

SIS 103

Normas de seguridad

15 minutos

En este curso:

- O Generalidades
- 1 Un nuevo enfoque
- 2 De IEC 61508 surgió IEC 61511
- 3 ¿Qué hay de S84?
- 4 Modelos de ciclo de vida
- 5 Aplicación del modelo en 61511
- 6 Recursos para cumplimiento
- 7 Beneficios del cumplimiento
- 8 Sumario
- Q Examen

© 2005 Emerson Process Management. Todos los derechos reservados.

Generalidades

Si su planta o proceso todavía no está usando normas de seguridad tales como IEC 61508, IEC 61511 y/o ANSI/ISA S84.00.01-2004, lo más probable es que lo hará en un futuro cercano.

Aunque al principio usted piense que son fuentes de papeleo, molestias y dolores de cabeza, estas normas juegan un papel vital para hacer que su planta sea segura – y mantenerla así. Su disciplinado enfoque también puede ayudar a garantizar que su sistema de control del proceso, sus procedimientos operativos y de mantenimiento y sus sistemas de seguridad estén en armonía de tal manera que se logre un mejor rendimiento operativo.

Este curso introduce las normas de seguridad más relevantes – IEC 61508, IEC 61511 y ANSI/ISA S84.00.01-2004 – y explica por qué cumplir con ellas tiene sentido desde un punto de vista de negocios.

¿Qué significan todos esos acrónimos?

IEC – Comisión Electrotécnica Internacional <www.iec.ch>

ISA – Sociedad de Instrumentación, Sistemas y Automatización <www.isa.org>

ANSI – Instituto Nacional Americano de Normas <www.ansi.org>

Al final del curso, usted encontrará un breve examen que puede usar para confirmar lo que ha aprendido – y ganar valiosos Puntos de Recompensa.

Sugerencia

Mientras estudia los temas de este curso, preste especial atención a lo siguiente:

- Cómo han cambiado las normas de seguridad.
- Qué norma es su mejor elección para nuevas aplicaciones de seguridad
- Los beneficios de modelos de ciclo de vida basados en normas
- Qué clases de recursos se requieren para el cumplimiento
- Los beneficios clave del cumplimiento

¿Listo(a) para comenzar? Sólo haga clic en el icono “>” a continuación.

Un nuevo enfoque

En el pasado, las normas de seguridad se desarrollaban para una aplicación, industria o país específicos. Por ejemplo, ANSI P1.1-1969 es una norma de consenso en la industria emitida por el Instituto Nacional Americano de Estándares) que define los requisitos de seguridad para las fábricas que producen pulpa, papel y cartón.

El principal problema con este enfoque es que las plantas, e incluso industrias completas, se han encontrado tratando de cumplir con múltiples normas de seguridad que se traslapan, a menudo desarrolladas usando filosofías de diseño y arquitectura completamente diferentes. Agregue las diferencias de normas nacionales o regionales; con todo esto es casi imposible estar seguro de que se ha logrado el cumplimiento.

Las normas de seguridad más recientes, sin embargo, han sido desarrolladas usando un enfoque que se concentra en la reducción del riesgo y en el establecimiento de un grado definido de excelencia operacional en cada etapa del ciclo de vida del proyecto de seguridad.

Este enfoque de **ciclo de vida** basado en el rendimiento produce una norma que se acopla más fácilmente con otras normas, logrando así que sean más atractivas y aceptadas. También es más fácil producir resultados de alta calidad al menor costo posible.

Para las industrias de procesos, las normas de seguridad relevantes son IEC 61508, IEC 61511 y ANSI/ISA S84.00.01-2004 (S84). Cada una de estas normas define **qué** se requiere para lograr el cumplimiento normativo, pero en el caso de IEC 61511 y S84, éstas dejan los detalles de **cómo** lograr el cumplimiento a los propietarios y operadores de las plantas.

De IEC 61508 surgió IEC 61511

Entonces, ¿por qué la IEC tiene **dos** normas de seguridad?

IEC 61508 (Partes 1 – 7), titulada *Functional safety of programmable electronic safety-related systems* (Seguridad funcional de sistemas electrónicos programables relacionados con la seguridad), es una norma de seguridad completa, global y funcional que está basada en rendimiento y aplica a los fabricantes e implementadores de sistemas de seguridad funcionales en una amplia gama de industrias.

En Europa, las siete partes de IEC 61508 se publicaron como EN 61508, y todas las normas nacionales CENELEC o CEN en conflicto fueron retiradas subsecuentemente.

IEC 61508 fue usada por algunas plantas de la industria de procesos para implementar sistemas instrumentados de seguridad (SIS) que cumplieran con los requisitos normativos. Sin embargo, los que adoptaron la industria de procesos tempranamente notaron que la norma era incómoda y no era clara para la interpretación sobre cómo lograr el cumplimiento en estas industrias.

Después de una cuidadosa consideración, el comité de normas IEC extrajo las secciones relevantes de IEC 61508, las armonizó y las volvió a redactar para formar la norma IEC 61511 específicamente para industrias de procesos.

El resultado es que IEC 61511 proporciona guía de las industrias de procesos y ejemplos de cómo se implementa la norma – a la vez que sigue garantizando que se logre el cumplimiento dentro del marco establecido en IEC 61508.

Este enfoque hizo que la norma IEC 61511, *Functional safety: Safety instrumented systems for the process industry sector* (Seguridad funcional: Sistemas instrumentados de seguridad para el sector de las industrias de procesos), sea la norma de seguridad que eligen las industrias de procesos – como se hace evidente mediante el creciente número de referencias a ella por parte de las agencias de seguridad en China, Irlanda, Italia, India, Noruega, Reino Unido y los Estados Unidos; el número de ponencias que presentan los usuarios finales en conferencias y simposios; y las referencias en los sitios web de los fabricantes de sistemas de control.

Aunque las plantas todavía tienen la opción de aplicar la norma IEC 61508, su uso principal es por parte de los fabricantes de instrumentación y de sistemas de control que desarrollan y venden dispositivos SIS certificados para usarlos en las aplicaciones que cumplen con IEC 61511.

¿Qué hay de S84?

Muchas normas nacionales han sido reemplazadas por IEC 61508 y 61511. Un ejemplo es la norma de seguridad ANSI/ISA S84.01 que se usó ampliamente en los Estados Unidos.

Hace varios años, después de un desconcertante número de accidentes, los expertos en seguridad en la industria de procesos comenzaron una profunda revisión de las normas de seguridad existentes.

Incidentes que condujeron a las normas de seguridad mejoradas		
1968	Refinería en Pernis, Países Bajos	2 muertos, 85 lesionados
1974	Flixborough, Reino Unido	28 muertos, cientos de lesionados
1976	Seveso, Italia	700 lesionados
1984	Bhopal, India	2,500 muertos, 100,000 lesionados
1998	Piper Alpha, Mar del Norte	165 muertos, 61 lesionados

Entre sus conclusiones estaba la de que las normas existentes eran demasiado específicas a la industria y limitaban la habilidad de los expertos en seguridad de compartir las mejores prácticas.

A partir de sus descubrimientos se formó el comité ISA SP84. Casi inmediatamente, los miembros del comité estuvieron de acuerdo en que un enfoque de normas más adecuado sería usar un modelo de ciclo de vida basado en rendimiento. El resultado de su trabajo fue ANSI/ISA S84.01-1996, *Application of Safety Instrumented Systems for the Process Industries* (Aplicación de sistemas instrumentados de seguridad para las industrias de procesos) (S84).

Sin embargo, más recientemente, la norma S84 ha sido armonizada con IEC 61511, con una excepción: ANSI/ISA S84.00.01-2004 incluye una cláusula tipo “abuelo” que permite que las instalaciones que actualmente usan la versión 1996 de S84 continúen haciéndolo – siempre y cuando se determine que el equipo de seguridad se diseñe, se mantenga, se inspeccione, se pruebe y se opere en una manera segura.

Por lo tanto, a menos que ya esté usando la norma S84, su mejor elección sería dejar la antigua norma ANSI/ISA y adoptar IEC 61511 – que es lo mismo que S84-2004.

Modelos de ciclo de vida

Un modelo de ciclo de vida proporciona una estructura para una serie de procesos para crear o actualizar un producto o un servicio.



Los modelos de ciclo de vida pueden tomar muchas formas, pero cada una proporciona una estructura para enfocarse en las incontables tareas involucradas en la creación y gestión de un complejo producto o servicio.

Un importante beneficio de una norma basada en ciclo de vida es la facilidad que proporciona para usar e integrar otras normas o prácticas basadas en ciclo de vida. Como se muestra en la tabla, tales modelos son usados o recomendados por un número de agencias regulatorias y otros organismos.

Organizaciones y agencias que recomiendan el uso de modelos de ciclo de vida	
Organización Internacional de Normas (ISO)	Calidad del producto y del servicio
Oficina Ejecutiva de Salud y Seguridad del Reino Unido	Actividades relacionadas con la seguridad
Administración de Drogas y Alimentos de los Estados Unidos	Producción y aprobación de nuevas drogas
Instituto de Ingeniería de Software	Software de alta disponibilidad
Administración de Seguridad y Salud Laboral (OSHA) de los Estados Unidos	Seguridad de los trabajadores
Agencia de Protección Ambiental de los Estados Unidos	Protección ambiental

Por ejemplo, el Instituto de Ingeniería de Software <www.sei.cmu.edu> ha desarrollado un número de modelos de ciclo de vida de software, varios de los cuales se usan para crear software “que sobreviva” – es decir, software de aplicación crítico a la misión que requiera seguridad, tolerancia a fallas, seguridad, fiabilidad, reuso, rendimiento, verificación y pruebas.

Similarmente, las buenas prácticas de fabricación basadas en ciclo de vida son integrales a las industrias donde la calidad del producto es esencial, como las reguladas por la Administración de Drogas y Alimentos de los Estados Unidos.

Además de facilitar la integración de tales normas, la disciplina proporcionada por el enfoque de ciclo de vida ayuda a producir resultados de alta calidad al menor costo posible.

Aplicación del modelo en 61511

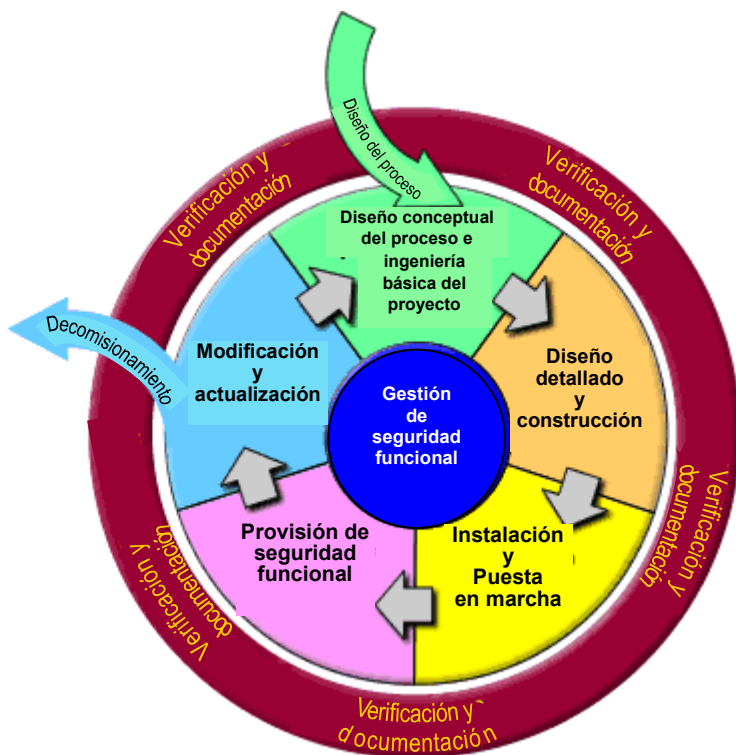
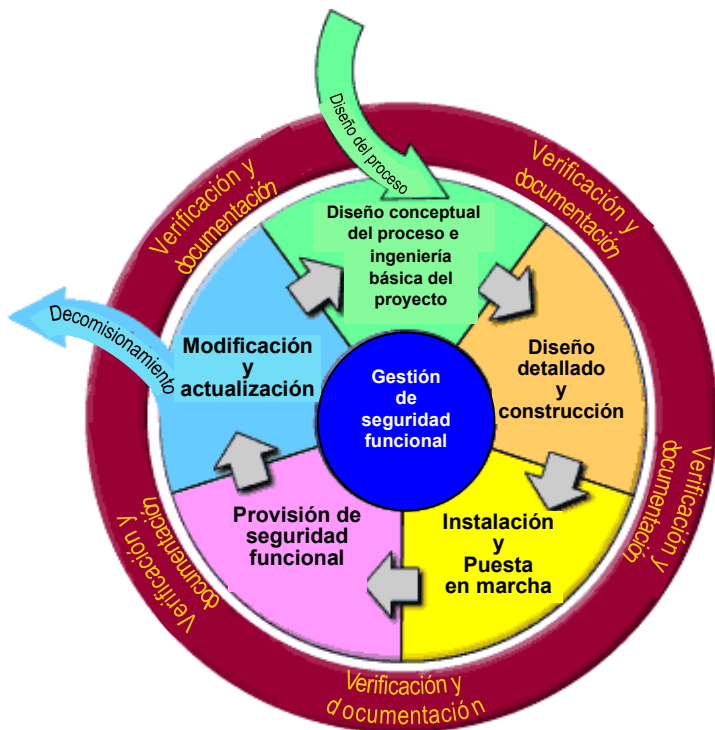
IEC 61511 permite personalizar el modelo de ciclo de vida para ajustarse a sus prácticas actuales – siempre y cuando se cumpla con los requisitos normativos.

Un enfoque usa cinco etapas principales de ciclo de vida para atender estos requisitos, además de un proceso de verificación y documentación a lo largo del ciclo:

Etapa de ciclo de vida	Requisitos de IEC 61511
1. Ingeniería básica del proyecto y diseño conceptual	<ul style="list-style-type: none"> ○ Evaluación de peligro y riesgo (<i>Cláusula 8</i>) ○ Asignación de funciones de seguridad a capas de protección (<i>Cláusula 9</i>) ○ Especificación de requisitos de seguridad para sistemas instrumentados de seguridad (<i>Cláusulas 10 y 11</i>)
2. Diseño e ingeniería detallados	<ul style="list-style-type: none"> ○ Diseño e ingeniería de sistemas instrumentados de seguridad (<i>Cláusulas 11 y 12.4</i>) ○ Construcción del sistema instrumentado de seguridad, integración y pruebas FAT (<i>Cláusula 13</i>)
3. Instalación y puesta en marcha	<ul style="list-style-type: none"> ○ Instalación y comisionamiento de sistemas instrumentados de seguridad (<i>Cláusula 14</i>) ○ Validación de seguridad de sistemas instrumentados de seguridad (<i>Cláusulas 12.3, 12.7 y 15</i>)
4. Provisión de seguridad funcional	<ul style="list-style-type: none"> ○ Operaciones y mantenimiento de sistemas instrumentados de seguridad (<i>Cláusula 16</i>)
5. Modificación y actualización	<ul style="list-style-type: none"> ○ Modificación de sistemas instrumentados de seguridad (<i>Cláusula 17</i>)
- Verificación y documentación (incluidas en cada etapa)	<ul style="list-style-type: none"> ○ Verificación (<i>Cláusulas 7, 12.4 y 12.7</i>) ○ Documentación (<i>Cláusula 19</i>)

Juntas, estas actividades permiten cumplir con el requisito central de la norma IEC 61511:

Gestión de seguridad funcional	<ul style="list-style-type: none"> ○ Gestión de seguridad funcional y evaluación y auditoría de la seguridad funcional (<i>Cláusula 5</i>) ○ Estructura de ciclo de vida de seguridad (<i>Cláusula 6.2</i>)
---------------------------------------	---



<p>Ingeniería básica del proyecto y diseño conceptual</p> <ul style="list-style-type: none"> • Crear diseño conceptual del proceso • Identificar peligros potenciales 	<p>Diseño detallado</p> <ul style="list-style-type: none"> • Diseño detallado de <ul style="list-style-type: none"> - instalación de dispositivos de campo del SIS - hardware de solucionadores lógicos del 	<p>Instalación y puesta en marcha</p> <ul style="list-style-type: none"> • Instalar los dispositivos de campo del SIS • Instalar los solucionadores lógicos del SIS • Integrar el SIS en el
--	--	---

<ul style="list-style-type: none"> • Asignar requisitos de seguridad • Decidir si se requiere un sistema instrumentado de seguridad (SIS) • Identificar niveles de riesgo tolerable y seleccionar niveles de integridad de seguridad objetivos • Crear una especificación de requisitos de seguridad • Seleccionar la tecnología, arquitectura y filosofía de pruebas de aceptación • Calcular el nivel de integridad de seguridad (SIL) para cada función de seguridad 	<p>SIS - Software del SIS</p> <ul style="list-style-type: none"> • Verificación del diseño • Construcción y verificación del hardware del solucionador lógico • Configuración del software del SIS y pruebas de la función de seguridad • Integración del solucionador lógico del SIS • Verificación de la integración (FAT) • Crear la documentación de la instalación y del comisionamiento • Crear la documentación de las operaciones y del mantenimiento 	<p>sistema de control básico del proceso según se requiera</p> <ul style="list-style-type: none"> • Verificar la instalación • Comisionar el SIS • Validar el SIS
<p>Provisión de seguridad funcional</p> <ul style="list-style-type: none"> • Operar y dar mantenimiento al SIS de acuerdo con los procedimientos documentados • Realizar las pruebas de aceptación como se define en el diseño para verificar la operación del SIS 	<p>Modificación y actualización</p> <ul style="list-style-type: none"> • Se evalúa el alcance de la modificación • Si el cambio no afecta el caso de seguridad, entonces se hace el cambio, y se completa toda la verificación requerida y se cambian los procedimientos de gestión • Si el cambio es significativo, entonces se repite el ciclo de vida de seguridad 	

Recursos para cumplimiento

Obviamente, decir que su compañía está comprometida a proporcionar un entorno de trabajo seguro no es suficiente. La gerencia tiene que proporcionar los recursos necesarios para cumplir ese compromiso – incluyendo los fondos adecuados, el personal y la capacitación. Eso es parte de la construcción del entorno y de la cultura que deben existir antes de que se pueda lograr el cumplimiento con IEC 61511.

La norma IEC 61511 requiere que haya personas con conocimiento y experiencia demostrados sobre ingeniería de seguridad adecuadas para el proceso y para las tecnologías de SIS que se estén usando. La norma también dice que la gente asignada para la ingeniería, diseño e implementación de los sistemas de seguridad deben tener

- capacitación adecuada,
- habilidades de gerencia y liderazgo adecuadas a su papel en las actividades de ciclo de vida de seguridad, y
- conocimiento de los requerimientos regulatorios legales y de seguridad aplicables.

Entonces, esto se convierte en el trabajo de estos profesionales de seguridad establecer evidencia documentada de que se ha definido, alcanzado y mantenido adecuadamente el cumplimiento con la norma de seguridad IEC.

Si usted no tiene todos los recursos correctos internamente, los proveedores y consultores conocedores le pueden ayudar. IEC 61511 es una norma internacional, su modelo de ciclo de vida es bien comprendido, y se aplica a un gran número de compañías. A medida que el número de compañías que lo usa aumenta, el número de recursos confiables también aumentará – haciendo que sea más fácil encontrar ayuda calificada.

La ventaja PlantWeb

Como proveedor del primer sistema instrumentado de seguridad inteligente en el ramo, Emerson también ofrece una amplia gama de servicios para ayudarle a garantizar que su sistema de seguridad proporcione la protección que necesita ... y que continúe proporcionándola. Estos servicios – incluyendo análisis y diseño, implementación, mantenimiento y modificación – abarcan el ciclo de vida completo de su sistema, con cumplimiento certificado por TUV con las mejores prácticas de IEC 61511. Si usted quiere, también podemos capacitar a su personal para que aproveche al máximo su sistema instrumentado de seguridad, o podemos proporcionar acceso a los ingenieros de seguridad de Emerson en campo en su planta para soporte y mantenimiento.

Beneficios del cumplimiento

Dependiendo de dónde esté ubicado, es posible que la conformidad con IEC 61511 ó con otras normas de seguridad sea un requisito legal. Incluso si no lo es, cumplir tiene sentido.

Por algo, el comité que desarrolló la norma IEC 61511 incluyó expertos de seguridad reconocidos mundialmente que combinaron su conocimiento y experiencia para crear la norma. El resultado es un riguroso conjunto de “mejores prácticas” para diseñar, implementar, verificar, operar y mantener sistemas instrumentados de seguridad robustos y fiables.

En breve, es una buena manera de ayudar a garantizar la seguridad de su planta y de su comunidad, a la vez que se minimizan los costos de operación.

Pero incluso cuando sí ocurren incidentes de seguridad, el hecho de haber cumplido con la norma puede ser útil.

Las investigaciones posteriores a un accidente o liberación de material al medio ambiente a menudo involucran agencias gubernamentales que tienen la autoridad de imponer multas, enviar a la gente a la cárcel, clausurar un establecimiento – o las tres cosas. Entre las preguntas que ellos pueden hacer, se encuentran las siguientes:

- ¿Ha ocurrido esta clase de incidente en esta compañía o establecimiento anteriormente?
- ¿Qué procesos proactivos se usaron para identificar los riesgos?
- ¿Qué métodos se usaron para cuantificar los riesgos?
- ¿Qué acciones se tomaron para mitigar los riesgos?
- ¿Qué proceso se siguió para garantizar que se desplegara la mitigación adecuadamente?
- ¿Qué procesos están implementados para garantizar que la solución de mitigación continúe funcionando como se espera?

Las respuestas a esas clases de preguntas son exactamente lo que se produce usando la norma IEC 61511. Es posible que usted se enfrente todavía a una dura investigación, pero si puede demostrar que se definió, se logró y se mantuvo adecuadamente el cumplimiento con la norma de seguridad de IEC, usted también reducirá el riesgo de que la agencia de investigación envíe a alguien a prisión o de que clausure la planta.

Agencias que respaldan IEC 61511 incluyen

- Factory Mutual Insurance Company
www.fmglobal.com
- Administración de Seguridad y Salud Laboral (OSHA) de los Estados Unidos
www.osha.gov
- Agencia de Protección Ambiental (EPA) de los Estados Unidos
www.epa.gov
- Automation, Software and Information Technology ASI of TÜV Industrial Services GmbH
www.tuvasi.com
- Oficina Ejecutiva de Salud y Seguridad (HSE) del Reino Unido www.hse.gov.uk

Sumario

En este curso usted ha aprendido que:

- Para las industrias de procesos, las normas de seguridad claves son IEC 61508, IEC 61511 y ANSI/ISA S84.00.01-2004.
- Actualmente, en las industrias de procesos, la norma IEC 61511 ó la nueva S84 es la mejor elección para que los usuarios finales implementen un proyecto de seguridad u operen y mantengan un sistema de seguridad.
- Las tres normas usan un modelo de ciclo de vida basado en el rendimiento, lo que hace más fácil integrarlas con otras normas – y producir resultados de alta calidad al menor costo posible.
- IEC 61511 permite alguna libertad de personalizar el modelo de ciclo de vida para satisfacer sus necesidades, siempre y cuando usted cumpla con los requisitos de la norma. Hacerlo requiere que se proporcionen los fondos adecuados, el personal y la capacitación.
- Además de ayudar a mantener la seguridad de su planta, personal y comunidad, el cumplimiento con las normas puede hacer más fácil lidiar con las investigaciones después de un incidente de seguridad.