IEC 61069-7

Edición 2.0 2016-06

ESTÁNDAR INTERNACIONAL.

Medición, control y automatización de procesos industriales. Valoración de las propiedades del sistema para fines de su evaluación. Parte 7: Evaluación de la seguridad del sistema.

COMISIÓN
ELECTROTECNICO
INTERNACIONAL

color dentro

ICS 25.040.40 ISBN 978-2-8322-3450-1

CONTENIDO

COMISIÓN ELECTROTÉCNICA INTERNACIONAL

_____

MEDICIÓN, CONTROL Y AUTOMATIZACIÓN DE PROCESOS INDUSTRIALES - EVALUACIÓN VALORACIÓN DE LAS PROPIEDADES DEL SISTEMA PARA FINES DE SU EVALUACIÓN - PARTE 7: EVALUACIÓN DE LA SEGURIDAD DEL SISTEMA

PREFACIO

1) La Comisión Electrotécnica Internacional (IEC) es una organización mundial de estandarización que comprende todos los comités electrotécnicos nacionales (Comités Nacionales IEC). El objetivo de IEC es promover la cooperación internacional en todas las cuestiones relacionadas con la estandarización en los campos eléctrico y electrónico. Con este fin y además de otras actividades, IEC publica Estándares internacionales, Especificaciones técnicas, Informes técnicos, Especificaciones disponibles públicamente (PAS) y Guías (en adelante, "Publicaciones de IEC"). Su preparación se confía a los comités técnicos; cualquier comité nacional de IEC interesado en el tema tratado puede participar en este trabajo preparatorio. Las organizaciones internacionales, gubernamentales y no gubernamentales que se relacionan con la IEC también participan en esta preparación. IEC colabora estrechamente con la Organización Internacional de Normalización (ISO) de acuerdo con las condiciones determinadas por acuerdo entre las dos organizaciones.

2) Las decisiones o acuerdos formales de IEC sobre asuntos técnicos expresan, lo antes posible, un consenso internacional de opinión sobre los temas relevantes ya que cada comité técnico tiene representación de todos los Comités Nacionales de IEC interesados.

3) Las publicaciones de IEC tienen la forma de recomendaciones para uso internacional y son aceptadas por los Comités Nacionales de IEC en ese sentido. Si bien se realizan todos los esfuerzos razonables para garantizar que el contenido técnico de las Publicaciones de IEC sea exacto, IEC no se hace responsable de la forma en que se utilizan o de cualquier mala interpretación por parte de cualquier usuario final.

4) Para promover la uniformidad internacional, los Comités Nacionales de IEC se comprometen a aplicar las Publicaciones de IEC de manera transparente en la mayor medida posible en sus publicaciones nacionales y regionales. Cualquier divergencia entre cualquier publicación IEC y la publicación nacional o regional correspondiente se indicará claramente en esta última.

5) IEC en sí no proporciona ninguna certificación de conformidad. Los organismos de certificación independientes proporcionan servicios de evaluación de la conformidad y, en algunas áreas, acceso a las marcas de conformidad IEC. IEC no es responsable de ningún servicio realizado por organismos de certificación independientes.

6) Todos los usuarios deben asegurarse de tener la última edición de esta publicación.

7) No se responsabilizará a IEC ni a sus directores, empleados, servidores o agentes, incluidos expertos individuales y miembros de sus comités técnicos y de los Comités Nacionales de IEC por daños personales, daños a la propiedad u otros daños de cualquier naturaleza, ya sea directa o indirecta. , o por los costos (incluidos los honorarios legales) y los gastos derivados de la publicación, uso o dependencia de esta publicación de IEC o de cualquier otra publicación de IEC.

8) Se llama la atención a las referencias normativas citadas en esta publicación. El uso de las publicaciones referenciadas es indispensable para la correcta aplicación de esta publicación.

9) Se llama la atención sobre la posibilidad de que algunos de los elementos de esta publicación IEC puedan estar sujetos a derechos de patente. IEC no será responsable de identificar ninguno o todos los derechos de patente.

La Norma Internacional IEC 61069-7 ha sido preparada por el subcomité 65A: Aspectos del sistema, del comité técnico 65 de IEC: Medición, control y automatización de procesos industriales.

Esta segunda edición cancela y reemplaza la primera edición publicada en 1999. Esta edición constituye una revisión técnica.

Esta edición incluye los siguientes cambios técnicos significativos con respecto a la edición anterior:

a) reorganización del material de IEC 61069-7: 1999 para hacer que el conjunto general de estándares sea más organizado y consistente;

b) IEC TS 62603-1 se ha incorporado a esta edición.

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

FDIS	Reporte sobre la votación
65A / 795 / FDIS	65A / 805 / RVD

La información completa sobre la votación para la aprobación de esta norma se puede encontrar en el informe sobre votación indicado en la tabla anterior.

Esta publicación ha sido redactada de acuerdo con las Directivas ISO / IEC, Parte 2.

En el sitio web de IEC se puede encontrar una lista de todas las partes de la serie IEC 61069, publicada bajo el título general Medición, control y automatización de procesos industriales: valoración de las propiedades del sistema para fines de su evaluación.

El comité ha decidido que el contenido de esta publicación permanecerá sin cambios hasta la fecha de estabilidad indicada en el sitio web de IEC en "http://webstore.iec.ch" en los datos relacionados con la publicación específica. En esta fecha, la publicación le será

- reconfirmado,
- retirado,
- reemplazado por una edición revisada, o
- modificado.

IMPORTANTE: el logotipo de "color dentro" en la portada de esta publicación indica que contiene colores que se consideran útiles para la correcta comprensión de su contenido. Por lo tanto, los usuarios deben imprimir este documento con una impresora a color.

INTRODUCCIÓN

IEC 61069 trata con el método que debe usarse para evaluar las propiedades del sistema de un sistema de control básico (BCS). IEC 61069 consta de las siguientes partes:

Parte 1: Terminología y conceptos básicos.

Parte 2: metodología de evaluación.

Parte 3: Evaluación de la funcionalidad del sistema.

Parte 4: Evaluación del rendimiento del sistema.

Parte 5: Evaluación de la confiabilidad del sistema.

Parte 6: Evaluación de la operabilidad del sistema.

Parte 7: Evaluación de la seguridad del sistema.

Parte 8: Evaluación de otras propiedades del sistema.

La evaluación de un sistema es el juicio, basado en la evidencia, de la idoneidad del sistema para una misión específica o variedad de misiones.

Para obtener evidencia total se requeriría una evaluación completa (por ejemplo, bajo todos los factores que influyen) de todas las propiedades relevantes del sistema para la misión específica o variedad de misiones.

Dado que esto rara vez es práctico, el fundamento en el que debe basarse una evaluación de un sistema es:

- la identificación de la importancia de cada una de las propiedades relevantes del sistema;
- la planificación para la evaluación de las propiedades relevantes del sistema con una dedicación rentable de esfuerzo a las diversas propiedades del sistema.

Al realizar una evaluación de un sistema, es crucial tener en cuenta la necesidad de obtener el máximo de confianza en la idoneidad de un sistema dentro de las limitaciones prácticas de costo y tiempo.

Una evaluación solo puede llevarse a cabo si se ha declarado (o dado) una misión, o si se puede hipotetizar alguna misión. En ausencia de una misión, no se puede hacer una evaluación; sin embargo, es posible examinar el sistema para recopilar y organizar datos para una evaluación posterior realizada por otros. En tales casos, el estándar puede usarse como una guía para planificar una valoración y proporciona métodos para realizar evaluaciones, ya que las valoraciones son una parte integral de la evaluación.

Al preparar la evaluación, se puede descubrir que la definición del sistema es demasiado limitada. Por ejemplo, una instalación con dos o más sistemas de control que comparten recursos, por lo que la revisión de la red debería considerar cuestiones de coexistencia e interoperabilidad. En este caso, el sistema a investigar no debe limitarse al "nuevo" BCS; Debe incluir ambos. Es decir, debería cambiar los límites del sistema para incluir suficiente del otro sistema para abordar estas preocupaciones.

La estructura de la parte y la relación entre las partes de IEC 61069 se muestran en la Figura 1.

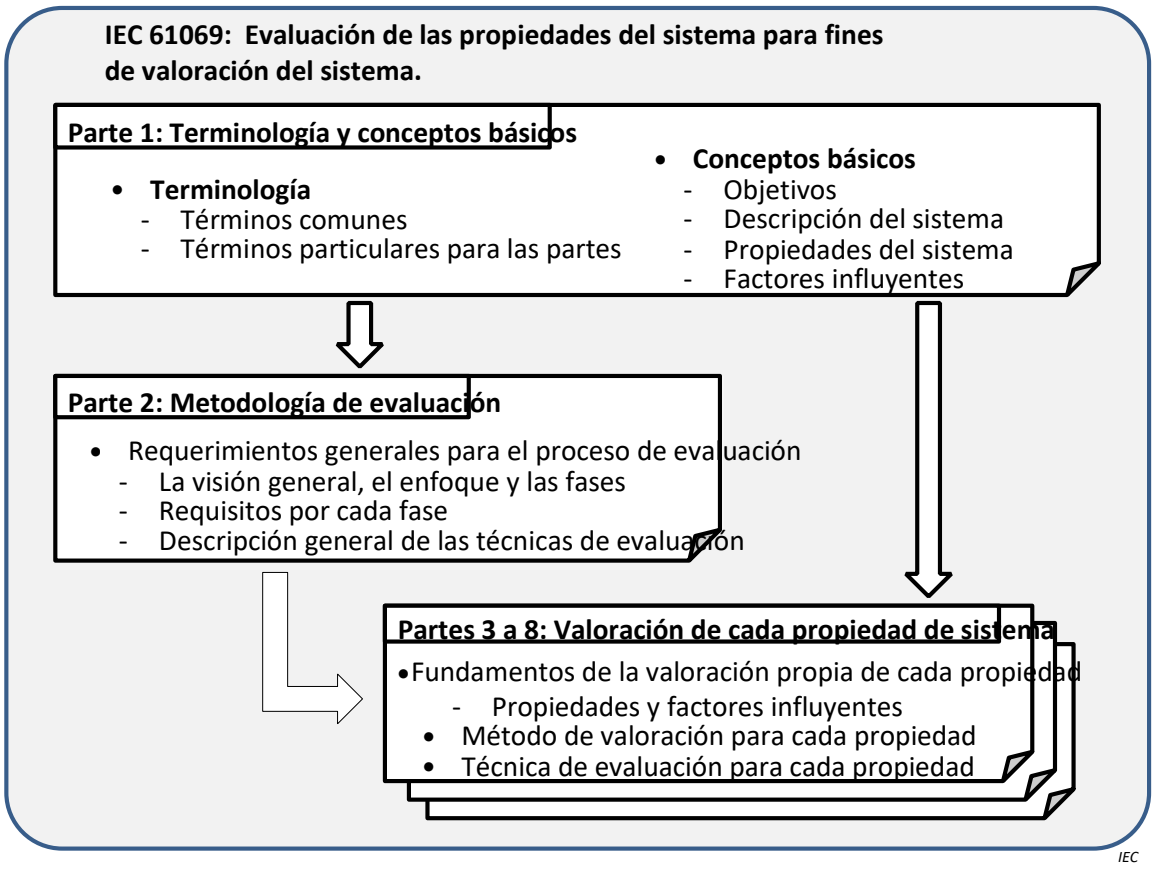


Figura 1 - Diseño general de IEC 61069.

MEDICIÓN, CONTROL Y AUTOMATIZACIÓN DE PROCESOS INDUSTRIALES - VALORACIÓN DE LAS PROPIEDADES DEL SISTEMA PARA FINES DE SU EVALUACIÓN - PARTE 7: EVALUACIÓN DE LA SEGURIDAD DEL SISTEMA.

1 Alcance.

Esta parte de IEC 61069:

- especifica el método detallado de evaluación de la seguridad de un sistema de control básico (BCS) basado en loAs conceptos básicos de IEC 61069-1 y la metodología de IEC 61069-2,

- define la categorización básica de las propiedades de seguridad del sistema,

- describe los factores que influyen en la seguridad del sistema y que deben tenerse en cuenta para la evaluación, y

- proporciona orientación para seleccionar técnicas, de un conjunto de opciones (con referencias) para evaluar la seguridad del sistema.

El tratamiento de seguridad en esta norma se limita a los riesgos que pueden estar presentes dentro del BCS. Es decir, el BCS en sí mismo como entidad física no impondrá un peligro.

Se excluyen las consideraciones de los peligros que pueden ser introducidos por el proceso o el equipo bajo control, del BCS a evaluar.

2 Referencias normativas.

Los siguientes documentos, en su totalidad o en parte, están referenciados normativamente en este documento y son indispensables para su aplicación. Para referencias fechadas, solo la edición citó aplicaciones. Para referencias sin fecha, se aplica la última edición del documento referenciado (incluidas las enmiendas).

IEC 61069-1: 2016, Medición, control y automatización de procesos industriales. Evaluación de las propiedades del sistema para fines de evaluación del sistema. Parte 1: Terminología y conceptos básicos.

IEC 61069-2: 2016, Medición, control y automatización de procesos industriales. Evaluación de las propiedades del sistema para fines de evaluación del sistema. Parte 2: Metodología de evaluación.

3 Términos, definiciones, términos abreviados, acrónimos, convenciones y símbolos.

3.1 Términos y definiciones.

Para los propósitos de este documento, se aplican los términos y definiciones dados en IEC 61069-1.

3.2 Términos abreviados, acrónimos, convenciones y símbolos.

Para los propósitos de este documento, se aplican los términos abreviados, acrónimos, convenciones y símbolos dados en IEC 61069-1.

4 Bases de evaluación específicas para la seguridad.

4.1 Propiedades de seguridad del sistema.

4.1.1 Generalidades

Un sistema puede tener varias interacciones con su entorno, algunas de las cuales pueden imponer una condición peligrosa.

Esta norma se concentra en las condiciones del sistema que pueden causar daños. Es importante reconocer que estas condiciones pueden cambiar a lo largo del ciclo de vida del sistema.

La medida en que el sistema está libre de peligros se puede expresar como propiedades de seguridad del sistema. Un sistema no siempre está libre de riesgos, incluso si las partes individuales que lo componen están libres de los mismos; por ejemplo, las partes individuales pueden ser estables, mientras que las mismas partes configuradas para formar un sistema pueden ser inestables y, por lo tanto, peligrosas.

Las propiedades de seguridad del sistema de un BCS en todos sus aspectos (mecánico, eléctrico, etc.) dependen de factores de su diseño y de su fiabilidad.

La evaluación de la seguridad del sistema debe incluir la evaluación de las propiedades de seguridad del sistema relacionadas con las actividades y medidas para el sistema durante cada fase de su ciclo de vida.

Ejemplos de estas actividades y medidas son:

- procedimientos de operación, mantenimiento y desmantelamiento,

- símbolos y advertencias textuales,

- eliminación de material de embalaje, productos de desecho del equipo, componentes reemplazados y material de limpieza.

La evaluación también debe incluir aspectos ambientales.

Las propiedades de seguridad del sistema pueden cambiar en las diferentes fases de su ciclo de vida debido a la cantidad de condiciones peligrosas presentes, tales como:

- acumuladores hidráulicos donde las presiones pueden bloquearse mediante válvulas de retención,

- dispositivos con carga eléctrica (por ejemplo, condensadores),

- Residuos nucleares y productos químicos almacenados en contenedores expuestos a la corrosión.

Al evaluar la seguridad del sistema, se deben considerar los siguientes aspectos:

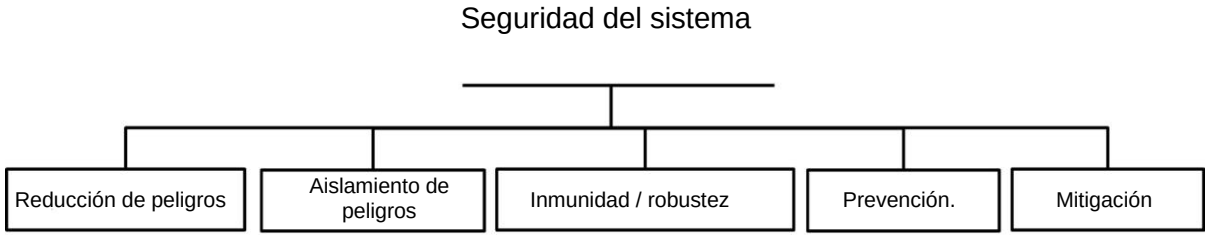
- tipos de peligros,

- receptores de las consecuencias de un peligro,

- caminos de propagación,

- medidas de reducción de riesgos.

Las propiedades de seguridad del sistema se clasifican como se muestra en la Figura 2.



IEC

Figura 2 - Seguridad del sistema.

La seguridad del sistema no puede evaluarse directamente y no puede describirse por una sola propiedad. La seguridad del sistema solo puede determinarse mediante análisis y pruebas de cada una de sus propiedades individualmente.

4.1.2 Reducción de riesgos.

La reducción del peligro es el esfuerzo por reducir el número y / o la gravedad del peligro.

Ejemplo: si se usa menos energía, es probable que las temperaturas de los dispositivos sean más bajas. Se utiliza la presión hidráulica más baja necesaria para transferir la potencia necesaria, para evitar la alta energía atrapada.

4.1.3 Aislamiento de peligro.

El aislamiento del peligro es el esfuerzo para aislar el peligro.

Ejemplo: instalación de disyuntores y desconectivos dentro de paneles diseñados para suprimir el arco eléctrico.

4.1.4 Inmunidad / robustez.

La inmunidad / robustez permite que el sistema absorba o sea inmune a los peligros.

Ejemplo: un BCS es inmune a los aumentos repentinos de la línea eléctrica un 20% más allá de su índice operativo. O puede absorber la interferencia EMC y aun así proporcionar transferencias de datos adecuadas.

4.1.5 Prevención.

La prevención permite que un sistema evite un peligro.

Ejemplo: se proporcionan enclavamientos o capacidad SIS para garantizar que el peligro no pueda ocurrir.

4.1.6 Mitigación.

La mitigación protege solo una parte del sistema si otros sistemas están comprometidos.

Ejemplo: las alarmas, y la evacuación son ejemplos en los que un peligro puede haberse hecho sentir, pero todavía se proporciona algún método para hacer el mejor esfuerzo para minimizar la pérdida.

4.2 Factores que influyen en la seguridad del sistema.

La seguridad del sistema puede verse afectada por los factores que influyen en la lista IEC 61069-1: 2016, 5.3.

En general, el factor más influyente son los seres humanos.

4.3 Peligros, daños y vías de propagación.

4.3.1 Tipos de peligros

4.3.1.1 Generalidades

Esta subcláusula abarca un conjunto de peligros.

Como mínimo, se deben considerar los tipos de riesgos tratados en 4.3.1.2 a 4.3.1.8.

Como se describe en el alcance, se excluyen las consideraciones de los peligros que pueden ser introducidos por el proceso o el equipo bajo control, del BCS a evaluar.

4.3.1.2 Mecánico.

El peso puede ser una fuente de daño, por ejemplo, durante el levantamiento o al caerse.

La presión puede ser una fuente de daño, por ejemplo, debido a la rotura de tuberías o contenedores.

La elasticidad puede ser una fuente de daño, por ejemplo, debido a la rotura de resortes o estructuras mecánicas.

La vibración puede ser una fuente de daño, por ejemplo, debido a la fatiga del material o la emisión de sonido excesivo.

La temperatura puede ser una fuente de daños, por ejemplo, debido a elementos que se calientan por fricción, enfriamiento insuficiente, aislamiento deficiente / defectuoso. En ciertas circunstancias, el frío extremo también puede ser peligroso al reducir la flexibilidad y afectar el tejido humano.

El desgaste puede ser una fuente de daño, por ejemplo, debido a la liberación de partículas tóxicas o debido al debilitamiento de las piezas.

El diseño mecánico puede ser una fuente de daños, por ejemplo, debido a la incorporación de bordes afilados o superficies rugosas.

4.3.1.3 Eléctrico.

El voltaje o la corriente pueden ser una fuente de daños, por ejemplo, debido a cortocircuitos (calor) u omisión del aislamiento (descarga eléctrica).

NOTA Las energías eléctricas que son las fuentes de riesgos pueden originarse dentro del sistema y / o de la fuente de alimentación del sistema.

4.3.1.4 Campo electromagnético.

El sistema puede emitir campos electromagnéticos de diferentes intensidades y frecuencias que pueden ser una fuente de daño. Los límites de emisión para el equipo se dan en el producto relevante, la familia de productos y los estándares genéricos de EMC, por ejemplo, CISPR 22. Puede encontrar orientación sobre los límites de daños a los humanos, por ejemplo, en ENV 50166-1 y ENV 50166-2.

4.3.1.5 Luz.

El sistema puede emitir luz de diferentes intensidades y frecuencias que pueden ser una fuente de daño; por ejemplo, el cortocircuito o el funcionamiento de los emisores ópticos (como las fuentes láser) pueden producir y propagar luz a una intensidad que puede alcanzar un nivel peligroso. Para fuentes láser, consulte IEC 60825-1.

4.3.1.6 Radioactividad.

Un sistema que incluye elementos radiactivos (como sensores) puede ser una fuente de daño.

4.3.1.7 Biológico.

Un sistema que incluye elementos biológicos (como sensores) puede ser una fuente de daño.

4.3.1.8 Químico.

Un sistema que incluye sustancias químicas puede ser una fuente de daño (por ejemplo, toxicidad o corrosión).

4.3.2 Receptores de daños.

4.3.2.1 Generalidades

El nivel de daño que puede ser aceptado por un receptor depende de

- las características del tipo de receptor y

- el área en la que se encuentra el receptor.

Dentro del entorno de un BCS, se pueden identificar diferentes áreas, como la sala de control, la instalación de fabricación o el área que rodea la instalación de fabricación. Estas clasificaciones de área se dan típicamente en estándares internacionales, nacionales o patentados. Dentro de cada una de estas áreas, los niveles individuales de daños y situaciones peligrosas pueden ser aceptables para cada tipo de receptor.

Los diferentes tipos de receptores se enumeran en 4.3.2.2 a 4.3.2.4.

4.3.2.2 Humanos.

Los peligros que pueden existir en el BCS pueden afectar al cuerpo humano de diferentes maneras. Algunos ejemplos se dan a continuación:

a) mecánico:

1) el peso puede, por ejemplo, romper huesos;

2) el exceso de presión puede, por ejemplo, provocar lesiones generales, fractura de huesos, daños en los ojos y / o los oídos, o el colapso de los pulmones;

3) la elasticidad puede, por ejemplo, provocar lesiones generales o la rotura de huesos;

4) la vibración puede, por ejemplo, provocar daños en el oído;

5) la temperatura puede, por ejemplo, provocar quemaduras;

b) un cortocircuito eléctrico o una descarga eléctrica pueden, por ejemplo, causar quemaduras, fibrilación del corazón o daños oculares;

c) los campos electromagnéticos pueden, por ejemplo, causar alteración del metabolismo, daño ocular o destrucción de un órgano;

d) la luz puede, por ejemplo, causar daño ocular o quemaduras;

e) la radiactividad puede, por ejemplo, alterar el metabolismo, dañar los ojos o destruir un órgano;

f) las sustancias biológicas pueden penetrar y, por ejemplo, alterar el metabolismo o modificar la vía alimentaria;

g) las sustancias químicas pueden penetrar y, por ejemplo, causar alteración del metabolismo, daño ocular, destrucción de un órgano, irritación de la piel o daño neurológico.

4.3.2.3 Biológico.

Los peligros que pueden existir en el BCS pueden afectar los sistemas biológicos como la flora, la fauna y el sistema ecológico, de manera similar a la descrita en 4.3.2.2. El grado de daño físico a un sistema biológico puede ser diferente del de un humano.

4.3.2.4 Equipamiento.

Los peligros que pueden existir en el BCS pueden afectar el equipo circundante de diferentes maneras. Algunos ejemplos se dan a continuación:

a) mecánico:

1) el peso, la presión y la elasticidad pueden, dependiendo de la gravedad, provocar desalineación, doblar o romper piezas, etc .;

2) la vibración puede, dependiendo de la gravedad, provocar una desalineación, fatiga del metal, piezas sueltas, etc .;

3) la temperatura puede, según su nivel, provocar desalineación, disminución del tiempo de vida, pérdida de resistencia mecánica, desgasificación, quemaduras, etc .;

b) las fuentes eléctricas pueden, según la gravedad, provocar una distorsión de la alimentación, averías debido a sobrecargas, sobrecargas de corriente, descargas disruptivas, quemaduras, etc .;

c) los campos electromagnéticos pueden, dependiendo de la gravedad, provocar interferencias electromagnéticas, alteración de los datos, etc .;

d) la luz o la radiactividad pueden, dependiendo del nivel, provocar cambios en las propiedades del material debido a la luz ultravioleta o láser, etc .;

e) biológico: sin efecto previsto ;

f) las sustancias químicas pueden, dependiendo de la gravedad, provocar una transformación química del material, etc.

4.3.3 Rutas de propagación.

4.3.3.1 Generalidades

Para que un peligro sea dañino, hay una ruta de propagación entre la fuente del daño y el receptor.

Aunque se pueden identificar rutas de propagación únicas, es muy frecuente que una ruta de propagación completa sea una combinación de varios tipos de rutas de propagación.

Algunas rutas de propagación individuales se enumeran en 4.3.3.2 a 4.3.3.5.

4.3.3.2 Ruta de propagación directa.

Una ruta de propagación directa significa que el receptor está en contacto directo con la fuente de daño (por ejemplo, un dedo tocando un conductor de alto voltaje).

4.3.3.3 Ruta de propagación indirecta.

Una ruta de propagación indirecta significa que el receptor está en contacto con la fuente de daño a través de cualquier elemento móvil (por ejemplo, una herramienta o una escalera) o un elemento de construcción fijo (por ejemplo, soportes o rieles).

4.3.3.4 Ruta de propagación dinámica.

Una ruta de propagación dinámica significa que el receptor está en contacto dependiente del tiempo con la fuente de daño a través de cualquier medio dinámico (por ejemplo, líquidos o gases que fluyen).

4.3.3.5 Ruta de propagación sin contacto.

Una ruta de propagación sin contacto significa que el receptor está expuesto a la fuente de daño a través de, por ejemplo, radiaciones, luz o campos electromagnéticos.

5 Método de evaluación.

5.1 Generalidades

La evaluación deberá seguir el método establecido en IEC 61069-2: 2016, Cláusula 5.

5.2 Definición del objetivo de la evaluación.

La definición del objetivo de la evaluación debe seguir el método establecido en IEC 61069-2: 2016, 5.2.

5.3 Diseño y disposición de la evaluación.

El diseño y la disposición de la evaluación deberán seguir el método establecido en IEC 610692: 2016, 5.3.

La definición del alcance de la evaluación debe seguir el método establecido en IEC 61069-2: 2016, 5.3.1.

La recopilación de información documentada se realizará de acuerdo con IEC 61069-2: 2016, 5.3.3.

Las declaraciones compiladas de acuerdo con IEC 61069-2: 2016, 5.3.3 s deben incluir lo siguiente además de los elementos enumerados en IEC 61069-2: 2016, 5.3.3:

- tipos de peligros y sus rutas de propagación del sistema a su entorno;

- factores influyentes que pueden crear una condición peligrosa dentro del sistema;

- medidas de reducción de riesgos proporcionadas para minimizar las consecuencias de condiciones peligrosas;

- medidas de reducción de riesgos proporcionadas para minimizar la probabilidad de que pueda surgir una conjunción de fenómenos que puedan crear condiciones peligrosas;

- la forma en que interactúan los diferentes módulos y elementos del sistema y la posibilidad de que pueda surgir una falta de seguridad a nivel del sistema como resultado de las interacciones;

- conocimiento previo global disponible y la medida en que se debe evaluar la propiedad de seguridad del sistema.

La documentación de la información recopilada debe seguir el método de IEC 61069-2: 2016, 5.3.4.

La selección de los elementos de evaluación debe seguir la norma IEC 61069-2: 2016, 5.3.5.

La especificación de evaluación debe desarrollarse de acuerdo con IEC 61069-2: 2016, 5.3.6.

La comparación del SRD y el SSD deberá seguir la norma IEC 61069-2: 2016, 5.3.

NOTA 1 En el Anexo A se proporciona una lista de verificación de SRD para la confiabilidad del sistema.

NOTA 2 En el Anexo B se proporciona una lista de verificación de SSD para la confiabilidad del sistema.

5.4 Planificación del programa de evaluación.

La planificación del programa de evaluación debe seguir el método establecido en IEC 61069-2: 2016, 5.4.

Las actividades de evaluación se desarrollarán de acuerdo con IEC 61069-2: 2016, 5.4.2.

El programa de evaluación final debe especificar los puntos especificados en IEC 61069 -2: 2016, 5.4.3.

5.5 Ejecución de la evaluación.

La ejecución de la evaluación se realizará de acuerdo con IEC 61069-2: 2016, 5.5.

5.6 Informe de la evaluación.

El informe de la evaluación debe estar de acuerdo con IEC 61069-2: 2016, 5.6.

El informe debe incluir la información especificada en IEC 61069-2: 2016, 5.6. Además, el informe de evaluación debe abordar los siguientes puntos:

- No se observan elementos adicionales.

6 Técnicas de evaluación.

6.1 Generalidades

Dentro de este estándar, se sugieren varias técnicas de evaluación. Se pueden aplicar otros métodos, pero, en todos los casos, el informe de evaluación debe proporcionar referencias a los documentos que describen las técnicas utilizadas.

Esas técnicas de evaluación se clasifican como se describe en IEC 61069-2: 2016, Cláusula 6.

Se deben tener en cuenta los factores que influyen en la seguridad del sistema de acuerdo con 4.2.

Las técnicas dadas en 6.2, 6.3 y 6.4 se recomiendan para evaluar la seguridad del sistema.

No es posible evaluar las propiedades de seguridad del sistema como una sola entidad. En cambio, las propiedades de seguridad de cada sistema deben abordarse por separado.

6.2 Técnicas de evaluación analítica

Las técnicas de evaluación de seguridad para BCS son principalmente analíticas.

Para cada tipo de peligro, se deben seguir los siguientes pasos:

- verifique si hay un peligro presente y, para cada peligro presente, verifique si las certificaciones están disponibles y también son válidas bajo las condiciones de operación establecidas en el SRD o por las regulaciones obligatorias;

- si no se dispone de certificaciones satisfactorias, se debe aplicar un análisis de riesgo apropiado, por ejemplo, el análisis descrito en ISO 31010. En apoyo de dicho análisis, se puede aplicar una de las técnicas de evaluación de 6.3.

6.3 Técnicas de evaluación empírica.

Las técnicas de evaluación empírica son complementarias a las analíticas.

Siempre que las técnicas analíticas no puedan garantizar el nivel de seguridad del sistema, se debe realizar una evaluación empírica para evaluar aquellos aspectos en los que faltan datos.

Siempre se llevará a cabo una evaluación empírica cuando lo requieran los organismos reguladores (consulte también IEC 61069-2: 2016, 5.3.5).

Para este propósito, se pueden aplicar varias técnicas, de las cuales se enumeran las siguientes para la guía:

- mecánico: métodos de prueba de recintos como se describe, por ejemplo, en IEC 60529;

- eléctrico: coordinación de aislamiento y pruebas de resistencia eléctrica como se describe, por ejemplo, en las series IEC 60243 e IEC 60664-1;

- campos electromagnéticos: técnicas de medición descritas, por ejemplo, en CISPR 22;

- térmica: prueba de peligro de incendio como se describe, por ejemplo, en IEC 60695-2, IEC 60695-11-10 e IEC 60695-11-20.

6.4 Temas adicionales para técnicas de evaluación.

No se observan elementos adicionales.

Anexo A

(informativo)

Lista de verificación y / o ejemplo de SRD para la funcionalidad del sistema

El documento de requisitos del sistema debe revisarse para verificar que las medidas de reducción de riesgos requeridas para el sistema se hayan abordado y se enumeren como se describe en I EC 61069-2.

La efectividad de la evaluación de seguridad depende en gran medida de la exhaustividad de la declaración de requisitos.

Se debe prestar especial atención a verificar que se brinde información adecuada sobre:

- las normas o reglamentaciones de seguridad internacionales, nacionales o empresariales aplicables y, en particular, las normas IEC 60664-1 e IEC 61010-1,

- los niveles de emisión admisibles para los tipos de peligros enumerados en 4.2,

- las áreas donde se ubicarán el BCS y sus módulos y elementos, en referencia a los estándares de clasificación de áreas, por ejemplo,

- las condiciones de trabajo dentro de estas áreas que deben cumplirse para permitir el acceso al BCS, y los procedimientos para obtener permisos de trabajo,

- las infracciones permitidas de estas condiciones de trabajo, su frecuencia y los procedimientos de emergencia a seguir en este caso,

- los niveles de emisión admisibles para los tipos de riesgos enumerados en 4.2 para las áreas vecinas del BCS,

- la medida en que el BCS está destinado a ser utilizado para proporcionar funciones de seguridad fuera del alcance de la serie IEC 61508.

Anexo B

(informativo)

Lista de verificación y / o ejemplo de SSD para la funcionalidad del sistema

B.1 Información de SSD

El documento de especificación del sistema debe revisarse para verificar que las propiedades dadas en el SRD se enumeran como se describe en IEC 61069-2: 2016, Cláusula B.2.

B.2 Puntos de verificación para la seguridad del sistema

El documento de especificación del sistema debe revisarse para verificar que las medidas de reducción de riesgos del BCS se enumeran como se describe en IEC 61069-2.

Se debe prestar especial atención a verificar que se brinde información adecuada sobre lo siguiente:

- tipos de peligro dentro del BCS, y las medidas de reducción de riesgos tomadas para limitar las posibles consecuencias;

- niveles de emisiones, incluso si son inferiores a los límites seguros y / o permitidos;

- certificaciones de seguridad apropiadas, instituciones emisoras y coherencia con las reglamentaciones nacionales;

- cualquier acción de mantenimiento requerida que pueda infringir la seguridad del sistema y las precauciones a tomar en estas circunstancias, para evitar condiciones peligrosas; - requisitos especiales de instalación para garantizar la seguridad del sistema.

Bibliografía

[1] IEC 60243 (todas las partes), Resistencia eléctrica de materiales aislantes - Métodos de prueba

[2] IEC 60529, Grados de protección proporcionados por los gabinetes (Código IP)

[3] IEC 60695-2 (todas las partes), Prueba de peligro de incendio - Parte 2: Métodos de prueba

[4] IEC 60664-1, Coordinación de aislamiento para equipos dentro de sistemas de baja tensión. Parte 1: Principios, requisitos y pruebas.

[5] IEC 60695-11-10, Prueba de peligro de incendio - Parte 11-10: Llamas de prueba - Métodos de prueba de llama horizontal y vertical de 50 W

[6] IEC 60695-11-20, Prueba de peligro de incendio - Parte 11-20: Llamas de prueba - Método de prueba de llama de 500 W

[7] IEC 60825-1, Seguridad de los productos láser. Parte 1: Clasificación y requisitos del equipo.

[8] IEC 61010-1: 2010, Requisitos de seguridad para equipos eléctricos de medición, control y uso en laboratorio . Parte 1: Requisitos generales

[9] IEC 61069-3, Medición, control y automatización de procesos industriales. Evaluación de las propiedades del sistema para fines de evaluación del sistema. Parte 3: Evaluación de la funcionalidad del sistema.

[10] IEC 61069-4, Medición, control y automatización de procesos industriales. Evaluación de las propiedades del sistema para fines de evaluación del sistema. Parte 4: Evaluación del rendimiento del sistema.

[11] IEC 61069-5: 2016, Medición, control y automatización de procesos industriales. Evaluación de las propiedades del sistema para fines de evaluación del sistema. Parte 5: Evaluación de la confiabilidad del sistema.

[12] IEC 61069-6: 2016, Medición, control y automatización de procesos industriales. Evaluación de las propiedades del sistema para fines de evaluación del sistema. Parte 6: Evaluación de la operatividad del sistema.

[13] IEC 61069-8, Medición, control y automatización de procesos industriales. Evaluación de las propiedades del sistema para fines de evaluación del sistema. Parte 8: Evaluación de otras propiedades del sistema.

[14] IEC 61508 (todas las partes), Seguridad funcional de sistemas eléctricos / electrónicos electrónicos / programables relacionados con la seguridad

[15] IEC TS 62603-1, Sistemas de control de procesos industriales. Directriz para evaluar sistemas de control de procesos. Parte 1: Especificaciones.

[16] CISPR 22, Equipos de tecnología de la información. Características de las perturbaciones radioeléctricas. Límites y métodos de medición.

[17] Guía ISO / IEC 51, Aspectos de seguridad: directrices para su inclusión en las normas

[18] ISO 31010: 2009, Gestión de riesgos. Técnicas de evaluación de riesgos.

[19] ENV 50166-1, Exposición humana a campos electromagnéticos. Baja frecuencia y (0 Hz a 10 kHz)

[20] ENV 50166-2, Exposición humana a campos electromagnéticos. Alta frecuencia (10 kHz a 300 GHz)