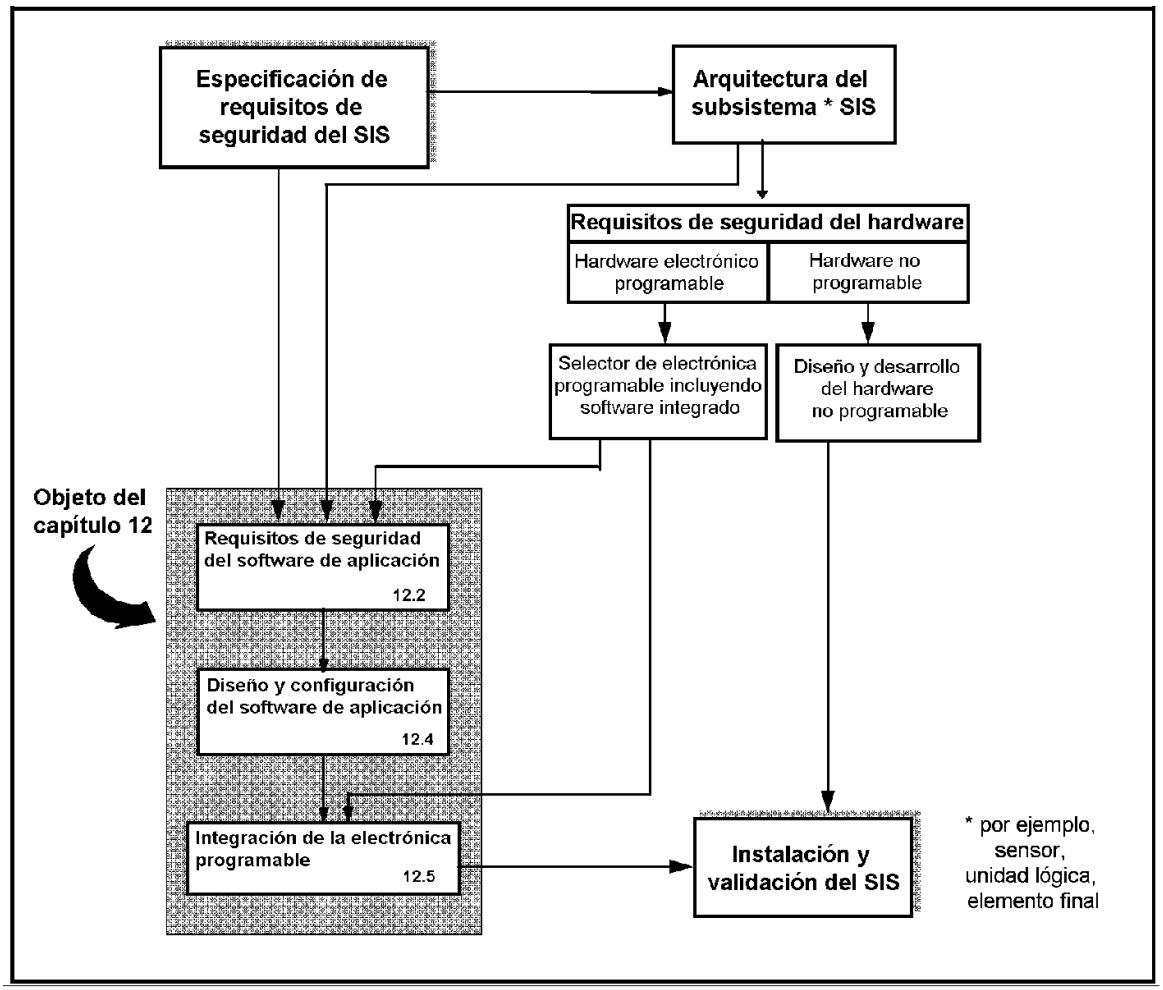


Fig. 10 – Ciclo de vida de seguridad del software de aplicación y su relación con el ciclo de vida de seguridad del SIS

12.1.2 Requisitos

12.1.2.1 Se debe especificar un ciclo de vida de seguridad para el desarrollo de la aplicación que satisfaga los requisitos de este capítulo durante la planificación de la seguridad y debe ser integrado con el ciclo de vida de seguridad del SIS.

12.1.2.2 Se debe definir cada fase del ciclo de vida de seguridad de la aplicación en términos de las actividades elementales, objetivos, información de entrada requerida y resultados de salida, requisitos de verificación (véase apartado 12.7) y responsabilidades (véase la tabla 7 y la figura 11).

NOTA 1 – Siempre que el ciclo de vida del software de aplicación satisfaga los requisitos de la tabla 7, es aceptable adaptar la profundidad, número y tamaño de las fases del modelo en V (véase la figura 12) para tener en cuenta la integridad de seguridad y la complejidad del proyecto.

NOTA 2 – El tipo de lenguaje de software utilizado (FPL, LVL, o FVL) y la adecuación del lenguaje a las funciones de la aplicación pueden repercutir en el objeto del modelo en V.

NOTA 3 – Se pueden incluir las especificaciones de los requisitos de seguridad del software de aplicación como parte de las especificaciones de los requisitos de seguridad del SIS.

NOTA 4 – Se pueden incluir el plan de validación del software de aplicación como parte del plan de validación general del SIS o del subsistema del SIS.

12.1.2.3 El dispositivo de PE que realiza el software de aplicación debe ser adecuado para la integridad de seguridad requerida por cada SIF a la que da servicio.

12.1.2.4 Para cada fase del ciclo de seguridad, se deben seleccionar y aplicar los métodos, técnicas y herramientas de forma que

- se reduzca al mínimo el riesgo de introducir defectos en el software de aplicación;
- se revelen y eliminen los defectos que existen ya en el software;
- se asegure que los defectos remanentes en el software no conducirán a resultados inaceptables;
- se asegure que se puede mantener el software durante toda la vida del SIS;
- se demuestre que el software tiene la calidad requerida.

NOTA – La selección de los métodos y técnicas debería depender de las circunstancias específicas. Los factores para esta decisión son susceptibles de incluir:

  – la cantidad de software;
  – el grado de complejidad;
  – el nivel de integridad de seguridad del SIS;
  – las consecuencias en caso de fallo;
  – el grado de normalización de los elementos de diseño.

12.1.2.5 Se debe verificar cada fase del ciclo de vida de seguridad del software de aplicación (véase el apartado 12.7) y se deben hacer disponibles los resultados (véase el capítulo 19).

12.1.2.6 Si en cualquier etapa del ciclo de vida de seguridad del software de aplicación se requiere un cambio que corresponde a una fase anterior del ciclo de vida, entonces se debe reexaminar la fase anterior del ciclo de vida de seguridad y las fases siguientes y, si se requieren cambios, repetir y volverlas a verificar.

12.1.2.7 El software de aplicación, le hardware del SIS y el software integrado y el software utilitario (herramientas) deben ser sometidos a la gestión de configuración (véase apartado 5.2.7).

12.1.2.8 Se debe realizar la planificación de los ensayos. Se deberían tratar los puntos siguientes:

- la política para la integración del software y el hardware;
- los casos de ensayo y los datos de ensayo;
- los tipos de ensayos a realizar;
- el entorno del ensayo, incluyendo las herramientas, el software de soporte y la descripción de la configuración;
- los criterios de ensayo con los cuales se juzgará el final de los ensayos;
- el(los) emplazamiento(s) físico(s) (por ejemplo, fábrica o en instalación);
- la dependencia de la funcionalidad externa;
- el personal apropiado;
- las no conformidades.

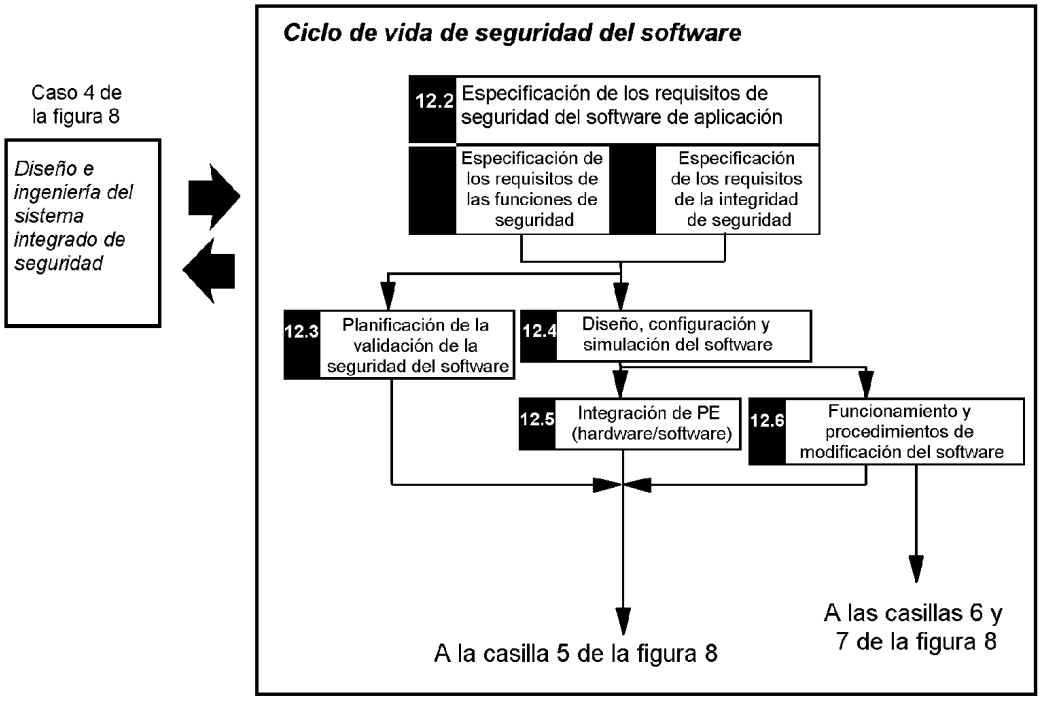


Fig. 11 – Ciclo de vida de seguridad del software de aplicación (en fase de realización)

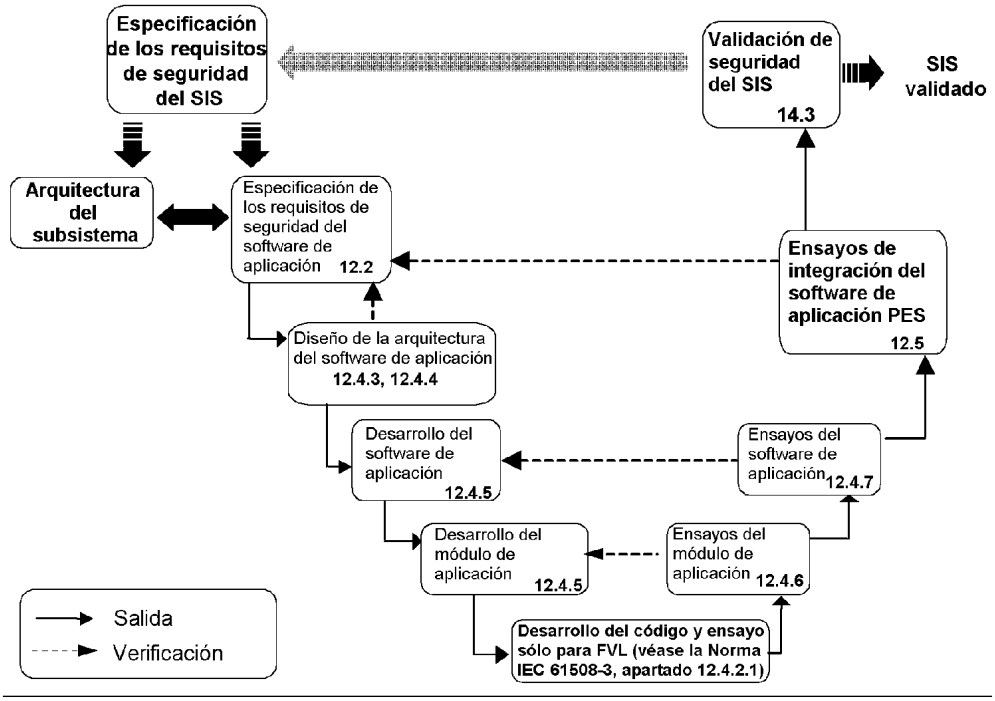


Fig. 12 – Ciclo de vida de desarrollo del software (modelo en V)

Tabla 7 *(Continuación)*
Ciclo de vida de seguridad del software de aplicación: vista de conjunto

Fases del ciclo de vida de seguridad		Objetivos	Apartado de los requisitos	Información requerida	Resultados requeridos
Número de casilla de la figura 11	**Título**				
12.2	Especificación de los requisitos de seguridad del software de aplicación	Especificar los requisitos de seguridad del software de las funciones instrumentadas de seguridad para cada función del SIS necesaria para realizar las funciones instrumentadas de seguridad requeridas. Especificar los requisitos para la integridad de seguridad del software de cada una de las funciones instrumentadas de seguridad asignadas a ese SIS	12.2.2	Especificación de los requisitos de seguridad del SIS Manuales de seguridad del SIS seleccionado Arquitectura del SIS	Especificación de los requisitos de seguridad del software de aplicación del SIS Información de verificación
12.3	Planificación de la validación de seguridad del software de aplicación	Desarrollar un plan para validar el software de aplicación	12.3.2	Especificación de los requisitos de seguridad del software de aplicación del SIS	Plan de validación del software de aplicación del SIS Información de verificación
12.4	Diseño y desarrollo del software de aplicación	Arquitectura Crear una arquitectura de software que cumpla los requisitos especificados para la seguridad del software Revisar y evaluar los requisitos impuestos al software por la arquitectura del hardware del SIS	12.4.3	Especificación de los requisitos de seguridad del software de aplicación del SIS Manuales de diseño de la arquitectura del hardware del SIS	Descripción del diseño de la arquitectura, por ejemplo, segregación de l software de aplicación en subsistemas relativos al proceso y al (a los) SIL, por ejemplo, reconocimiento de módulos de software de aplicación común tales como secuencias de bombas y válvulas Arquitectura del software de aplicación y especificación de ensayo de la integración de subsistemas Información de verificación

(Continúa)

Tabla 7
Ciclo de vida de seguridad del software de aplicación: vista de conjunto

Fases del ciclo de vida de seguridad		Objetivos	Apartado de los requisitos	Información requerida	Resultados requeridos
Número de casilla de la figura 11	**Título**				
12.4	Diseño y desarrollo del software de aplicación	Herramientas de soporte y lenguajes de programación. Identificar un conjunto adecuado de herramientas de configuración, biblioteca, gestión, simulación y ensayo para el conjunto del ciclo de vida de seguridad del software (software utilitario) Especificar los procedimientos para el desarrollo del software de aplicación	12.4.4	Especificación de los requisitos de seguridad del software de aplicación del SIS Descripción del diseño de la arquitectura Manuales del SIS Manual de seguridad de la unidad lógica del SIS seleccionada	Lista de procedimientos para el uso del software utilitario Información de verificación
12.4	Diseño y desarrollo del software de aplicación	Desarrollo del software de aplicación y desarrollo del módulo de aplicación Realización del software de aplicación que cumple los requisitos especificados para la seguridad de la aplicación	12.4.5	Descripción del diseño de la arquitectura Lista de manuales y procedimientos del PES seleccionado para su uso en el software utilitario	1) Programa del software de aplicación (por ejemplo, diagramas de bloques de las funciones, escalera lógica) 2) Simulación del programa de aplicación y ensayo de integración 3) Especificación de los requisitos de seguridad del software de aplicación para fines específicos 4) Información de verificación
12.4	Desarrollo del programa de aplicación usando lenguajes de variabilidad total	Desarrollo de programa y ensayo – sólo FVL Implantar el lenguaje de variabilidad total que cumple los requisitos especificados para la seguridad del software	12.4.6 y 12.4.7	Especificación de los requisitos de seguridad del software de aplicación para fines específicos	Se refiere a la Norma IEC 61508-3

(Continúa)

Tabla 7 *(Fin)*
Ciclo de vida de seguridad del software de aplicación: vista de conjunto

Fases del ciclo de vida de seguridad		Objetivos	Apartado de los requisitos	Información requerida	Resultados requeridos
Número de casilla de la figura 11	**Título**				
12.4	Diseño y desarrollo del software de aplicación	Ensayo del software de aplicación 1) verificar que se han cumplido los requisitos de seguridad del software 2) Mostrar que todos los programas de aplicación, los subsistemas y los sistemas interactúan correctamente para realizar las funciones a las que se destinan y no realizan funciones imprevistas Se puede juntar con la fase siguiente (12.5) sujeto a una cobertura de ensayo satisfactoria	12.4.6, 12.4.7, 12.7	Especificación de simulación de programa de aplicación y ensayo de integración (ensayos basados en estructura) Especificación de ensayo de integración de arquitectura de software	1) Resultados de ensayo de software 2) Sistema de software verificado y ensayado 3) Información de verificación
12.5	Integración de la electrónica programable (hardware y software)	Integrar el software en el hardware de electrónica programable objetivo	12.5.2	Especificación del ensayo de integración del software y del hardware	Resultados del ensayo de integración del software y del hardware Software y hardware verificados
12.3	Validación del SIS	Validar que el SIS (incluyendo el software de aplicación de seguridad satisface los requisitos de seguridad	12.3	Planes de validación de seguridad del software y del SIS	Información de verificación

12.2 Especificación de los requisitos de seguridad del software de aplicación

NOTA – Esta fase corresponde a la casilla 12.2 de la figura 11.

12.2.1 Objetivo

12.2.1.1 El objetivo de este capítulo es proporcionar requisitos para la especificación de los requisitos de seguridad del software de aplicación para cada subsistema programable del SIS necesario para realizar la(s) función(es) instrumentada(s) de seguridad necesarias, coherentes con la arquitectura del SIS.

NOTA – Véase la figura 13 que muestra la relación de arquitectura entre el hardware y el software.

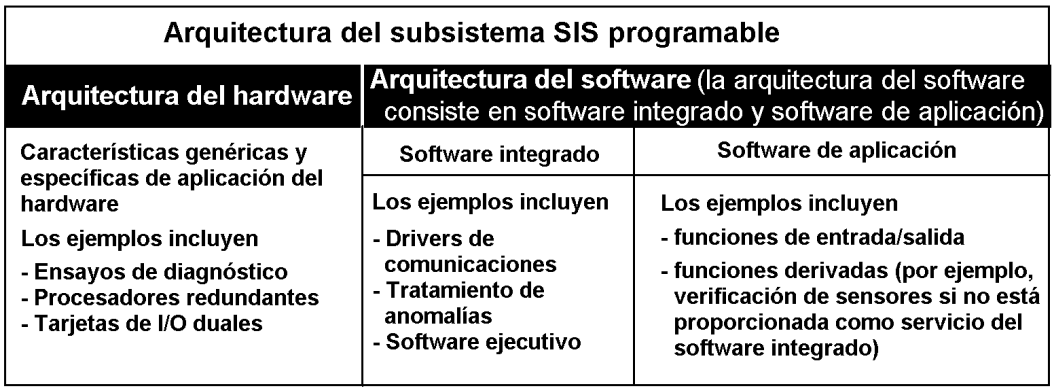


Fig. 13 – Relación entre las arquitecturas del hardware y del software del SIS

12.2.2 Requisitos

12.2.2.1 Se debe desarrollar una especificación de los requisitos de seguridad del software de aplicación.

NOTA 1 – Un SIS consiste generalmente en tres subsistemas de arquitectura: los sensores, la unidad lógica y los elementos finales. Además los subsistemas podrían tener dispositivos redundantes para lograr el nivel de integridad requerido.

NOTA 2 – Una arquitectura del hardware del SIS con sensores redundantes puede plantear requisitos adicionales a la unidad lógica del SIS (por ejemplo, aplicación de la lógica 1oo2).

NOTA 3 – Los requisitos de seguridad del software del subsistema del SIS que hayan sido ya especificados en los requisitos del SIS (véase capítulo 10) no necesitan ser repetidos.

NOTA 4 – Se requiere una especificación de los requisitos de seguridad del software para identificar las capacidades mínimas de la funcionalidad del software de PE y también para limitar la selección de cualquier funcionalidad que daría lugar a un estado inseguro.

12.2.2.2 La entrada a la especificación de los requisitos de seguridad del software para cada subsistema del SIS debe incluir

a) los requisitos de seguridad especificados de la SIF;

b) los requisitos resultantes de la arquitectura del SIS; y

c) cualesquiera requisitos de la planificación de la seguridad (véase el capítulo 5).

NOTA 1 – Esta información debería hacerse disponible al desarrollador del software de aplicación.

NOTA 2 – Este requisito no significa que no debería haber interacción entre el desarrollador de la arquitectura del SIS, la organización responsable de la configuración de los dispositivos y el desarrollador del software de aplicación. Conforme los requisitos de seguridad del software de aplicación y la arquitectura del software de aplicación posible (véase el apartado 12.4.3) se hacen más precisos, puede haber un impacto sobre la arquitectura del hardware del SIS y, por esta razón, es esencial una cooperación estrecha entre el desarrollador de la arquitectura del SIS, el proveedor del subsistema del SIS y el desarrollador del software de aplicación (véase la figura 5).

12.2.2.3 La especificación de los requisitos para la seguridad del software de aplicación debe ser suficientemente detallada para permitir que el diseño y la realización alcancen la integridad de seguridad requerida y para permitir que se lleve a cabo una evaluación de la seguridad funcional. Se deben considerar los puntos siguientes:

- las funciones a las que da soporte el software de aplicación;
- las características de capacidad y tiempo de respuesta;
- las interfaces del equipo y del operador y su eficacia operacional;

- todos los modos de funcionamiento del proceso relevantes tal como se indican en la especificación de requisitos de seguridad del SIS;
- las acciones a tomar respecto a las variables erróneas del proceso tales como valores de sensor fuera del intervalo, un circuito abierto detectado, un cortocircuito detectado;
- los ensayos periódicos y los ensayos de diagnóstico de los dispositivos externos (por ejemplo, sensores y elementos finales);
- la supervisión del software por sí mismo (por ejemplo, incluye perros guardianes activados por la aplicación y validación de intervalo de datos);
- la supervisión de otros dispositivos dentro del SIS (por ejemplo, sensores y elementos finales);
- la activación de los ensayos periódicos de las funciones instrumentadas de seguridad cuando el proceso esté operativo;
- las referencias a los documentos de entrada (por ejemplo, especificación de la SIF, configuración o arquitectura del SIS, requisitos de integridad de seguridad del SIS).

12.2.2.4 El desarrollador del software de aplicación debe revisar la información de la especificación para asegurar que los requisitos no son ambiguos, son coherentes y entendibles. Se debe identificar cualquier deficiencia de los requisitos de seguridad especificados al desarrollador del subsistema del SIS.

12.2.2.5 Los requisitos especificados para la seguridad del software se deberían expresar y estructurar de tal manera que

- sean claros para aquellos que utilizarán el documento en cualquier etapa del ciclo de vida de seguridad del SIS; esto incluye el uso de terminología y descripciones que sean claras y entendidas por los operadores de la planta y los mantenedores así como por los programadores de la aplicación.
- sean verificables, ensayables, modificables;
- se les pueda trazar hasta la especificación de los requisitos de seguridad del SIS;

12.2.2.6 Las especificación de los requisitos de seguridad del software de aplicación deberían proporcionar información que permita una selección apropiada del equipo. Se deberían considerar los puntos siguientes:

- las funciones que permiten al equipo alcanzar o mantener un estado seguro;
- las funciones relativas a la detección, anuncio y gestión de defectos en subsistemas del SIS;
- las funciones relativas a los ensayos periódicos de las funciones instrumentadas de seguridad en línea;
- las funciones relativas a los ensayos periódicos de las funciones instrumentadas de seguridad fuera de línea;
- las funciones que permiten la modificación segura del SIS;
- las interfaces con las funciones que no se relacionan con de seguridad;
- la capacidad y tiempo de respuesta;
- los niveles de integridad de seguridad para cada una de las funciones anteriores.

NOTA 1 – Dependiendo de las propiedades del subsistema del SIS algunas de estas funciones pueden formar parte del software del sistema.

NOTA 2 – Las interfaces incluyen las instalaciones de modificación tanto en línea como fuera de línea.

12.3 Planificación de la validación del software de aplicación

NOTA – Esta fase corresponde a la casilla 12.3 de la figura 11.

12.3.1 Objetivo

12.3.1.1 El objetivo de los requisitos de este apartado es asegurar que se realiza una planificación adecuada de la validación del software de aplicación.

12.3.2 Requisitos

12.3.2.1 La planificación de la validación del software de aplicación se debe realizar de acuerdo con el capítulo 15.

12.4 Diseño y desarrollo del software de aplicación

NOTA – Esta fase corresponde a la casilla 12.4 de la figura 11.

12.4.1 Objetivos

12.4.1.1 El primer objetivo de los requisitos de este apartado es crear una arquitectura de software de aplicación que sea coherente con la arquitectura del software y que cumpla los requisitos especificados para la seguridad del software (véase el apartado 12.2).

12.4.1.2 El segundo objetivo de los requisitos de este apartado es revisar y evaluar los requisitos impuestos al software por la arquitectura del hardware y el software integrado del SIS. Éstos incluyen los efectos laterales del comportamiento del hardware/software del SIS, la configuración específica de hardware del SIS, la tolerancia a los defectos inherentes del SIS y la interacción de la arquitectura del hardware del SIS y del software integrado con el software de aplicación en lo que se refiere a la seguridad.

12.4.1.3 El tercer objetivo de los requisitos de este apartado es seleccionar un conjunto de herramientas adecuado (incluyendo software utilitario) para desarrollar el software de aplicación.

12.4.1.4 El cuarto objetivo de los requisitos de este apartado es diseñar y realizar o seleccionar un software de aplicación que cumpla los requisitos especificados para la seguridad del software (véase el apartado 12.2), que sea analizable, verificable y apto para ser modificado con seguridad.

12.4.1.5 El quinto objetivo de los requisitos de este apartado es verificar que los requisitos para la seguridad del software (en términos de las funciones instrumentadas de seguridad del software requeridas) han sido alcanzados.

12.4.2 Requisitos generales

12.4.2.1 El desarrollo, ensayo, verificación y validación del programa de aplicación del lenguaje de variabilidad total deben estar de acuerdo con la Norma IEC 61508-3.

12.4.2.2 El método de diseño debe ser coherente con las herramientas de desarrollo y las restricciones dadas para el subsistema del SIS aplicado.

NOTA – Se deberían definir las restricciones sobre la aplicación del subsistema del SIS necesario para asegurar el cumplimiento con la Norma IEC 61511 en el manual de seguridad del equipo.

12.4.2.3 El método de diseño seleccionado y el lenguaje de la aplicación (LVL o FPL) deberían poseer características que faciliten

a) la abstracción, modularidad y otras características que controlan la complejidad; siempre que sea posible, se debería basar el software en módulos de software bien probados que pueden incluir funciones de biblioteca de usuario y reglas bien definidas para enlazar los módulos de software;

b) la expresión de

- la funcionalidad, idealmente como una descripción lógica o como funciones de algoritmo;
- el flujo de información entre los elementos modulares de las funciones de la aplicación;
- los requisitos de secuenciamiento;
- la seguridad de que las funciones instrumentadas de seguridad funcionan siempre dentro de las limitaciones de tiempo definidas;
- la ausencia de comportamiento indeterminado;
- la seguridad de que los datos elementales internos no son duplicados por error, se definen todos los tipos de datos usados y se producen las acciones apropiadas cuando los datos están fuera de intervalo o son erróneos;
- las hipótesis de diseño y sus dependencias;

c) la comprensión por los desarrolladores y otras personas que necesitan comprender el diseño, tanto desde el entendimiento funcional de una aplicación como desde un conocimiento de las limitaciones de la tecnología;

d) la verificación y la validación, incluyendo la cobertura del código de software de aplicación, la cobertura funcional de la aplicación integrada, la interfaz con el SIS y su configuración de hardware específico de aplicación;

e) la modificación del software de aplicación. Tales características incluyen la modularidad, la trazabilidad y la documentación.

12.4.2.4 El diseño logrado debe:

a) incluir verificaciones de integridad de los datos y verificaciones de verosimilitud;

NOTA – Por ejemplo verificaciones de un extremo a otro en los enlaces de comunicación, verificaciones de limitaciones de entradas de sensor, verificaciones de límites de parámetros de datos y ejecución diversa de las funciones de la aplicación.

b) ser rastreable respecto a los requisitos;

c) ser susceptible de ensayo;

d) tener la capacidad de modificación segura;

e) mantener la complejidad y tamaño del software de aplicación del SIS en un mínimo.

12.4.2.5 En los casos en los que el software de aplicación vaya a realizar funciones instrumentadas de seguridad de niveles de integridad de seguridad diferentes, o funciones que no sean de seguridad, se debe tratar todo el software como perteneciente al nivel de integridad de seguridad más alto, salvo que se pueda demostrar en el diseño la independencia entre las funciones instrumentadas de seguridad de diferentes niveles de integridad de seguridad. La justificación para la independencia debe ser documentada. Tanto si se reivindica la independencia como si no, se debe identificar para cada SIF el SIL previsto.

NOTA 1 – La Norma IEC 61511-2 proporciona una guía sobre como diseñar y desarrollar el software de aplicación cuando en el SIS se realizan tanto funciones de seguridad como funciones no de seguridad.

NOTA 2 – La Norma IEC 61511-2 proporciona una guía sobre como diseñar y desarrollar el software de aplicación cuando en el SIS se realizan SIF de diferente SIL.

12.4.2.6 Si se van a usar funciones de biblioteca de software de aplicación previamente desarrolladas como parte del diseño, se debe justificar su adecuación para satisfacer la especificación de los requisitos para la seguridad del software de aplicación (véase el aparatado 12.2). La adecuación se debe basar en

- el cumplimiento de la Norma IEC 61508-3 cuando se usa FVL; o
- el cumplimiento de la Norma IEC 61511 cuando se usa FPL o LVL; o
- evidencias de funcionamiento satisfactorio en una aplicación similar donde se ha demostrado tener una funcionalidad similar o que haya sido sometida a los mismos procedimientos de verificación y validación que los que se hubieran previsto para cualquier software recién desarrollado (véanse los apartados 11.5.4 y 11.5.5).

NOTA – Se puede desarrollar la justificación durante la planificación de la seguridad (véase el capítulo 6).

12.4.2.7 En la documentación del programa de aplicación o documentación relacionada, se debe incluir como mínimo la información siguiente:

a) la entidad legal [por ejemplo, empresa, autor(es)];

b) la descripción;

c) la trazabilidad respecto a los requisitos funcionales de la aplicación;

d) los convenios lógicos utilizados;

e) las funciones normales de biblioteca utilizadas;

f) las entradas y salidas; y

g) la gestión de la configuración, incluyendo un histórico de los cambios.

12.4.3 Requisitos relativos a la arquitectura del software de aplicación

12.4.3.1 El diseño de la arquitectura del software de aplicación debe basarse en la especificación del SIS requerida dentro de los límites de la arquitectura de sistema del SIS. Debe cumplir con los requisitos del diseño de subsistema seleccionado, su conjunto de herramientas y manual de seguridad.

NOTA 1 – La arquitectura del software define los componentes principales y subsistemas del sistema y del software de aplicación, como están interconectados, y como se logran los atributos requeridos, particularmente la integridad de seguridad. Los ejemplos de módulos de software de sistema incluyen sistemas operativos, bases de datos, subsistemas de comunicación. Los ejemplos de módulos de software de aplicación incluyen funciones de aplicación que se repliquen a través de la planta.

NOTA 2 – También se debería determinar la arquitectura del software de aplicación por la arquitectura subyacente del subsistema del SIS proporcionado por el suministrador.

12.4.3.2 La descripción del diseño de la arquitectura del software de aplicación debe

a) proporcionar una descripción completa de la estructura interna y del funcionamiento del subsistema del SIS y de sus componentes;

b) incluir la especificación de todos los componentes identificados, y la descripción de las conexiones e interacciones entre los componentes identificados (software y hardware);

c) identificar los módulos de software incluidos en el subsistema del SIS pero no usados en ninguna SIF;

d) describir el orden del procesamiento lógico de los datos con respecto a los subsistemas de entrada/salida y la funcionalidad de la unidad lógica, incluyendo cualesquiera limitaciones impuestas por los tiempos de barrido;

e) identificar todas las funciones que no sean SIF y asegurarse de que no pueden afectar el funcionamiento correcto de ninguna SIF.

NOTA – Es de particular importancia que la documentación de la arquitectura esté actualizada y completa con respecto al subsistema del SIS.

12.4.3.3 Se debería identificar el conjunto de métodos y técnicas usados para desarrollar el software de aplicación y se deberían justificar las razones para su selección.

NOTA – Estos métodos y técnicas deberían estar dirigidos a asegurar

- la posibilidad de prever el comportamiento del subsistema del SIS;
- la tolerancia de defectos (coherente con el hardware) y la evitación de defectos, incluyendo la redundancia y la diversidad.

12.4.3.4 Los métodos y técnicas usados en el diseño del software de aplicación deberían ser consistentes con cualesquiera limitaciones identificadas en el manual de seguridad del subsistema del SIS.

12.4.3.5 Las disposiciones usadas para mantener la integridad de seguridad de todos los datos deben ser descritas y justificadas. Tales datos pueden incluir los datos de entrada/salida, los datos de comunicaciones, datos de funcionamiento, datos de mantenimiento y datos de la base de datos interna.

NOTA – Habrá iteración entre la arquitectura del hardware y del software (véase la figura 11) y existe por tanto una necesidad de discutir con el desarrollador del hardware aspectos tales como la especificación de ensayo para la integración del hardware de la electrónica programable y el software (véase el apartado 12.5).

12.4.4 Requisitos relativos a las herramientas de soporte, al manual del usuario y a los lenguajes de aplicación

12.4.4.1 Se debe seleccionar un conjunto de herramientas adecuado, incluyendo un subconjunto del lenguaje de programación de la aplicación, herramientas de gestión de la configuración, de simulación, herramientas de banco de ensayo, y en los casos en que sea aplicable, herramientas de medición de cobertura de ensayo automáticas.

12.4.4.2 Se debería considerar la disponibilidad de herramientas adecuadas (no necesariamente las usadas durante el desarrollo inicial del sistema) para proporcionar los servicios relevantes durante toda la vida del SIS.

NOTA – La selección de las herramientas de desarrollo debería depender de la naturaleza de las actividades de desarrollo del software de aplicación, del software integrado y de la arquitectura del software (véase el apartado 12.4.3).

12.4.4.3 Se debería identificar un conjunto adecuado de procedimientos para el uso de las herramientas, teniendo en cuenta las limitaciones del manual de seguridad, las debilidades conocidas que pueden introducir defectos en el software de aplicación y cualquier limitación relativa a la cobertura de las verificaciones y validaciones precedentes.

12.4.4.4 El lenguaje de aplicación seleccionado debe

- ser realizado usando un traductor/compilador que haya sido evaluado para establecer su adecuación para estos fines;
- ser definido completamente y sin ambigüedad o restringido a características definidas sin ambigüedad;
- corresponder a las características de la aplicación;
- contener características que faciliten la detección de los errores de programación; y
- dar soporte a características que correspondan con el método de diseño.

12.4.4.5 Cuando no se puede satisfacer el apartado 12.4.4.4, se debe documentar una justificación del lenguaje usado durante la descripción del diseño de la arquitectura del software de aplicación (véase el apartado 12.4.3). La justificación debe detallar la aptitud del lenguaje para los fines, y cualesquiera otras medidas que traten cualquier deficiencia identificada del lenguaje.

12.4.4.6 Los procedimientos para el uso del lenguaje de aplicación deberían especificar la buena práctica de programación, proscribir el software genérico no seguro (por ejemplo, funciones de lenguaje no definido), identificar las verificaciones para detectar los fallos en la configuración y especificar los procedimientos para la documentación del programa de aplicación.

12.4.4.7 El manual de seguridad debe tratar los aspectos siguientes, según sea apropiado:

a) el uso de diagnósticos para realizar las funciones seguras;

b) la lista de bibliotecas de seguridad certificadas/verificadas;

c) los ensayos obligatorios y la lógica de parada del sistema;

d) el uso de perros guardianes;

e) los requisitos para las herramientas y los lenguajes de programación y sus limitaciones;

f) los niveles de integridad de seguridad para los cuales es adecuado el dispositivo o sistema.

12.4.4.8 Se debe verificar la aptitud de las herramientas.

12.4.5 Requisitos relativos al desarrollo del software de aplicación

12.4.5.1 Antes del inicio del diseño del software de aplicación, se debe disponer de la información siguiente:

a) la especificación de los requisitos de seguridad del software (véase el apartado 12.2);

b) la descripción del diseño de la arquitectura del software de aplicación (véase el apartado 12.4.3), incluyendo la identificación de la lógica de la aplicación y la funcionalidad de tolerancia a los defectos, una lista de los datos de entrada y salida, los módulos de software genéricos y las herramientas de soporte a usar y los procedimientos para programar el software de aplicación.

12.4.5.2 Se debería producir el software de aplicación de una manera estructurada, a fin de obtener:

- la modularidad de funcionalidad;
- la posibilidad de ensayar la funcionalidad (incluyendo las características de tolerancia a defectos) y de estructura interna;
- la capacidad de modificación segura;
- la trazabilidad respecto a las funciones de la aplicación y las limitaciones asociadas y una explicación de las mismas.

NOTA – Siempre que fuera posible se deberían usar módulos de software probados.

12.4.5.3 El diseño de cada módulo de aplicación debe tener en cuenta la robustez, incluyendo

- verificaciones de la verosimilitud de cada variable de entrada incluyendo todas las variables globales usadas para proporcionar datos de entrada;
- la definición completa de las interfaces de entrada y de salida;
- las verificaciones de configuración del sistema, incluyendo la existencia y accesibilidad de módulos previstos de hardware y software.

12.4.5.4 Se debe especificar el diseño de cada módulo de software de aplicación y los ensayos estructurales a realizar en cada módulo de software de aplicación.

12.4.5.5 El software de aplicación debería

- ser legible, entendible y susceptible de ensayo;
- satisfacer los principios de diseño relevantes;
- satisfacer los requisitos especificados durante la planificación de la seguridad (véase el apartado 5.2.4).

12.4.5.6 Se debe revisar el software de aplicación para asegurarse de su conformidad con el diseño especificado, los principios de diseño y los requisitos de la planificación de la validación de la seguridad.

NOTA – La revisión del software de aplicación incluye técnicas tales como las inspecciones de software, las lecturas cruzadas, y el análisis formal. Se debería usar en conjunción con la simulación y los ensayos para proporcionar la seguridad de que el software de aplicación satisface la especificación asociada.

12.4.6 Requisitos relativos a los ensayos de los módulos de software de aplicación

NOTA – Los ensayos de que el módulo de software de aplicación satisface correctamente la especificación constituyen una actividad de verificación (véase también el apartado 12.7). Es la combinación de revisión y ensayos estructurales la que proporciona seguridad de que un módulo de software de aplicación satisface la especificación asociada, es decir, está verificado.

12.4.6.1 Se debe verificar por medio de la revisión, la simulación y las técnicas de ensayo que la configuración de cada punto de entrada a través de la lógica de proceso hasta el punto de salida, para confirmar que los datos de I/O son puestos en correspondencia con la lógica de aplicación correcta.

12.4.6.2 Se debe verificar por medio de la revisión, la simulación y las técnicas de ensayo cada módulo de software de aplicación para determinar que la función a que se destina se ejecuta correctamente y no se ejecutan funciones no previstas.

Los ensayos deben ser adecuados para el módulo específico que se ensaya y se debe considerar los siguientes puntos:

- ejercitar todas las partes del modelo de aplicación;
- ejercitar las fronteras de los datos;
- los efectos de temporización debidos a la secuencia de ejecución;
- la realización de una secuencia correcta.

12.4.6.3 Se deben hacer disponibles los resultados de los ensayos del módulo de software de aplicación.

12.4.7 Requisitos relativos a los ensayos de integración del software de aplicación

NOTA – Los ensayos de que el software de aplicación está correctamente integrado constituyen una actividad de verificación (véase también el apartado 12.7).

12.4.7.1 Los ensayos del software de aplicación deben mostrar que todos los módulos de software de aplicación y los componentes/subsistemas interactúan correctamente entre sí y con el software integrado subyacente para realizar la función a que se destinan.

NOTA – Se debería realizar ensayos también para confirmar que el software no realiza funciones no esperadas que perjudiquen sus requisitos de seguridad.

12.4.7.2 Se deben hacer disponibles los resultados de los ensayos de integración del software de aplicación y deben indicar

a) los resultados de ensayo; y

b) si se han cumplido los objetivos y criterios de la especificación de ensayo.

Si existe un fallo, se debería informar de las razones de dicho fallo.

12.4.7.3 Durante la integración del software de aplicación, cualquier modificación debe estar sujeta a un análisis de impacto en la seguridad que debe determinar:

a) todos los módulos de software que sufren impacto; y

b) las actividades necesarias de rediseño y nueva verificación (véase el apartado 12.6).

12.5 Integración del software de aplicación con el subsistema del SIS

NOTA – Esta fase corresponde a la casilla 12.5 de la figura 11.

12.5.1 Objetivo

12.5.1.1 El objetivo de este apartado es demostrar que el software de aplicación satisface su especificación de requisitos de seguridad del software cuando se ejecuta sobre el hardware y el software integrado usados en el subsistema del SIS.

NOTA – Dependiendo de la naturaleza de la aplicación, estas actividades se pueden combinar con las del apartado 12.4.7.

12.5.2 Requisitos

12.5.2.1 Se deben especificar los ensayos de integración tan pronto como sea posible en el ciclo de vida de seguridad del software para asegurar la compatibilidad del software de aplicación con el hardware y con la plataforma del software integrado de manera que se puedan cumplir los requisitos de seguridad funcional y de características de funcionamiento.

NOTA 1 – Se puede reducir el objeto de los ensayos en base a la experiencia previa.

NOTA 2 – Se deberían considerar los puntos siguientes

- la división del software de aplicación en conjuntos de integración manejables;
- los casos de ensayo y los datos de ensayo;
- los tipos de ensayos a realizar;
- el ambiente de ensayo, las herramientas, la configuración y los programas;
- los criterios de ensayo con los que se juzgará el ensayo; y
- los procedimientos para acción correctora en caso de fallo durante el ensayo.

12.5.2.2 Durante el ensayo, cualquier modificación o cambio debe estar sujeto a un análisis de impacto en la seguridad que debe determinar:

a) todos los módulos de software que sufren impacto; y

b) las actividades necesarias de nueva verificación (véase el apartado 12.7).

12.5.2.3 Debe hacerse disponible la siguiente información relativa al ensayo:

a) los elementos de configuración que se ensayan;

b) los elementos de configuración que soportan el ensayo (herramientas y funcionalidad externa);

c) el personal implicado;

d) los casos de ensayo y los guiones de ensayo;

e) los resultados de ensayo;

f) si se han satisfecho el objetivo y los criterios de los ensayos; y

g) si se ha producido un fallo, las razones para el fallo, el análisis del fallo y los registros de la corrección incluyendo la repetición del ensayo y la nueva verificación (véase el apartado 12.5.2.2).

12.6 Procedimientos de modificación del software utilizando el FPL y el LVL

NOTA – El término modificación se aplica principalmente a los cambios que se producen durante la fase operacional del software.

12.6.1 Objetivo

12.6.1.1 El objetivo de los requisitos de este apartado es asegurar que el software continúa satisfaciendo la especificación de los requisitos de seguridad del software después de las modificaciones.

12.6.2 Requisitos de modificación

12.6.2.1 Las modificaciones se deben llevar a cabo de acuerdo con los apartados 5.2.6.2.2, 5.2.7 y el capítulo 17, con los siguientes requisitos adicionales:

a) Antes de la modificación se debe realizar un análisis de los efectos de la modificación en la seguridad del proceso y en el estado del diseño del software y se debe usar para dirigir la modificación.

b) Debe estar disponible la planificación de seguridad para la modificación y la nueva verificación.

c) Las modificaciones y las nuevas verificaciones se deben realizar de acuerdo con la planificación.

d) Se debe considerar la planificación relativa a las condiciones requeridas durante la modificación y los ensayos.

e) Se debe actualizar toda la documentación afectada por la modificación.

f) Se deben hacer disponibles los detalles de todas las actividades de modificación del SIS (por ejemplo, un libro de registro).

12.7 Verificación del software de aplicación

12.7.1 Objetivos

12.7.1.1 El primer objetivo de este apartado es demostrar que la información es satisfactoria.

12.7.1.2 El segundo objetivo de este apartado es demostrar que los resultados de salida satisfacen los requisitos definidos en cada fase del ciclo de vida de seguridad del software de aplicación.

12.7.2 Requisitos

12.7.2.1 Se debe realizar la planificación de la verificación para cada fase del ciclo de vida del software de aplicación de acuerdo con el capítulo 7.

12.7.2.2 Se deben verificar los resultados de cada fase respecto a

a) la adecuación de las salidas de la fase particular del ciclo de vida respecto a los requisitos relativos a esa fase;

b) la adecuación de la cobertura de la revisión, la inspección y/o el ensayo correspondiente a las salidas;

c) la compatibilidad entre las salidas generadas en las diferentes fases del ciclo de vida;

d) la exactitud de los datos.

12.7.2.3 La verificación debería tratar también:

a) la susceptibilidad de ensayo;

b) la legibilidad;

c) la trazabilidad.

NOTA 1 – Se debería verificar el formato de datos en el programa de aplicación en cuanto a:
- el carácter completo;
- la coherencia intrínseca;
- la protección contra alteraciones no autorizadas;
- la coherencia con los requisitos funcionales.

NOTA 2 – También se deberían verificar los datos de aplicación en cuanto a
- la coherencia con las estructuras de los datos;
- su carácter completo;
- la compatibilidad con el software del sistema subyacente (por ejemplo, secuencia de ejecución, tiempo de marcha):
- los valores de datos correctos;
- el funcionamiento dentro de un perímetro de seguridad conocido.

NOTA 3 – Se deberían verificar los parámetros modificables en cuanto a la protección contra
- los valores iniciales no válidos o indefinidos;
- los valores erróneos;
- los cambios no autorizados:
- la alteración de los datos;

NOTA 4 – Se deberían verificar las interfaces de comunicación, de proceso y el software asociado en cuanto a
- la detección de fallos;
- la protección contra la alteración de mensajes; y
- la validación de datos.

12.7.2.4 Se deberían verificar las funciones que no sean de seguridad y las interfaces de proceso integradas con las señales y funciones relacionadas con la seguridad en cuanto a

- no interferencia con las funciones de seguridad;
- protección contra la interferencia con las funciones de seguridad en el caso de mal funcionamiento de las funciones que no sean de seguridad.

13 ENSAYOS DE ACEPTACIÓN EN FÁBRICA (FAT)

NOTA – Este capítulo es informativo.

13.1 Objetivos

13.1.1 El objetivo de un ensayo de aceptación en fábrica (FAT) es ensayar la unidad lógica y el software asociado juntos para asegurarse de que satisface los requisitos definidos en la especificación de requisitos de seguridad. Ensayando la unidad lógica y el software asociado antes de instalarlos en una planta, se pueden identificar y corregir errores fácilmente.

NOTA – A veces el ensayo de aceptación en fábrica se denomina ensayo de integración y puede ser parte de la validación.

13.2 Recomendaciones

13.2.1 Durante la fase de diseño de un proyecto se debería especificar la necesidad de un FAT.

NOTA 1 – Puede ser necesaria una estrecha cooperación entre el suministrador de la unidad lógica y el contratista de diseño a fin de desarrollar los ensayos de integración.

NOTA 2 – Las actividades siguen a las fases de diseño y desarrollo y preceden a las de instalación y recepción.

NOTA 3 – Las actividades son aplicables a los subsistemas de un SIS con electrónica programable o sin ella.

NOTA 4 – Es habitual que el FAT tenga lugar en un entorno de fábrica antes de la instalación y de la recepción en la planta.

13.2.2 La planificación de un FAT debería especificar los puntos siguientes:

- Tipos de ensayos a realizar, incluyendo los ensayos de funcionalidad del sistema de caja negra (es decir, el método de diseño de ensayo que trata al sistema como una "caja negra", de manera que no usa explícitamente el conocimiento de su estructura interna. El diseño de ensayo de caja negra se describe habitualmente como enfocado a los requisitos de ensayos de función. Los sinónimos de caja negra incluyen ensayos de comportamiento, funcional, caja opaca, y caja cerrada); ensayos de características de funcionamiento (temporización, fiabilidad y disponibilidad, integridad, objetivos de seguridad y limitaciones), ensayos ambientales (incluyendo los ensayos de CEM, vida y esfuerzos), ensayos de interfaces, ensayos en modos degradados y/o con defectos, ensayos de excepción, aplicación de los manuales de operación y mantenimiento del SIS.

- Los casos de ensayo, la descripción del ensayo y los datos del ensayo.

  NOTA – Es muy importante dejar claro quién es responsable de desarrollar el caso de ensayo y quién va a ser responsable de realizar el ensayo y de presenciarlo.

- La dependencia de otros sistemas/interfaces.

- El entorno y herramientas de ensayo.

- La configuración de la unidad lógica.

- Los criterios de ensayo con los que se debe juzgar la terminación del ensayo.

- Los procedimientos para la acción correctora en caso de fallo en el ensayo.

- Las competencias del personal de ensayo.

- El emplazamiento físico.

NOTA – Para los ensayos que no se pueden demostrar físicamente, éstos se resuelven normalmente por un argumento formal tal como por qué cumple el SIS el requisito, objetivo o limitación.

13.2.3 El FAT debería tener lugar con una versión definida de la unidad lógica.

13.2.4 Se debería hacer el FAT de acuerdo con la planificación del FAT. Estos ensayos deberían mostrar que toda la lógica funciona correctamente.

13.2.5 Para cada ensayo realizado se deberían tratar los puntos siguientes:

- la versión de la planificación de ensayo que se está usando;

- la función instrumentada de seguridad y la característica de funcionamiento que se está ensayando;

- los procedimientos de ensayo detallados y la descripción del ensayo;

- un registro cronológico de las actividades de ensayo;
- las herramientas, equipos e interfaces utilizadas.

13.2.6 Se deberían documentar los resultados del FAT, indicando

a) los casos de ensayo;

b) los resultados de ensayo; y

c) si se han cumplido los objetivos y criterios del ensayo.

Si durante el ensayo se produjera un fallo, se deberían documentar y analizar las razones de dicho fallo y se debería realizar la acción correctiva apropiada.

13.2.7 Durante el FAT, cualquier modificación o cambio debería estar sujeto a un análisis de seguridad para determinar:

a) la extensión del impacto en cada función instrumentada de seguridad; y

b) se debería definir la extensión de la repetición del ensayo.

NOTA – Puede comenzar la recepción mientras se realiza la acción correctiva, dependiendo de los resultados del FAT.

14 INSTALACIÓN Y RECEPCIÓN DEL SIS

14.1 Objetivos

14.1.1 Los objetivos de los requisitos de este capítulo son:

- instalar el sistema instrumentado de seguridad según las especificaciones y planos;
- recepcionar el sistema instrumentado de seguridad de forma que esté listo para la validación final del sistema.

14.2 Requisitos

14.2.1 La planificación de la instalación y de la recepción debe definir todas las actividades requeridas para la instalación y la recepción. La planificación debe establecer los siguientes puntos:

- las actividades de instalación y de recepción;
- los procedimientos, medidas y técnicas a utilizar para la instalación y la recepción;
- cuándo deben tener lugar estas actividades;
- las personas, departamentos y organismos responsables de estas actividades.

La planificación de la instalación y de la recepción puede ser integrada en la planificación general del proyecto en los casos en los que sea apropiado.

14.2.2 Todos los componentes del sistema instrumentado de seguridad deben ser instalados adecuadamente según el(los) plan(es) de diseño e instalación (véase el apartado 14.2.1).

14.2.3 Se debe recepcionar el sistema instrumentado de seguridad de acuerdo con la planificación con vistas a la preparación de la validación final del sistema. Las actividades de recepción deben incluir, sin limitarse a ello, la confirmación de los puntos siguientes:

- se ha conectado adecuadamente la puesta a tierra (o a masa);
- se han conectado adecuadamente las fuentes de energía y son operacionales;
- se han retirado los bloqueos de transporte y los materiales de embalaje;
- no se constatan daños físicos;
- todos los instrumentos han sido adecuadamente calibrados;
- todos los dispositivos de campo son operativos;
- la unidad lógica y las entradas/salidas son operativas;
- las interfaces con otros sistemas y periféricos son operativas.

14.2.4 Se deben realizar registros adecuados de la recepción del SIS, indicando los resultados de ensayo, y si se han cumplido los objetivos y criterios establecidos durante la fase de diseño. Si existe un fallo, se deben registrar las razones de dicho fallo.

14.2.5 En los casos en los que se ha establecido que la instalación real no satisface la información de diseño, se deben evaluar la diferencias por una persona competente y se debe determinar el impacto probable sobre la seguridad. Si se establece que las diferencias no tienen impacto sobre la seguridad, entonces se debe actualizar la información de diseño al estado "como se construyó". Si las diferencias tienen un impacto negativo sobre la seguridad, entonces se debe modificar la instalación para satisfacer los requisitos de diseño.

15 VALIDACIÓN DE LA SEGURIDAD DEL SIS

15.1 Objetivos

15.1.1 Los objetivos de los requisitos de este capítulo son validar mediante la inspección y los ensayos, que el sistema instrumentado de seguridad y sus funciones instrumentadas de seguridad asociadas cumplen los requisitos establecidos en la especificación de requisitos de seguridad

NOTA – A veces esto se denomina ensayo de recepción in situ (SAT).

15.2 Requisitos

15.2.1 La planificación de validación del SIS debe definir todas las actividades requeridas para la validación. Se deben incluir los siguientes puntos:

- las actividades de validación que incluyen la validación del (de los) sistema(s) instrumentado(s) respecto a la especificación de los requisitos de seguridad incluyendo la realización y resolución de las recomendaciones resultantes;
- la validación de todos los modos de funcionamiento relevantes del proceso y sus equipos asociados, incluyendo:
  - la preparación para la utilización, incluyendo la inicialización y el ajuste;
  - el funcionamiento en el arranque, en automático, en manual, en semiautomático y en régimen estable;
  - la reinicialización, la parada y el mantenimiento;
  - las condiciones anormales razonablemente previsibles, por ejemplo, las identificadas a lo largo de la fase de análisis de riesgo;

- los procedimientos, medidas y técnicas a usar para la validación;
- cuándo deben tener lugar estas actividades;
- las personas, departamentos y organismos responsables de estas actividades y los niveles de independencia para las actividades de validación;
- la información de referencia contra la cual se debe llevar a cabo la validación (por ejemplo, diagrama de causa y efecto).

NOTA – Los ejemplos de actividades de validación incluyen el ensayo de bucles, los procedimientos de calibración, la simulación del software de aplicación.

15.2.2 Una planificación adicional de la validación relativa al software de aplicación debe incluir los puntos siguientes:

a) La identificación del software de seguridad que tiene que ser validado para cada modo de funcionamiento del proceso antes que comience la recepción.

b) La información sobre la estrategia técnica para la validación, incluyendo:

   – las técnicas manuales y automáticas;

   – las técnicas estáticas y dinámicas;

   – las técnicas analíticas y estadísticas.

c) De acuerdo con el punto b), las medidas (técnicas) y procedimientos que se deben usar para confirmar que cada función instrumentada de seguridad cumple con los requisitos especificados para las funciones instrumentadas de seguridad del software (véase el apartado 12.2) y los requisitos especificados para la integridad de seguridad del software (véase el apartado 12.2).

d) El ambiente requerido en el que deben tener lugar las actividades de validación (por ejemplo, para los ensayos esto incluiría herramientas y equipos calibrados).

e) Los criterios de aceptación/rechazo para cumplir la validación del software, incluyendo:

   – el proceso requerido y las señales de entrada del operador con sus secuencias y sus valores;

   – las señales de salida anticipadas con sus secuencias y sus valores; y

   – otros criterios de aceptación, por ejemplo, el uso de la memoria, la temporización y las tolerancias de valor.

f) Las reglas y los procedimientos relativos a la evaluación de los resultados de la validación, en particular los fallos.

NOTA – Estos requisitos se basan en los requisitos generales del apartado 12.2.

15.2.3 En los casos en los que se requiere precisión de medición como parte de la validación, los instrumentos usados para esta función deberían ser calibrados contra una especificación referida a una norma dentro de una incertidumbre apropiada para la aplicación. Si no es factible una calibración de este tipo, se debe usar y documentar un método alternativo.

15.2.4 La validación del sistema instrumentado de seguridad y sus funciones instrumentadas de seguridad asociadas se debe llevar a cabo de acuerdo con la planificación de la validación del sistema instrumentado de seguridad. Las actividades de validación deben incluir, sin limitarse a ellos, los puntos siguientes:

- el sistema instrumentado de seguridad funciona en modos de funcionamiento normales y anormales (por ejemplo, arranque, parada) como se identifican en la especificación de requisitos de seguridad;

- la confirmación de que la interacción adversa del sistema básico de control de proceso y de otros sistemas conectados no afecta al funcionamiento correcto del sistema instrumentado de seguridad;

- el sistema instrumentado de seguridad se comunica adecuadamente (en los casos en los que se requiere) con el sistema básico de control de proceso o con cualquier otro sistema o red;

- los sensores, la unidad lógica, y los elementos finales funcionan de acuerdo con la especificación de requisitos de seguridad, incluyendo todos los canales redundantes;

  NOTA – Si se realizó un ensayo de aceptación en fábrica (FAT) en la unidad lógica como se describe en el capítulo 13, se puede dar crédito a la validación de la unidad lógica por el FAT.

- la documentación del sistema instrumentado de seguridad es coherente con el sistema instalado;

- la confirmación de que la función instrumentada de seguridad actúa como se especificó ante valores no válidos de las variables de proceso (por ejemplo, fuera del intervalo);

- se ha activado la secuencia de parada correcta;

- el sistema instrumentado de seguridad da una señalización y una presentación del funcionamiento correctos;

- los cálculos que se incluyen en el sistema instrumentado de seguridad son correctos;

- las funciones de reinicialización del sistema instrumentado de seguridad actúan como se define en la especificación de requisitos de seguridad;

- las funciones de desvío actúan correctamente;

- las anulaciones de arranque funcionan correctamente;

- los sistemas de parada manual funcionan correctamente;

- los intervalos de los ensayos periódicos están documentados en los procedimientos de mantenimiento;

- las funciones de alarma de diagnóstico actúan en la forma requerida;

- la confirmación de que el sistema instrumentado de seguridad actúa como se requiere ante la pérdida de servicios (por ejemplo, de energía eléctrica, aire, sistema hidráulico) y la confirmación de que, cuando se restablecen los servicios, el sistema instrumentado de seguridad vuelve al estado deseado;

- la confirmación de que se ha logrado la inmunidad CEM, tal como se define en la especificación de requisitos de seguridad (véase apartado 10.3).

15.2.5 La validación del software debe mostrar que todos los requisitos de seguridad del software (véase al apartado 12.2) se han cumplido correctamente, y el software no perjudica los requisitos de seguridad en condiciones de defecto del SIS y en modos de funcionamiento degradados o por ejecutar la funcionalidad del software no definida en la especificación. Debe estar disponible la información de las actividades de validación.

15.2.6 Se debe dar una información apropiada de los resultados de la validación del SIS que proporcione:

- la versión de la planificación de la validación del SIS que se está utilizando;

- la función instrumentada de seguridad que se ensaya o analiza), junto con la referencia específica al requisito identificado durante la planificación de la validación del SIS;

- las herramientas y equipos usados , junto con los datos de calibración;
- los resultados de cada ensayo;
- la versión de la especificación de ensayo utilizada;
- los criterios para la aceptación de los ensayos de integración;
- la versión del hardware y del software que se ensaya;
- toda divergencia entre los resultados esperados y los reales;
- el análisis efectuado y las decisiones tomadas sobre si se continúan los ensayos o se emite una solicitud de cambio, en el caso de que se produzcan divergencias.

15.2.7 Cuando se producen divergencias entre los resultados esperados y los reales, el análisis efectuado y las decisiones tomadas sobre si se continúa la validación o se emite una solicitud de cambio y se retorna a una parte anterior del ciclo de vida de desarrollo, deben estar disponibles como parte de los resultados de la validación de la seguridad.

15.2.8 Después de la validación del sistema instrumentado de seguridad, y antes de que se presenten los peligros identificados, se deben llevar a cabo las actividades siguientes.

- Se deben devolver a su posición inicial todas las funciones de desvío (por ejemplo, la unidad lógica y las fuerzas de sensor de PE, alarmas desactivadas).
- Se deben colocar todas las válvulas de aislamiento de proceso según los requisitos y procedimientos de arranque de proceso.
- Se deben retirar todos los materiales de ensayo (por ejemplo, fluidos).
- Se deben retirar todas las fuerzas y si fuera aplicable todas las activaciones de fuerzas.

16 OPERACIÓN Y MANTENIMIENTO DEL SIS

16.1 Objetivos

16.1.1 Los objetivos de los requisitos de este capítulo son:

- asegurar que se mantiene el SIL requerido de cada función instrumentada de seguridad durante la operación y mantenimiento;
- operar y mantener el SIS de manera que se mantenga la seguridad funcional de diseño.

16.2 Requisitos

16.2.1 Se debe realizar la planificación de operación y mantenimiento para el sistema instrumentado de seguridad. Se deben tratar los siguientes puntos:

- las actividades de operación rutinaria y anómala;
- las actividades de ensayos periódicos, de mantenimiento preventivo y de avería;
- los procedimientos, medidas y técnicas a usar para la operación y el mantenimiento;

- la verificación del seguimiento de las operaciones y procedimientos de mantenimiento;
- cuándo deben tener lugar estas actividades;
- las personas, departamentos y organismos responsables de estas actividades.

16.2.2 Se debe desarrollar la operación y el mantenimiento de acuerdo con la planificación de seguridad correspondiente y debe incluir los puntos siguientes:

- las acciones de rutina que es preciso llevar a cabo para mantener la seguridad funcional del SIS "tal como se diseñó", por ejemplo siguiendo los intervalos entre ensayos periódicos definidos por la determinación del SIS;
- las acciones y las limitaciones que son necesarias para evitar un estado inseguro y/o para reducir las consecuencias de un acontecimiento peligroso durante el mantenimiento o la operación (por ejemplo cuando un sistema necesita ser desviado para ensayos o mantenimiento, qué etapas de atenuación adicional es preciso realizar);
- la información que es preciso mantener sobre los fallos del sistema y tasas de demanda sobre el SIS;
- la información que es preciso mantener mostrando los datos de las auditorías y ensayos sobre el SIS;
- los procedimientos de mantenimiento a seguir cuando se producen defectos o fallos en el SIS, incluyendo:
  - los procedimientos de diagnóstico y de reparación de defectos;
  - los procedimientos para repetir la validación;
  - los requisitos para informar del mantenimiento;
  - los procedimientos para dar seguimiento a la realización del mantenimiento.

  NOTA – Estas consideraciones incluyen:
  - los procedimientos para informar de los fallos;
  - los procedimientos para analizar los fallos sistemáticos.
- asegurar que el equipo de ensayo utilizado durante las actividades normales de mantenimiento está adecuadamente calibrado y mantenido.

16.2.3 Se debe realizar la operación y mantenimiento de acuerdo con los procedimientos relevantes.

16.2.4 Se debe formar a los operadores sobre la función y operación del SIS en su área. Esta formación debe asegurar los puntos siguientes:

- el entendimiento de cómo funciona el SIS (los puntos de disparo y la acción resultante que se toma por parte del SIS);
- el riesgo contra el que protege el SIS;
- el funcionamiento de todos los interruptores de desvío y en qué circunstancias se van a usar estos desvíos;
- el funcionamiento de cualesquiera interruptores manuales de parada y de la actividad de arranque manual y cuándo se van a activar estos interruptores manuales;

  NOTA – Esto puede incluir el "restablecimiento del sistema" y el "reinicio del sistema".
- las previsiones sobre la activación de cualesquiera alarmas de diagnóstico (por ejemplo, qué acción se debe tomar cuando se activa cualquier alarma indicando que existe un problema con el SIS).

16.2.5 El personal de mantenimiento debe ser formado según se requiera para mantener las características funcionales plenas del SIS (hardware y software) en su integridad objetivo.

16.2.6 Se deben analizar las divergencias entre el comportamiento esperado del SIS y el real y, en los casos en que sea necesario, se deben hacer modificaciones de manera que se mantenga la seguridad requerida del SIS. Esto debe incluir la supervisión de los aspectos siguientes:

- las acciones tomadas después de una demanda sobre el sistema;
- los fallos del equipo que forma parte del SIS establecidos durante los ensayos periódicos o la demanda real;
- la causa de las demandas;
- la causa de los falsos disparos.

NOTA – Es muy importante que se analicen TODAS las divergencias entre el comportamiento esperado y el real. Esto no se debería confundir con la supervisión de las solicitaciones que se encuentran durante el funcionamiento normal.

16.2.7 Los procedimientos de operación y mantenimiento pueden requerir una revisión, si fuera necesaria, después de

- auditorías de seguridad funcional;
- ensayos del SIS.

16.2.8 Se deben desarrollar procedimientos escritos de los ensayos periódicos para que cada SIF revele fallos peligrosos no detectados por los diagnósticos Estos procedimientos escritos de ensayo deben describir cada etapa a realizar y deben incluir

- el funcionamiento correcto de cada sensor y elemento final;
- la acción lógica correcta;
- las alarmas e indicaciones correctas.

NOTA – Se pueden usar los métodos siguientes para determinar los fallos no detectados que es preciso ensayar:

- examen del árbol de defectos;
- análisis de los modos de fallo y de sus efectos;
- mantenimiento centrado en la fiabilidad.

16.3 Ensayos periódicos e inspección

16.3.1 Ensayos periódicos

16.3.1.1 Se deben realizar ensayos periódicos usando un procedimiento escrito (véase el apartado 16.2.8) para revelar los defectos no detectados que impiden que el SIS funcione de acuerdo con la especificación de requisitos de seguridad.

16.3.1.2 Se debe ensayar el SIS en su conjunto (incluyendo el(los) sensor(es)), la unidad lógica y el(los) elemento(s) final(es) (por ejemplo, las válvulas de parada y los motores).

16.3.1.3 La frecuencia de los ensayos periódicos debe ser la decidida usando el cálculo de la PFD_{avg}.

NOTA – Las diferentes partes del SIS pueden requerir diferentes intervalos de ensayo, por ejemplo, la unidad lógica puede requerir un intervalo de ensayos diferente del de los sensores o los elementos finales.

16.3.1.4 Se deben reparar todas las deficiencias encontradas durante los ensayos periódicos de manera segura y rápida.

16.3.1.5 En algún intervalo periódico (determinado por el usuario), se debe reevaluar la frecuencia de los ensayos en base a diversos factores, incluyendo los datos de ensayo históricos, la experiencia en planta, la degradación del hardware y la fiabilidad del software.

16.3.1.6 Cualquier cambio en la lógica de la aplicación requiere ensayos periódicos completos. Se permiten excepciones a esto si se llevan a cabo una revisión apropiada y ensayos parciales de los cambios para asegurar que los cambios se realizaron correctamente.

16.3.2 Inspección. Cada SIS debe ser inspeccionado periódicamente en forma visual para asegurar que no se han producido modificaciones no autorizadas ni deterioros observables (por ejemplo, pérdida de tornillos o tapas de instrumentos, herrajes oxidados, hilos abiertos, conductos rotos, trazado térmico roto y pérdida de aislamiento).

16.3.3 Documentación de los ensayos periódicos y de la inspección. El usuario debe mantener registros que certifiquen que se completaron los ensayos periódicos y las inspecciones en la forma requerida. Estos registros deben incluir como mínimo la información siguiente:

a) la descripción de los ensayos y de las inspecciones efectuados;

b) las fechas de los ensayos y de las inspecciones;

c) el nombre de la(s) persona(s) que realizó los ensayos e inspecciones;

d) el número de serie u otro identificador único del sistema ensayado (por ejemplo, número de bucle, número de etiqueta, número de equipo, y número de SIF);

e) resultados de los ensayos y de la inspección (por ejemplo, condiciones “tal como se encontró” y “tal como se dejó”).

17 MODIFICACIÓN DEL SIS

17.1 Objetivos

17.1.1 Los objetivos de los requisitos de este capítulo son:

- que las modificaciones a cualquier sistema instrumentado de seguridad se planifiquen adecuadamente, se revisen y se aprueben antes de realizar el cambio; y

- asegurar que se mantiene la integridad de seguridad del SIS a pesar de cualquier cambio que se introduzca en el SIS.

NOTA – Se deberían revisar las modificaciones al BPCS, a otros equipos, o a las condiciones de proceso o funcionamiento para determinar si son tales que la naturaleza o la frecuencia de las solicitaciones sobre el SIS resulten afectadas. Se deberían considerar adicionalmente aquéllas que tengan un efecto adverso para determinar si el nivel de reducción de riesgo será todavía suficiente.

17.2 Requisitos

17.2.1 Antes de realizar cualquier modificación en un sistema instrumentado de seguridad se deben aplicar procedimientos para autorizar y controlar los cambios.

17.2.2 Los procedimientos deben incluir un método claro para identificar y reclamar el trabajo a realizar y los peligros que pudieran resultar afectados.

17.2.3 Se debe realizar un análisis para determinar el impacto sobre la seguridad funcional como resultado de una modificación propuesta. Cuando el análisis muestra que la modificación impactará en la seguridad, entonces se debe retornar a la primera fase del ciclo de vida de seguridad afectada por la modificación.

17.2.4 No debe comenzar la actividad de modificación sin una autorización adecuada.

17.2.5 Se debe mantener una información apropiada sobre todos los cambios al SIS. La información debe incluir:

- una descripción de la modificación o cambios;
- la razón para el cambio;
- los peligros identificados que pudieran resultar afectados;
- un análisis del impacto de la actividad de modificación en el SIS;
- todas las aprobaciones requeridas para los cambios;
- los ensayos usados para verificar que el cambio se realizó adecuadamente y el SIS funciona en la forma requerida;
- el historial adecuado de la configuración;
- los ensayos utilizados para verificar que el cambio no ha impactado en forma adversa a partes del SIS que no fueron modificadas.

17.2.6 Se debe realizar la modificación con personal cualificado que haya recibido la formación adecuada. Se debería notificar el cambio a todo el personal afectado y apropiado y debería ser formado en relación con el cambio.

18 RETIRADA DE SERVICIO DEL SIS

18.1 Objetivos

18.1.1 Los objetivos de los requisitos de este capítulo son:

- asegurar que antes de realizar la retirada de servicio de cualquier sistema instrumentado de seguridad, se realice una revisión correcta y se obtenga la autorización requerida;
- asegurar que las funciones instrumentadas de seguridad requeridas permanecen operativas durante las actividades de retirada del servicio.

18.2 Requisitos

18.2.1 Antes de realizar cualquier retirada del servicio de un sistema instrumentado de seguridad se debe aplicar procedimientos para autorizar y controlar los cambios.

18.2.2 Los procedimientos deben incluir un método claro para identificar y reclamar que se realice el trabajo e identificar los peligros que pudieran ser afectados.

18.2.3 Se debe realizar un análisis para determinar el impacto sobre la seguridad funcional como resultado de la actividad de retirada de servicio propuesta. La evaluación debe incluir una actualización de la evaluación de peligros y riesgos suficiente para determinar la anchura y la profundidad en la que las fases subsiguientes del ciclo de vida de seguridad deben necesitar ser retomadas. La evaluación debe considerar también

- la seguridad funcional durante la ejecución de las actividades de retirada del servicio; y
- el impacto de la retirada de servicio de un sistema instrumentado de seguridad en las unidades operacionales y servicios de instalaciones adyacentes.

18.2.4 Se deben usar los resultados de los análisis de impacto durante la planificación de seguridad para reactivar los requisitos relevantes de esta norma incluyendo la repetición de la verificación y de la validación.

18.2.5 No se deben comenzar las actividades de retirada de servicio sin una autorización adecuada.

19 REQUISITOS RELATIVOS A LA INFORMACIÓN Y A LA DOCUMENTACIÓN

19.1 Objetivos

19.1.1 Los objetivos de los requisitos de este capítulo son:

- asegurar que la información necesaria se encuentra disponible y documentada a fin de que se pueda realizar eficazmente todo el ciclo de seguridad; y
- asegurar que la información necesaria se encuentra disponible y documentada a fin de que se puedan realizar eficazmente las actividades de verificación, validación y evaluación de la seguridad funcional.

NOTA 1 – Véase en cuanto a ejemplos de estructura de la documentación la Norma IEC 61508-1, anexo A y para más detalles la Norma IEC 61506.

NOTA 2 – Se debería encontrar disponible la documentación en diferentes formatos (por ejemplo, en papel, película, o cualquier medio de soporte de datos que se pueda presentar en pantallas o monitores).

19.2 Requisitos

19.2.1 Debe estar disponible la documentación requerida por esta norma.

19.2.2 La documentación debería

- describir la instalación sistema o equipo y el uso del mismo;
- ser precisa;
- ser fácil de entender;
- adecuarse a la finalidad a la que se destina; y
- estar disponible en una forma accesible y que se pueda mantener.

19.2.3 La documentación debe tener identidades únicas, de manera que debe ser posible hacer referencia a sus diversas partes.

19.2.4 La información debe tener designaciones que indiquen el tipo de información.

19.2.5 La información debe ser trazable según los requisitos de esta norma.

19.2.6 La información debe tener un índice de revisiones (números de versión) para hacer posible identificar las diferentes versiones de la información.

19.2.7 La documentación debe estar estructurada para hacer posible buscar la información relevante. Debe ser posible identificar la última revisión (versión) de un documento.

NOTA – La estructura física de la documentación debería variar dependiendo de diversos factores tales como el tamaño del sistema, la complejidad y los requisitos de organización.

19.2.8 Se debe revisar, enmendar, poner al día y aprobar toda la documentación relevante y debe ponerse bajo el control de un esquema de información apropiado.

19.2.9 Se debe mantener la información vigente correspondiente a los siguientes aspectos:

a) los resultados de la evaluación de peligros y riesgos y los supuestos relativos a la misma;

b) el equipo usado para las funciones instrumentadas de seguridad junto con sus requisitos de seguridad;

c) el organismo responsable de mantener la seguridad funcional;

d) los procedimientos necesarios para alcanzar y mantener la seguridad funcional del SIS;

e) la información sobre las modificaciones como se define en el apartado 17.2.5;

f) el diseño, la realización, los ensayos y la validación.

NOTA – En los capítulos 14 y 15 se incluyen detalles adicionales sobre los requisitos relativos a la información.

ANEXO A (Informativo)

DIFERENCIAS

Este anexo ilustra las diferencias principales entre las Normas IEC 61511 e IEC 61508.

La Norma IEC 61511 tiene algunas diferencias con la Norma IEC 61508. Estas diferencias se discuten en los capítulos A.1 y A.2 y se basan en la comparación de esta versión de la Norma IEC 61511 con la Norma IEC 61508.

A.1 Diferencias organizacionales

IEC 61508	IEC 61511	Comentarios
Parte 1	Parte 1	Se han combinado las Normas IEC 61508-1, -2, -3, y -4 en la Norma IEC 61511-1
Parte 2	Parte 1	Incluida en la Norma IEC 61511-1
Parte 3	Parte 1	Incluida en la Norma IEC 61511-1
Parte 4	Parte 1	Incluida en la Norma IEC 61511-1
Parte 5	Parte 3	Incluida en la Norma IEC 61511-3
Parte 6	Parte 2	Directrices de la Norma IEC 61511-1
Parte 7	Todas las partes	Se han incluido referencias informativas en cada parte como anexos (en los casos en los que se requieren)

A.2 Terminología

IEC 61508-4	IEC 61511-1	Comentarios
Relacionada con los sistemas de seguridad E/E/PE	SIS	La Norma IEC 61508 se refiere a los sistemas relacionados con la seguridad, mientras que la Norma IEC 61511 se refiere a los sistemas instrumentados de seguridad
PES	SIS	En la Norma IEC 61508 “PES” incluye sensores y elementos finales de control, mientras que la Norma IEC 61511 usa el término SIS
Sistema de control de procesos	Sistema básico de control de procesos	El sistema básico de control de procesos es un término global para el sector de procesos
EUC	Proceso	La norma IEC 61508 se refiere a EUC (equipos bajo control), mientras que la Norma IEC 61511 se refiere a proceso
Función de seguridad	Función instrumentada de seguridad (SIF)	La función de seguridad de la Norma IEC 61508 se realiza por los sistemas E/E/PES, sistemas relacionados con la seguridad de otra tecnología, o instalaciones externas de reducción de riesgo. La Norma IEC 61511 se realiza exclusivamente por SIS.

BIBLIOGRAFÍA

IEC 60050(191):1990 – *Vocabulario electrotécnico internacional. Parte 191:* Seguridad de funcionamiento y calidad de servicio.

IEC 60050(351):1998 – *Vocabulario electrotécnico internacional. Parte 351: Control automático.*

IEC 60617-12:1997 – *Símbolos gráficos para esquemas. Parte 12: Elementos lógicos binarios.*

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

IEC 61506:1997 – *Industrial-process measurement and control. Documentation of application software.*

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

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

IEC 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 IEC 61508-2 e IEC 61508-3.*

IEC 61511-3:2003 – *Seguridad funcional. Sistemas instrumentados de seguridad para el sector de la industria de procesos. Parte 3: Guía para la determinación de los niveles requeridos de integridad de seguridad.*

ISO/IEC 2382 (all parts) – *Information technology. Vocabulary.*

ISO/IEC 2382-1:1993 – *Information technology. Vocabulary. Part 1: Fundamental terms.*

ISO/IEC Guide 51:1999 – *Safety aspects. Guidelines for their inclusion in standards.*

ISO 9000:2000 – *Sistemas de gestión de la calidad. Fundamentos y vocabulario*. (ISO 9000:2005)

ISO 9000-3:1997 – *Quality management and quality assurance standards. Part 3: Guidelines for the application of ISO 9001:1994 to the development, supply, installation and maintenance of computer software.*

ANEXO ZA (Normativo)

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

Las normas que a continuación se indican son indispensables para la aplicación de esta norma. Para las referencias con fecha, sólo se aplica la edición citada. Para las referencias sin fecha se aplica la última edición de la norma (incluyendo cualquier modificación de ésta).

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)]
IEC 60654-1	1993	Condiciones de funcionamiento de los equipos de medida y control de los procesos industriales. Parte 1: Condiciones climáticas	EN 60654-1	1993	UNE-EN 60654-1:1999
IEC 60654-3	1983	Condiciones de funcionamiento de los equipos de medida y control de los procesos industriales. Parte 3: Influencias mecánicas	EN 60654-3	1997	UNE-EN 60654-3:1998
IEC 61326	–[2)]	Material eléctrico para medida, control y uso en laboratorio. Requisitos de compatibilidad electromagnética (CEM). Parte 1: Requisitos generales	EN 61326	1997[3)]	UNE-EN 61326:1999
IEC 61508-2	–[2)]	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[3)]	UNE-EN 61508-2:2003
IEC 61508-3	–[2)]	Seguridad funcional de los sistemas eléctricos/electrónicos/electrónicos programables relacionados con la seguridad. Parte 3: Requisitos del software (soporte lógico)	EN 61508-3	2001[3)]	UNE-EN 61508-3:2003
IEC 61511-2	–[2)]	Seguridad funcional. Sistemas instrumentados de seguridad para el sector de las industrias transformadoras. Parte 2. Directrices para la aplicación de la Norma IEC 61511-1	EN 61511-2	2004[3)]	UNE-EN 61511-2[4)]

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

2) Referencia sin fecha.

3) Edición válida en la fecha de publicación.

4) En preparación.

Dirección C Génova, 6
28004 MADRID-España
Teléfono 91 432 60 00
Fax 91 310 40 32