SEGURIDAD FUNCIONAL EN INSTALACIONES DE PROCESO

Sistemas Instrumentados de Seguridad y Análisis SIL

Coordinadora:
Inmaculada Fernández de la Calle

Autores:
Alfonso Camacho López • Inmaculada Fernández de la Calle •
Carlos J. Gasco Lallave • Ana María Macías Juárez •
Mª Ángeles Martín Hernández • Gabriela Reyes Delgado •
Julio Rivas Escudero

DIAZ DE SANTOS
Madrid • Buenos Aires • México • Bogotá

ISA Sección Española

2ª edición

1ª edición 2012

Ediciones Díaz de Santos
Internet: http//www.editdiazdesantos.com
E-mail: ediciones@editdiazdesantos.com

ISBN: 978-84-9052-262-5
Depósito Legal: M-3676-2020

Fotocomposición: P55 Servicios Culturales
Diseño de cubierta: P55 Servicios Culturales

Printed in Spain - Impreso en España

ACERCA DE LOS AUTORES

A

COORDINADORA

Inmaculada Fernández de La Calle

Licenciada con Grado en Ciencias Químicas en la Universidad Complutense de Madrid en la Especialidad de Química Industrial. Experta en Seguridad Funcional con certificación vigente (CFSE).

Amplia y reconocida experiencia en Instrumentación y en Seguridad Funcional, actualmente trabaja en Técnicas Reunidas, S.A. Adjunta a jefe del departamento de Instrumentación y Control, responsable de Calidad y Formación. Durante cinco años estuvo vinculada a Intecsa Industrial.

Realiza labores docentes tanto en su empresa como en ISA España, impartiendo el curso sobre Válvulas de Seguridad y Dispositivos de Alivio y el de Experto en Seguridad Funcional. Es miembro de ISA España y participa activamente en las reuniones técnicas.

Imparte clases en el Máster de Instrumentación y Control de ISA España-Repsol en el módulo "Análisis de Riesgos y Sistemas Instrumentados de Seguridad Funcional". Es la coordinadora del Proyecto de Instrumentación en el mismo Máster.

Autora de numerosos artículos técnicos sobre Seguridad Funcional, Mantenimiento y Válvulas de Seguridad en revistas técnicas especializadas, tales como *Automática e Instrumentación,* e *Industria Química*.

Es la coordinadora de esta obra y ha escrito además los Capítulos 9 (Lógica del Sistema Instrumentado de Seguridad), 10 (Desarrollo de las especificaciones de seguridad-SRS), 11 (Diseño conceptual del SIS de cada función) y 12 (Diseño de detalle del SIS).

AUTORES

Alfonso Camacho López

Ingeniero Técnico. Amplia y reconocida experiencia en Instrumentación, Automatización y Control de Procesos Químicos, Sistemas de Control Distribuido y Sistemas Instrumentados de Seguridad en Refinerías de Petróleo, Plantas Petroquímicas y Central Nuclear.

Ha desarrollado su carrera profesional trabajando en el mantenimiento de instrumentación, en el diseño de la instrumentación y el control de unidades de procesos en empresas de ingeniería. Ha sido responsable de la organización y supervisión del montaje, de las pruebas y de la puesta en marcha de múltiples unidades de procesos en plantas petroquímicas.

Profesor en el Máster de Instrumentación y Control de Procesos de ISA/Repsol. Ha escrito el Capítulo 8 (Elementos de campo del Sistema Instrumentado de Seguridad).

Inmaculada Fernández de La Calle

Licenciada con Grado en Ciencias Químicas en la Universidad Complutense de Madrid en la Especialidad de Química Industrial. Experta en Seguridad Funcional con certificación vigente (CFSE).

Amplia y reconocida experiencia en Instrumentación y en Seguridad Funcional, actualmente trabaja en Técnicas Reunidas, S.A. Adjunta a jefe del departamento de Instrumentación y Control, responsable de Calidad y Formación. Durante cinco años estuvo vinculada a Intecsa Industrial.

Realiza labores docentes tanto en su empresa como en ISA España, impartiendo el curso sobre Válvulas de Seguridad y Dispositivos de Alivio y el de Experto en Seguridad Funcional. Es miembro de ISA España y participa activamente en las reuniones técnicas.

Imparte clases en el Máster de Instrumentación y Control de ISA España-Repsol en el módulo "Análisis de Riesgos y Sistemas Instrumentados de Seguridad Funcional". Es la coordinadora del Proyecto de Instrumentación en el mismo Máster.

Autora de numerosos artículos técnicos sobre Seguridad Funcional, Mantenimiento y Válvulas de Seguridad en revistas técnicas especializadas, tales como *Automática e Instrumentación,* e *Industria Química*.

Es la coordinadora de esta obra y ha escrito además los Capítulos 9 (Lógica del sistema instrumentado de seguridad), 10 (Desarrollo de las especificaciones de seguridad-SRS), 11 (Diseño conceptual del SIS de cada función) y 12 (Diseño de detalle del SIS).

Calos Javier Gasco Lallave

Licenciado en Ciencias Físicas por la UNED en la especialidad de Física Industrial y Experto Universitario en Regulación y Control de Procesos Industriales por la Universidad Politécnica de Madrid. Experto en Seguridad Funcional (CFSE) con certificación vigente y miembro del Consejo Asesor de Seguridad de Proceso.

En el desarrollo de su carrera profesional ha adquirido amplia experiencia tanto en el mundo de la Ingeniería, concretamente en disciplinas como la Instrumentación, Control y Seguridad de Procesos, como en el de la producción, trabajando en empresas como Initec Industrial o Dow Chemical. Ha sido uno de los responsables de

la Gerencia de la Seguridad Funcional en el proyecto Sadara, el mayor de la historia de la Ingeniería en una sola fase, y cuyas unidades se encuentran operacionales a día de hoy.

Miembro y patrocinador de ISA-España, actualmente es el CEO de ETC-FunSafe, y compagina su actividad con el mundo de la formación, impartiendo cursos de Instrumentación y Control, Electricidad Industrial y Seguridad de Procesos como formador senior de IFP-Training, empresa francesa de reconocido prestigio con importantes clientes a nivel global

Ha escrito los Capítulos 2 (Legislación,estándares y normativas), 3 (Capas de protección en instalaciones de proceso), 14 (Mantenimiento y explotación del SIS) y 15 (Modificaciones del SIS).

Ana María Macías Juárez

C.E.O. MAJA Consulting Group y Vicepresidente de Latin American Oil and Gas (LAOGA) en México. Licenciada en grado Ingenieria Industrial en el Instituto Técnologico de Boca Del Río,Veracruz, México. Maestría Técnica en automatización y control de procesos en el centro de formación REPSOL en Madrid, Esp. Maestría en Administración de Negocios (Executive MBA), en la Universidad Camilo Cela y EAE Business School comunidad de Madrid, España. Especialista con más de 20 años de experiencia en seguridad de procesos, certificado en Funciones Instrumentadas de Seguridad por TUV. Amplia y reconocida experiencia en el área de seguridad de procesos industriales; experto en el ciclo de vida de seguridad funcional; elaboración y participación en guías y normas de seguridad funcional de procesos. Ha escrito múltiples artículos para AICHE (American Institute Of Chemical Enginners) y la ISA-Intech referentes a seguridad de procesos, participación en la norma Argentina de Sistemas instrumentados de Seguridad, participación en la norma Mexicana de Diseño Inherentemente Seguro en sistemas de seguridad en terminales de almacenamiento de combustibles líquidos. Ha colaborado con múltiples centros de investigación en México, y es unidad Veridficadora en la norma Mexicana STPS 028-2012 (seguridad y salud de procesos). Ha escrito los Capítulos 5 (Diseño Conceptual) y 17 (Caso práctico).

Mª Ángeles Martín Hernández

Ingeniera Técnica Industrial, especialista Senior en Sistemas de Control y de Seguridad, experta en Seguridad Funcional Certificada (CFSE), trabaja desde el 2003 en el departamento de Control Avanzado e Instrumentación de la Dirección de Ingeniería-Dirección Técnica de Repsol.

Ha trabajado en Empresarios Agrupados en ingeniería para el mantenimiento eléctrico de la central nuclear de Almaraz desde 1989 hasta 1992. En Técnicas Reunidas S.A., desde 1993 al 2003, en el departamento de Sistemas para la Automatización de Procesos Industriales y en el departamento de Instrumentación y Control. Ha escrito el Capítulo 13 (FAT, instalación, comisionado y validación del SIS).

Gabriela Reyes Delgado

Jefe de Área de Seguridad de Procesos de la División de Seguridad Industrial de INERCO, S.A. Ingeniero Industrial Especialidad Química. Ha trabajado en INERCO desde el año 2000 y cuenta con una dilatada experiencia en Seguridad de Procesos y Seguridad Funcional y manejo completo de normativas al respecto, así como en aplicación de diversas metodologías de identificación y evaluación de riesgos, en nuevos proyectos e instalaciones existentes de las principales empresas del sector industrial, tanto a nivel nacional como internacional.

Dispone de las siguientes certificaciones en el campo de la Seguridad de Procesos:

- FS Eng (TÜV Rheinland): Process Hazard & Risk Analysis (PH&RA). ID-No. # 11964/16.
- FS Eng (TÜV Rheinland): Safety Instrumented Systems. ID-No. # 11956/16.

Profesora del "Máster de Instrumentación y Control" en el módulo "Análisis de Riesgos y Sistemas Instrumentados de Seguridad" que organiza REPSOL e ISA (International Society of Automation) Sección España.

Numerosas ponencias sobre Análisis de Riesgos de Procesos y Seguridad Funcional (SIS/SIL) en jornadas técnicas y congresos, así como cursos de capacitación *in-company* para personal de instalaciones de proceso.

Numerosos artículos publicados sobre Análisis de Riesgos de Procesos y Seguridad Funcional (SIS/SIL) en revistas técnicas especializadas, tales como *Ingeniería Química*, *Oil&gas*, *Proyectos Químicos*, *Química Universal*, etc

Ha escrito los Capítulos 6 (Análisis de Riesgos de Procesos), 7 (Metodologías para la determinación del índice SIL) y 16 (Gerencia de la Seguridad Funcional) y desarrolló el borrador del Índice de este libro.

Julio Rivas Escudero

Asesor de Grandes Proyectos en la Refinería de Somorrostro de Petronor.

Ingeniero eléctrico. Ha desarrollado su carrera profesional en Petronor. Anteriormente ha sido Jefe de Instrumentación y Electricidad de Mantenimiento y Jefe de Instrumentación de Ingeniería. En los años 90 lideró el proyecto de Reinstrumentación y Digitalización de la refinería y ha estado involucrado en numerosos proyectos de control avanzado. Jefe del departamento de Control Avanzado y Sistemas de Producción en la refinería de Somorrostro de Petronor durante quince años (1992-2007). Miembro de ISA España, perteneció a su comité ejecutivo durante seis años, de los que tres fue Presidente.

Profesor y asesor del Máster de "Instrumentación y Control de Procesos de ISA/Repsol" en los aspectos de Seguridad Industrial.

Ha escrito los Capítulos 1 (Introducción a los sistemas instrumentados de seguridad) y 4 (Introducción al ciclo de vida de los sistemas instrumentados de seguridad). Además de él partió la idea del libro y su empuje inicial.

PRESENTACIÓN

ISA, International Society of Automation, es una organización internacional sin ánimo de lucro cuya visión es la de crear un mundo mejor a través de la automatización. Para ello se ha fijado una misión: avanzar en la competencia técnica, conectando a la comunidad de automatización para lograr la excelencia operativa.

La Sección Española de ISA se fundó en 1998 y, en pocos años, se ha convertido en referente europeo por la calidad y número de actividades que realiza, entre las que destacan las reuniones técnicas, los cursos de formación y el prestigioso Máster en Instrumentación y Control de Procesos. En 2012 inauguramos, con la primera edición de este libro, una actividad que nos ilusiona particularmente: la edición de libros técnicos. El éxito de acogida de la primera edición nos motivó para publicar otros cuatro libros, tratando temas tan variados como los analizadores de proceso, las válvulas de control, la ingeniería de instrumentación y el diseño de las salas de control.

Para la elaboración de este libro se ha reunido a un magnífico grupo de profesionales con gran experiencia en el área de la Seguridad Funcional. Cada uno ha aportado su conocimiento y experiencia, de forma que la obra representa un completo análisis teórico y práctico.

Hemos pretendido crear un libro útil para todos los interesados en la Seguridad, tanto estudiantes como profesionales, y así cumplir con la misión de ISA, ayudando a los profesionales del sector a resolver sus problemas técnicos, a mejorar sus conocimientos y capacidad de liderazgo y favorecer en general su desarrollo profesional.

Finalmente, quiero agradecer a todos los que han contribuido a que este libro haya salido a la luz. De forma especial a Inmaculada Fernández, por su eficaz labor de coordinación general de la obra, fundamental para lograr que todo el libro tenga continuidad, un estilo único y coherencia, a pesar de estar realizado por diversos autores. A los autores y revisores de los distintos capítulos, por su esfuerzo, robando muchas veces tiempo a su vida personal. A Francisco Díaz-Andreu y Manuel Bollaín por su trabajo y empuje y a Fernando Trucharte por su esfuerzo en esta segunda edición.

Esperamos haber cumplido nuestro objetivo.

Francisco Javier Calmuntia Arroyo
Presidente de la Sección Española de ISA

PRÓLOGO A LA SEGUNDA EDICIÓN

Cuando conocemos, pues, que algo sucede, siempre estamos presuponiendo que algo antecede y que a ese algo sigue lo que sucede conforme a una regla.

Critica de la Razón Pura - Inmanuel Kant.

Esta segunda edición surge por la necesidad de actualización con respecto a la edición emitida a lo largo de 2016 de la IEC-61511, que es el estándar base de la seguridad funcional en la industria de procesos.

Cuando se gestó la idea de escribir este libro, asumimos el reto que se nos planteaba de ser los pioneros, de dar las explicaciones a nuestro modo, desde nuestra experiencia, plasmando las dificultades que a lo largo de estos años nos hemos ido encontrando, y llegar a todos los que formamos este gran sector, desde el consultor hasta el usuario final, en nuestro idioma y en los años que han pasado desde la primera edición, hemos conseguido que sea un libro de referencia del sector.

Es un libro de estudio y de consulta que recorre paso a paso todos los aspectos del ciclo de vida de seguridad, basándonos en los estándares europeos IEC-61508 e IEC-61511.

Comenzamos por desarrollar la normativa aplicable, la que es de obligado cumplimiento y la que se recomienda utilizar en su defecto.

Pasamos al estudio de las capas de protección, las que son IPL, los créditos asociados (o su factor), recorriendo también sus tipos.

Estudiamos de manera global el ciclo de vida de la seguridad, el diseño conceptual, los documentos que se originan en cada etapa del proyecto, qué información proporcionan, y cómo se utiliza esa información

Estudiamos los diferentes métodos de análisis de riesgos, así como los de asignación de SIL.

Analizamos la instrumentación de campo y la lógica con respecto a la seguridad funcional, los tipos de instrumentos, su instalación, y su mantenimiento.

Desarrollamos en el Capítulo 10 la *Especificación de Seguridad* (SRS), incluyendo un formato recomendado, y además qué información debe recoger cualquier especificación de seguridad.

En el Capítulo 11 incluimos el detalle de cada *Función Instrumentada de Seguridad* (SIF), cómo se verifica una SIF, qué aspectos hay que considerar en su verificación, las distintas arquitecturas y su influencia en los resultados de *probabilidad de*

fallo en demanda (PFD), *disponibilidad* (A) y *fiabilidad* (R).

Pasaremos a ver el detalle del SIS, qué consideraciones hay que tener en el diseño: los *bypasses*, consideraciones ambientales, minimización de los fallos con causa común.

En el Capítulo 13 desarrollamos la instalación, comisionado y la validación del SIS, y en el apéndice incluimos listas de chequeo para cada uno de los aspectos que hay que comprobar.

En los Capítulos 14 y 15 pasamos por las tan importantes pruebas manuales, incluyendo ejemplos de procedimientos de mantenimiento y de operación y la gestión de los cambios en el SIS.

Incluimos también un capítulo sobre gerencia funcional, identificando las actividades de gestión necesarias para asegurar que se cumplen los objetivos de la seguridad funcional.

En el Capítulo 17 hemos desarrollado un ejemplo práctico del ciclo de vida de seguridad aplicada a una SIF en una torre de absorción del proceso de desulfuración.

Al final de cada capítulo hemos añadido dos apartados importantes:

- CONSEJOS PRÁCTICOS
- PARA NO OLVIDAR

De manera que sea más fácil fijar los conocimientos que se desarrollan y que hemos querido transmitir.

Para finalizar, se incluyen dos anexos:

- Glosario de términos y acrónimos.
- Referencias bibliográficas.

Es, por lo tanto, un libro global sobre Seguridad Funcional basado en los estándares internacionales y en nuestra propia experiencia.

Inmaculada Fernández de la Calle
(Coordinadora de la obra)

ÍNDICE

INTRODUCCIÓN A LOS SISTEMAS INSTRUMENTADOS DE SEGURIDAD (SIS)

1

Julio Rivas Escudero

SUMARIO: **Introducción. Necesidad y ámbito de aplicación de un SIS. Terminología y definiciones más importantes.** ***Para no olvidar. Consejos prácticos.***

1.1. INTRODUCCIÓN

Cuando un accidente ocurre es debido normalmente a una serie de causas o sus combinaciones que producen un evento peligroso.

En la Industria están implementados los Sistemas de Parada de Emergencia (ESD) para la protección a los seres humanos, al medio ambiente y a los equipos. No es por lo tanto un concepto nuevo, lo que sí es novedoso es la forma de tratarlo, es decir, los sistemas de parada de emergencia van a disponer de un ciclo de vida, que denominaremos Ciclo de Vida de Seguridad, que empezará en su etapa de definición y acabará en la de desmantelamiento.

La variedad de nombres asignados a los Sistemas de Parada de Emergencia parece algo ilimitado: Sistema de enclavamientos (IS), Sistema Instrumentado de Seguridad (SIS), Sistema de Parada de Emergencia (ESD), etc.

Dentro de la Industria de Proceso, el debate continúa sobre el significado de cada uno de ellos. Incluso en el comité ISA SP84 hubo discusiones continuas (y cambios frecuentes) sobre la terminología, definición y significado de cada uno de esos términos.

No obstante la confusión en la industria va más allá del propio significado, afecta al propio diseño, instalación, puesta en marcha, mantenimiento, modificaciones, etc., de estos sistemas. Así, nos encontraremos con muchos ejemplos y preguntas que no son fáciles de responder o que la respuesta no es la misma, dependiendo de la norma, estándar o persona que la dé. A título de ejemplo se exponen algunas dudas típicas.

1.1.1. Selección de la tecnología a utilizar

¿Qué tecnología deberá ser usada: relés, estado sólido, microprocesador (PLC)? ¿Depende dicha selección de la aplicación?

Los relés son todavía usados en pequeñas aplicaciones pero, ¿diseñaría un sistema de 500 entradas/salidas con relés? ¿Es económico diseñar un sistema con 20 entradas/salidas con PLC redundantes?

Algunos prefieren no usar sistemas basados en software en aplicaciones de seguridad. ¿Es una buena recomendación?

1.1.2. Selección de redundancia

¿Cómo de redundante debería ser diseñado un sistema instrumentado de seguridad?

¿Depende de la tecnología o del nivel de riesgo?

Si la mayoría de los sistemas basados en relés son simples, ¿por qué son tan populares, actualmente, los sistemas programables de triple redundancia?

1.1.3. Elementos de campo

¿Deberían los elementos sensores iniciadores ser de tipo transmisor o interruptor (*switch*)? Si usamos transmisores, ¿analógicos o digitales?

¿Redundancia o no en los elementos de campo? ¿Pueden usarse los mismos elementos de campo para enclavamientos y para control?

¿Frecuencia de prueba de dichos elementos?

Un objetivo de este libro es tratar de dar respuestas a estas preguntas y de clarificar la confusión general que sobre estos sistemas se está produciendo.

1.2. NECESIDAD Y ÁMBITO DE APLICACIÓN DE UN SIS

Los accidentes industriales raramente suceden por una sola causa. Lo normal es que sean consecuencia de una combinación de eventos poco comunes que se piensa son independientes y que no deberían suceder al mismo tiempo. Tomad, como ejemplo, el peor accidente químico ocurrido hasta la fecha que tuvo lugar en Bhopal (India) en una planta de pesticidas. Unas 3.000 personas murieron de inmediato y al menos 12.500 fallecieron en las semanas posteriores por inhalar gas y beber agua contaminada. Desde entonces se estima que unas 25.000 personas han perdido la vida por las secuelas y unos 150.000 están afectados de alguna manera.

Ocurrió de esta manera:

El material que fugó en dicha planta fue *isocionato de metilo* (MIC). Dicha fuga (del orden de 40 toneladas) se produjo en un tanque de almacenamiento que *contenía más cantidad* de lo que establecían los *procedimientos de seguridad de la compañía.*

Los procedimientos de operación establecían asimismo usar un sistema de refrigeración para mantener la *temperatura en el producto* de dicho tanque en *5 ºC* disponiendo de una *alarma* cuando la temperatura subiese de 11 ºC.

El sistema de refrigeración estaba desconectado, el MIC se había almacenado a una temperatura cercana a los 20 ºC y se había reajustado la alarma a 20 ºC.

Un trabajador fue comisionado para lavar con agua unas tuberías y filtros que se encontraban obstruidos. El agua pasó al tanque de almacenamiento del MIC a través de una fuga de una válvula produciéndose una reacción violenta con gran producción de gases.

Los medidores de presión y temperatura del tanque que indicaban la situación anormal no fueron tenidos en cuenta al pensar que eran imprecisos.

El separador/lavador de venteo de gases a antorcha que podía haber neutralizado la fuga estaba fuera de servicio por estar suspendida la producción de MIC y pensar que no era por tanto necesario.

Asimismo la propia antorcha que podría haber quemado parte de dichos gases estaba fuera de servicio por mantenimiento.

Finalmente hubo una serie de acontecimientos y errores en los planes de emergencia que completaron el fatal escenario de dicho accidente.

Por lo explicado anteriormente, queda claro que los accidentes suelen ser una combinación de raros eventos que se suelen asumir como independientes y de difícil coincidencia en el tiempo. Uno de los métodos de protegerse contra ellos es implementando múltiples e independientes capas de protección que hagan más difícil que dichos eventos deriven a condiciones peligrosas.

Es por tanto fundamental que desde el inicio de un proyecto y en su etapa de explotación y mantenimiento se disponga de dichas capas de protección perfectamente estructuradas, sujetas a procedimientos y mantenidas con una idea muy simple:

No poner todos los huevos en la misma cesta.

En el Capítulo 3 de este libro se explicarán con detalle cada una de las capas de protección tanto las de tipo preventivo como las de mitigación.

De manera general, las primeras son aquellas diseñadas para prevenir y anticiparse a que un determinado peligro pueda ser efectivo y llegue a darse. Son las que se aplican en primer lugar, y las más importantes son:

- Diseño de planta.
- Sistemas de control.
- Sistemas de alarmas.
- Sistemas Instrumentados de Seguridad (SIS).

Las segundas son aquellas que se diseñan para paliar o limitar las consecuencias de un suceso una vez que este realmente ha sucedido. Las más importantes son:

- Sistemas de fuego y gas.
- Sistemas de contención.
- Planes de emergencia.

Como se puede constatar, los Sistemas Instrumentados de Seguridad constituyen la última capa de seguridad preventiva y ahí radica su gran importancia y necesidad dentro de la seguridad industrial de las industrias de proceso.

Conviene, no obstante, clarificar la diferencia existente entre lo que es de obligado cumplimiento por ley y lo que es una buena práctica de diseño y trabajo recogido en especificaciones, estándares y normas. También decir que lo que puede ser obligatorio en un país (ejemplo, USA), puede no serlo en otros, o viceversa. Esto se verá con detalle en el Capítulo 2, pero incluimos aquí algunas ligeras pinceladas:

- En la Unión Europea, y como es lógico en España, *lo obligado por ley* se recoge en directivas y su transposición a reales decretos.
- Un ejemplo (entre muchos) es la Directiva 96/82 CE (9/12/96) llamada Seveso II y su traslado al RD 1254/1999 (16 julio 99) de "Prevención de accidentes graves en los que intervienen sustancias peligrosas". También está en este caso la Directiva ATEX.
- Referente a los Sistemas Instrumentados de Seguridad (SIS). *No* hay en Europa/España al día de hoy ninguna directiva ni RD que obligue a su cumplimiento. (Pero sí que existen estándares europeos, como por ejemplo la EN-746-2, que obliga a un determinado SIL en algunos lazos de seguridad, estableciendo además el intervalo de pruebas y la arquitectura que debe ser implementada).
- Existen estándares y normas cuyo cumplimiento se considera recomendable, y con visión de futuro deberá ponerse en práctica en los proyectos y modificaciones ya que, como en otros campos, finalmente aparecerá la directiva que obligue a su cumplimiento.

Centrándonos en el tema de los SIS, como hemos anticipado, se cubrirán en el Capítulo 2, de forma detallada, todo lo relativo a legislación y normativas existentes. A modo de preámbulo, y para completar este apartado, se describe lo más relevante de los dos organismos internacionales que disponen de los estándares que son la base de todo lo relacionado con los SIS:

1.2.1. ANSI/ISA

En el primer grupo está la ISA (Sociedad Internacional de Automatización) y la IEC (Comisión Electrotécnica Internacional).

El estándar de ISA relacionado con los SIS es el ANSI / ISA 84.01, denominado "Aplicación de SIS para las Industrias de Proceso".

El ISA SP84 (Comité de estándares y prácticas nº 84) ha trabajado muchos años en la elaboración y desarrollo de este estándar. Inicialmente, estaba direccionado solo a la lógica y con posterioridad se incluyeron los elementos de campo. El documento ha sufrido muchos cambios a lo largo del tiempo y su futuro a largo plazo está condicionado al desarrollo del estándar IEC 61511.

El primer documento fue editado en 1996 (actualmente está el de 2004) y ya que dentro de la IEC está representando a USA el ANSI (Instituto Nacional de Estandarización Americano), este Instituto soportará el estándar IEC 61511 y podrá reemplazar al ANSI/ISA S84.01. En cualquier caso, al día de hoy el ISA 84.01/2004 es básicamente idéntico al IEC 61511 con la inclusión de una cláusula de salvaguarda (abuelo-grandfather) que afecta a modificaciones en instalaciones existentes y que básicamente dice lo siguiente:

- Para los sistemas instrumentados de seguridad existentes (SIS), diseñados y construidos de acuerdo con los códigos, normas, prácticas con anterioridad a la emisión de esta norma (por ejemplo, ANSI / ISA 84.01-1996), el propietario/operador de la planta debe determinar y documentar que el equipo está diseñado, mantenido, inspeccionado, probado y funciona de una manera segura. De hecho al día de la fecha la edición 2 del 2016 de la IEC 61511 ha incluido dicha cláusula en su documentación.

1.2.2. I.E.C

IEC tiene dos estándares relacionados con los sistemas instrumentados de seguridad:

- IEC 61508 "Seguridad Funcional: Sistemas Relacionados con la Seguridad" que afecta a todo tipo de industrias y que se usa básicamente por fabricantes y suministradores. IEC formó posteriormente un grupo de trabajo para desarrollar un documento específico de SIS para el sector de las industrias del proceso y aplicable, no solo a fabricantes y suministradores, sino también a diseñadores, integradores y usuarios. El estándar se denominó IEC 61511 "Seguridad Funcional: SIS para el Sector de la Industria del Proceso" que debe ser usado en complemento con el IEC 61508. Por la importancia que tiene la Comisión Electrotécnica Internacional (IEC) en los Sistemas Instrumentados de Seguridad sobre todo en lo referente a las industrias de proceso con su estándar IEC 61511, haremos una exposición más detallada de dicho estándar incluyendo su historia y contenido.
- IEC 61511 es una norma técnica que establece las prácticas en la ingeniería de sistemas que garantizan la seguridad de un proceso industrial mediante el uso de la instrumentación. Estos sistemas se denominan Sistemas Instrumentados de Seguridad. El título de la norma es "Seguridad funcional - Sistemas instrumentados de seguridad para el sector de la industria de procesos".

Contenido:

El sector de la industria de proceso incluye muchos tipos de procesos de fabricación, tales como refinerías, petroquímicas, químicas, farmacéuticas de pasta y papel, energía, etc. El estándar del sector proceso no se aplica a las instalaciones de energía nuclear o reactores nucleares. IEC 61511 cubre el uso de equipos eléctricos, electrónicos y electrónicos programables. Mientras IEC 61511 es aplicable a los equipos que utilizan sistemas hidráulicos o neumáticos para manipular elementos finales, el estándar no cubre el diseño e implementación de la lógica neumática o hidráulica. Esta Norma define los requisitos de seguridad funcional establecida por la Norma IEC 61508 en el sector de las industrias de proceso. IEC 61511 centra la atención en un tipo de sistema instrumentado de seguridad utilizado en el sector de proceso, el denominado Sistema Instrumentado de Seguridad (SIS). La Norma no establece

requisitos de otros sistemas de seguridad instrumentados, tales como sistemas contra incendios y de gas, sistemas de alarmas, etc.

Historia

En 1998, la IEC, que es sinónimo de "Comisión Electrotécnica Internacional", publicó un documento, IEC 61508, titulado: "La seguridad funcional de sistemas eléctricos / electrónicos / sistemas electrónicos programables relacionados con la seguridad". Este documento establece las normas para el diseño de sistemas relacionados con la seguridad tanto del hardware como del software. IEC 61508 es la norma genérica de seguridad funcional, es la base y contiene los requisitos básicos para cada norma específica del sector. Tres normas específicas han sido realizadas con el marco de la Norma IEC 61508: IEC 61511 (proceso), IEC 61513 (nuclear) e IEC 62061 (de fabricación). IEC 61511 proporciona buenas prácticas de ingeniería para la aplicación de los sistemas instrumentados de seguridad (SIS) en el sector de proceso. En Estados Unidos, ANSI / ISA 84.00.01-2004 se publicó en septiembre de 2004. Es principalmente un espejo de la IEC 61511 en su contenido incluyendo una cláusula de derechos adquiridos llamada del abuelo (*grandfather*).

El organismo europeo de normalización, CENELEC, ha adoptado la norma como la EN 61511. Esto significa que en cada uno de los estados miembros de la Unión Europea, la norma se publica como una norma nacional. Por ejemplo, en Gran Bretaña, que es publicado por el organismo nacional de normalización según la Norma BS EN 61511. El contenido de estas publicaciones nacionales es idéntico a la de la Norma IEC 61511. Debe tenerse en cuenta, sin embargo, que la IEC 61.511 no está armonizada como directiva de la Comisión Europea hasta la fecha (año 2011).

La Norma

La primera Norma IEC 61511 fue publicada en el año 2003 y cubre los requisitos de diseño y gestión de SIS desde la cuna hasta la tumba constituyendo un Ciclo de Vida completo lo que constituye el mayor valor de la misma. Su ámbito de aplicación incluye: el diseño conceptual y básico, el diseño e ingeniería de detalle, montaje e implementación, pruebas, operación y mantenimiento, modificaciones y eventualmente una eliminación de parte o del completo SIS. Se inicia en la primera fase de un proyecto y continúa hasta la puesta en marcha. Contiene secciones que cubren las eventuales modificaciones, junto con las actividades de mantenimiento y las actividades de posibles desmantelamientos.

La Norma consta de tres partes:

1. Marco, definiciones, sistema y requerimientos de hardware y software .
2. Directrices y guías para la aplicación de la Norma IEC 61511-Parte1.
3. Orientación y guías para la determinación de los niveles requeridos de integridad de seguridad (SIL).

Actualmente se ha editado la 2ª edición de la Norma (2016) que en lo que afecta a la parte1 se ha publicado en febrero de 2016 y a las partes 2 y 3 en julio de 2016. Los aspectos más importantes revisados en la misma se han incluido en los capítulos del presente libro.

ISA 84.01/IEC 61511 requiere un sistema de gestión para cada SIS. El SIS se compone de una combinación separada e independiente de sensores, revolvedores de lógica, elementos finales y sistemas de apoyo que se diseñan y gestionan para conseguir un nivel de integridad de seguridad especificado (SIL). Un SIS puede estar formado por una o más funciones instrumentadas de seguridad (SIF), que son diseñadas e implementadas para hacer frente a un peligro de proceso específico o suceso peligroso.

El sistema de gestión del SIS debe definir cómo un propietario/operador tiene intención de evaluar, diseñar, verificar, instalar, validar, operar, mantener y mejorar continuamente sus SIS. Las funciones esenciales del personal asignado a la gestión del SIS deben estar contempladas y bien definidas en procedimientos, según sea necesario, para apoyar la ejecución coherente de sus responsabilidades.

ISA 84.01/IEC 61511 utiliza un orden de magnitud métrica, el SIL, para establecer el objetivo necesario. Un análisis de riesgos operativo es parte del ciclo de vida para identificar las funciones de seguridad necesarias y la reducción del riesgo respecto a determinados eventos peligrosos. Las funciones de seguridad asignadas al SIS son las funciones instrumentadas de seguridad (SIF), la reducción del riesgo, atribuido a cada una de ellas, se relaciona con el SIL. La base de diseño y operación se ha desarrollado para garantizar que el SIS cumple con el SIL requerido. Los datos de campo se recogen a través de actividades programadas para evaluar el rendimiento real del SIS. Cuando los rendimientos no se cumplen, deben tomarse medidas para cerrar la brecha, asegurando un funcionamiento seguro y fiable.

1.3. TERMINOLOGÍA Y DEFINICIONES MÁS IMPORTANTES

Veamos algunas terminologías y definiciones más usadas.

1.3.1. ¿Qué es un Sistema Instrumentado de Seguridad (SIS)?

Un Sistema Instrumentado de Seguridad (SIS) es un nuevo término usado en los estándares que normalmente también ha sido y es conocido por la mayoría como: Sistema de Parada de Emergencia (ESD), Sistema de Parada de Seguridad, Sistema de Enclavamientos, Sistema de Disparos de Emergencia, Sistemas de Seguridad, etc.

También podría ser definido como la última capa de seguridad preventiva para que si el sistema de control y la actuación del operador son insuficientes y se alcanzan niveles de variables predeterminados que no deben superarse bajo ningún concepto, debe disponerse de un sistema que de forma automática realice las acciones oportunas (paradas parciales o totales de equipos y plantas) para así evitar el peligro.

Estos sistemas instrumentados de seguridad están normalmente separados e independizados de los sistemas de control, incluyendo la lógica, los sensores y válvulas

de campo y a diferencia de los Sistemas de Control, que son activos y dinámicos, los SIS son básicamente pasivos y dormidos por lo que normalmente requieren un alto grado de seguridad y de diagnósticos de fallos así como prevenir cambios inadvertidos y manipulaciones y un buen mantenimiento.

ANSI/ISA 84.01 define el término SIS como:

> "Un Sistema compuesto por sensores, lógica y elementos finales con el propósito de llevar el proceso a un estado seguro cuando determinadas condiciones preestablecidas son violadas."

Y ahora nos surge la pregunta: ¿Qué es un estado seguro. Lo definiremos como:

> "El estado que consigue un sistema cuando se alcanza la seguridad, es decir cuando el sistema está libre de un riesgo inaceptable."

Por lo tanto el objetivo de un SIS es llevar a los sistemas a un estado de riesgo tolerable.

IEC-61511 define el término SIS como:

> "Un Sistema Instrumentado usado para implementar una ó más funciones instrumentadas de Seguridad (SIF) y se compone de una ó más combinaciones de sensores, lógica y elementos finales."

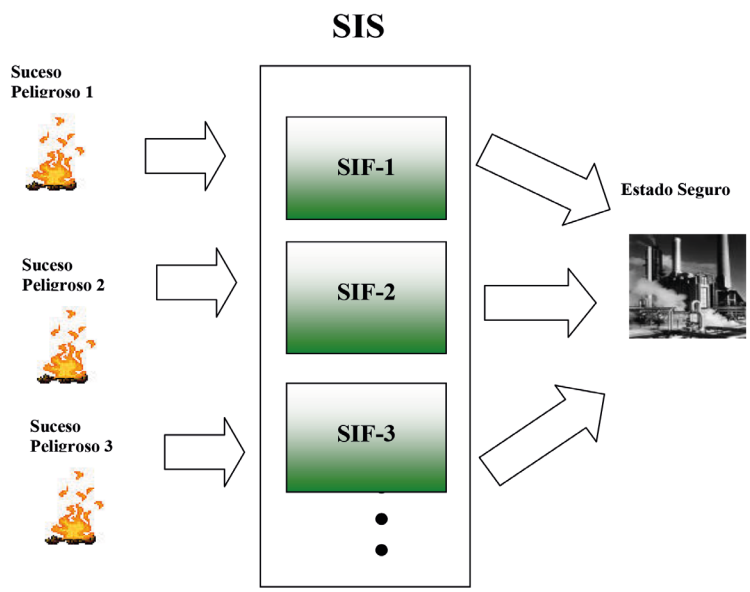

Figura 3.1. Sistema Instrumentado de Seguridad.

Cada SIF estará formada por iniciadores, lógica y elementos finales y tendrá asignado un SIL.

1.3.2. ¿Qué es un Nivel Integrado de Seguridad (SIL)?

La integridad de la seguridad indica la disponibilidad de un sistema de seguridad. Es decir (sic) "La probabilidad de que un sistema relacionado con la seguridad ejecute de forma satisfactoria las funciones de seguridad requeridas en todas las condiciones especificadas en un periodo de tiempo especificado".

Esto conlleva a lograr un factor de reducción de riesgo (RRF) que hace posible alcanzar un riesgo razonable que minimice los accidentes.

Especificar la integridad de la seguridad no consiste en definir solo qué es lo que debe hacer el sistema de seguridad, sino también en especificar la bondad con la cual dicho sistema debe llevar acabo su función.

El SIL es el nivel de integridad de la seguridad asociado y exigible a un sistema de seguridad. Se definen hasta cuatro niveles de integridad de la seguridad, donde el nivel 4 posee el grado más elevado de integridad de la seguridad y el nivel 1 el más bajo.

SIL	Disponibilidad	Factor Reducción de Riesgo
1	90,00 – 99,00%	10 a 100
2	99,00 – 99,90%	100 a 1.000
3	99,90 – 99,99%	1.000 a 10.000
4	> 99,99%	>10.000

En la determinación de la integridad de seguridad se deben incluir todas las causas de fallo que conducen a un estado inseguro: los fallos de hardware (tanto los aleatorios como los sistemáticos), los fallos inducidos de software y los fallos debidos a las perturbaciones eléctricas. Aunque algunos de estos tipos de fallos se pueden cuantificar (utilizando medidas como la *tasa de fallos* o la *probabilidad de fallo de funcionamiento a la demanda*), la integridad de la seguridad depende también de muchos factores que no se pueden cuantificar con precisión, sino que solo se pueden considerar de forma cualitativa.

1.3.3. ¿Qué es la probabilidad de fallo en demanda media (PFDavg)?

Para calcular de una forma numérica el SIL uno de los parámetros mas utilizados es la PFD_{MEDIA}. Este parámetro indica la probabilidad media de fallo al ejecutar, bajo demanda, la función para la cual ha sido diseñado.

Supongamos una función de seguridad: cierre de la válvula de vapor al calentador de fondo cuando se detecta alta presión en la cabeza de la torre. La PFD_{MEDIA} es la probabilidad de que cuando haya alta presión en la cabeza de la torre, el sistema cierre efectivamente la válvula de vapor.

La relación de la $PFD_{MEDIA\ para\ SIF\ en\ "modo\ Demanda"}$ con los SIL es la siguiente:

SIL	Disponibilidad	PFD_{MEDIA}	Factor Reducción de Riesgo
1	90,00 – 99,00%	$10^{-2} – 10^{-1}$	10 a 100
2	99,00 – 99,90%	$10^{-3} – 10^{-2}$	100 a 1.000
3	99,90 – 99,99%	$10^{-4} – 10^{-3}$	1.000 a 10.000
4	> 99,99%	$10^{-5} – 10^{-4}$	>10.000

Matemáticamente, el cálculo de la PFD_{MEDIA} es muy complejo si se intenta hacer sobre la función de seguridad en su conjunto.

Para simplificarlo, lo que se hace es lo siguiente:

- Descomponer dicha función de seguridad en sus elementos principales.
- Calcular la PFD_{MEDIA} de cada elemento.
- Realizar la suma de las PFD_{MEDIA} de todos los elementos.

Por ejemplo, para el caso citado se calcularían las PFD_{MEDIA} de la parte sensora, la parte del operador lógico y la parte actuadora. La suma de todas ellas sería la PFD_{MEDIA} de la función de seguridad:

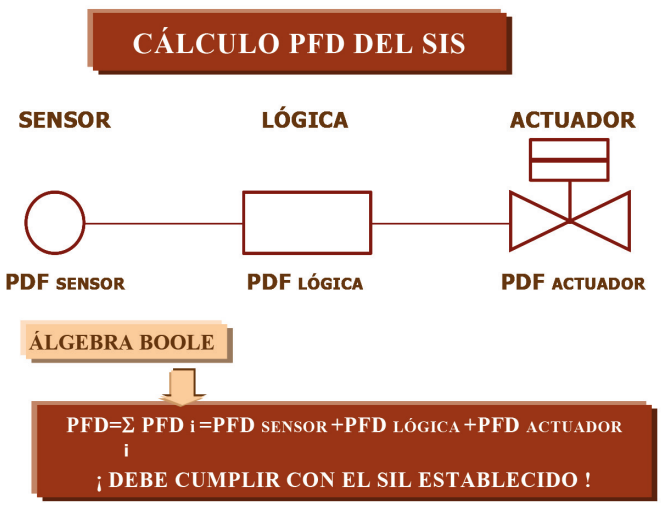

Figura 1.2. Cálculo de la PFDavg de un sistema.

1.3.4. ¿Qué es una función instrumentada de seguridad (SIF)?

Es una función de seguridad con un nivel de integridad de la seguridad necesario para lograr la seguridad funcional y en el que puede haber una función de protección instrumentada de seguridad o una función de control instrumentada de la seguridad. Los elementos que forman una SIF son el sensor (compuesto a su vez por un con-

junto de uno o más elementos de medida), el sistema lógico (normalmente situado en un PLC) y el elemento final (compuesto generalmente por una o más válvulas).

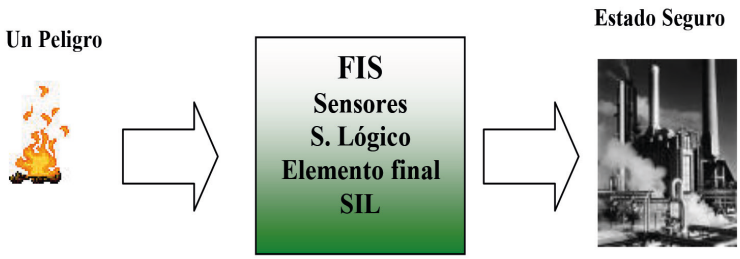

Figura 1.3.

Inicialmente, en la IEC 61508-4 sección 3.5.16 existían tres tipos de SIF en su relación modo-operación denominadas Modo Demanda Baja (*low demand mode*), Modo Alta Demanda (*high demand mode*) y Modo Demanda Continua (*continuous mode*). Asimismo en la IEC 61511-2003 figuraban solo dos modos de operación de las SIF a saber: Modo Demanda y Modo Continuo. La actual revisión del 2016 de dicha IEC 61511 ha clarificado este tema definiendo tres clases: Modo Baja Demanda, Modo Alta Demanda y Modo Continuo aunque las dos primeras las agrupa genéricamente como Modo Demanda. A estos efectos define como Modo Baja Demanda al modo de operación donde la SIF se ejecuta solo si es demandada para llevar el proceso a una situación segura y donde la frecuencia de dicha demanda no es muy alta (se espera que dicha demanda sea más que un año o que la frecuencia prevista de actuación, sea muy baja respecto al posible intervalo de prueba entre tests funcionales (ejemplo: pruebas funcionales bianuales y frecuencia de demanda esperada de 10 años). Se definen SIF de Modo Alta Demanda cuando la SIF solo se ejecuta bajo demanda y la frecuencia de dicha demanda puede ser inferior al año. Finalmente denomina SIF de Modo Continuo a aquellas cuyo modo de operación mantiene al proceso de forma segura como parte normal de la operación. El presente curso contempla las SIF activadas en demanda (baja o alta) que son las normalmente requeridas en la mayoría de las industrias de proceso y cuya tabla se reflejó en el apartado anterior.

Para el caso de SIF a modo continuo el único factor que se considera para el cumplimiento del SIL es la frecuencia del fallo peligroso no detectado (λdu) y en este caso ISA/IEC las llama Función Instrumentada de Seguridad/Control.

Definición del SIL para modo continuo EN 61508.

SIL	Rango de λdu (fallos por hora)	~ Rango de MTTF (años)
4	$10^{-9} \leq \lambda < 10^{-8}$	100.000 ≥ MTTF > 10.000
3	$10^{-8} \leq \lambda < 10^{-7}$	10.000 ≥ MTTF > 1.000
2	$10^{-7} \leq \lambda < 10^{-6}$	1.000 ≥ MTTF > 100
1	$10^{-6} \leq \lambda < 10^{-5}$	100 ≥ MTTF > 10

1.3.5. ¿Qué es tiempo medio entre fallos (MTBF)?

El tiempo medio entre fallos MTBF (del inglés *Mean Time Between Failure*) es la suma del tiempo medio de fallo (MTTF) más el tiempo medio empleado en detectar el fallo y el tiempo empleado en repararlo (MTTR). Normalmente el fabricante debería de dar el MTTF (*mean time to fail*) aunque a veces se da el MTBF como si fuera el MTTF. Realmente, los tiempos de detección y reparación son despreciables con respecto al MTTF por lo que no existe demasiada diferencia entre el MTBF y el MTTF.

En esencia: **MTBF = MTTF + MTTR**

Donde:

- MTBF: tiempo medio entre fallos (*mean time between failure*).
- MTTF: tiempo medio de fallos (*mean time to fail*).
- MTTR: tiempo medio de restauración (MTTD+TR).
- MTTD: tiempo medio de detección del fallo (*mean time to detect*).
- TR: tiempo de reparación.

1.3.6. ¿Qué es fallo seguro y fallo peligroso?

Conocer la diferencia entre estos dos tipos de fallos es esencial para el uso correcto de las fórmulas empleadas en los cálculos de la probabilidad de fallo en demanda. Se dice que un fallo de un determinado instrumento es seguro cuando como consecuencia del mismo el proceso va a una condición segura. Si dicho fallo posibilita que, ante la necesidad o demanda de la correspondiente función lógica, el sistema no actúa correctamente y deja al proceso en condiciones inseguras, dicho fallo se denomina peligroso.

Saber que la tasa de fallo global (λ) de cualquier instrumento es :

$$\lambda = \frac{1}{MTTF}$$

Asimismo, de la tasa de fallo global una fracción es peligrosa (λd) y otra segura (λs).

Se puede decir que

$$\lambda = \frac{1}{MTTF}, \quad \lambda d = \frac{1}{MTTFd}, \quad \lambda s = \frac{1}{MTTFs}$$

Dependiendo del tipo de elemento/instrumento pueden existir parte de las tasas de fallo peligrosas y seguras que sean detectadas y otras que no. En este caso se añade otro subíndice a λd y a λs con las letras “u” (*undetected*) y “d” (*detected*).

Como se verá más adelante esta diferencia es básica a la hora de los cálculos de la probabilidad de fallo en demanda (usa la fracción de tasa de fallo peligrosa) y del cálculo del tiempo de disparo esporius no deseado (usa la fracción de tasa de fallo segura). Asimismo, estos fallos pueden ser total o parcialmente detectados añadiendo un segundo subíndice a la tasa de fallos con las letras d (detectado) y u (no detectados). Añadir que tanto IEC 61508 como IEC 61511 establecen una mínima tolerancia de fallo de hardware (HTF), tanto para la lógica como para los sensores y elementos finales, para el cumplimiento de un determinado SIL con independencia del cálculo de la PFD_{MEDIA}. En el capítulo de este libro dedicado al diseño detallado del SIS, se explican con todo detalle estas restricciones de arquitectura y las diferentes tablas que han sido usadas hasta la fecha. A modo de introducción diremos que IEC 61511 proporciona tablas mostrando los niveles mínimos de redundancia que dependen del nivel de SIL y de la fracción de fallo segura (SFF), así como que los instrumentos de campo sean sin uso o con uso previo. IEC61511 también permite utilizar tablas (algo más complicadas) de la IEC 61508 como alternativa.

IEC 61508 proporciona dos rutas para satisfacer las restricciones de arquitectura requeridas para guardar un determinado nivel de SIL:

- Ruta 1H basada en la tolerancia de fallo de hardware y el concepto de fracción de fallo seguro (SFF) de cada elemento.
- Ruta 2H basada en datos reales de fiabilidad de los diferentes componentes provenientes de la información de los usuarios finales que aportan mayor confianza en la tolerancia de fallo de hardware y por tanto en el cumplimiento del SIL especificado (ejemplo: EXIDA dispone de bases de datos para diferentes componentes y su uso con la ruta 2H).

Tolerancia fallo de hardware (IEC 61508) Ruta 1H

Elemento tipo A (simples sin procesador o inteligencia; ejemplo: presostato, válvulas de corte, etc.).

Safe failure fraction of an element	Hardware fault tolerance		
	0	1	2
<60%	SIL 1	SIL 2	SIL 3
60% - <90%	SIL 2	SIL 3	SIL 4
90% - <99%	SIL 3	SIL 4	SIL 4
≥99%	SIL 3	SIL 4	SIL 4

Tolerancia fallo de hardware (IEC 61508) Ruta 1H

Elemento tipo B (con procesador; ejemplo: PLC, *smart transmiter*, etc.).

Safe failure fraction of an element	Hardware fault tolerance		
	0	1	2
<60%	Not allowed	SIL 1	SIL 2
60% - <90%	SIL 1	SIL 2	SIL 3
90% - <99%	SIL 2	SIL 3	SIL 4
≥99%	SIL 3	SIL 4	SIL 4

IEC 61508 RUTA 2H de Restriciones de Arquitectura

SIL	Minimum required HFT
1. (any mode)	0
2. (low demand mode)	0
2. (high demand or continuous mode)	1
3. (any mode)	1
5. (any mode)	2

Esta tabla es básicamente la misma que describe IEC 61511 para elementos con justificación de uso previo.

1.3.7. Otras definiciones

- ***Arquitectura***
  Composición de los elementos de hardware y/o software en un sistema. Por ejemplo:
  — Composición de los subsistemas del Sistema Instrumentado de Seguridad (SIS).
  — Estructura interna de un subsistema SIS.
  — Composición de los programas de software.

- ***Ciclo de vida de la seguridad***
  Lo conforman todas aquellas actividades necesarias involucradas en la implementación de las funciones instrumentadas de la seguridad que se producen durante un periodo de tiempo.

  Se nicia en la fase conceptual del proyecto y concluye cuando todas las funciones instrumentadas de seguridad ya no están disponibles para su uso (desmanteladas).

- ***Componente***
  Una de las piezas de un sistema, subsistema o dispositivo que ejecuta una función específica. Son los sensores o iniciadores, la lógica y los elementos finales de las SIF.

- ***Elemento final***
  Parte de un sistema instrumentado de seguridad que implementa la acción física necesaria para lograr un estado seguro.
  Los ejemplos comprenden válvulas, dispositivos de conmutación, motores con sus elementos auxiliares incluidos, por ejemplo, una válvula solenoide y un actuador si están involucrados en la función instrumentada de seguridad.

- ***Mitigación***
  Acción que reduce la(s) consecuencia(s) de un evento peligroso.

- ***MooN***
  Indica la votación de un sistema que está formado por "N" canales independientes, que están conectados de tal manera que basta activar "M" canales para que se ejecute la función instrumentada de seguridad (*M out of N*).

- ***Prevención***
  Acción que reduce la frecuencia con que se produce un evento peligroso.

- ***Protección de los activos***
  Función asignada al diseño del sistema con el objeto de evitar la pérdida de activos.

- ***Prueba funcional***
  Pruebas realizadas con el objeto de revelar defectos no detectados en un sistema instrumentado de seguridad de manera que, si fuera necesario, se puede volver a ajustar el sistema a su funcionalidad de diseño.

- ***Reducción del riesgo***
  Es la cuantificación del riesgo que tenemos que exigir para alcanzar un valor tolerable.

- ***Resolvedor lógico***
  La parte del SIS que realiza una o más funciones lógicas.

- ***Resolvedor lógico configurado para la seguridad***
  Resolvedor lógico electrónico y programable, para usos generales, de grado industrial, que está configurado específicamente para su utilización en aplicaciones de seguridad de acuerdo con la cláusula 11.5 de la Norma IEC61511-

I. Esta definición excluye las tarjetas de entrada y salida y amplificadores. Ejemplos son los relés electromecánicos y las unidades centrales de proceso (CPU) de los sistemas electrónicos programables (PLC en general).

- ***Riesgo del proceso***
  El riesgo que surge de las condiciones del proceso causado por hechos anormales (incluido el mal funcionamiento del BPCS).

- ***Seguridad funcional***
  La parte de la seguridad general relacionada con el proceso y el BPCS que depende del funcionamiento correcto de los SIS y otros sistemas protectores.

- ***Sensor***
  Dispositivo o combinación de dispositivos, que miden la condición del proceso (por ejemplo: transmisores, transductores, interruptores de proceso, interruptores de posición).

  En el caso de las funciones instrumentadas de seguridad el concepto de sensor (también llamado elemento iniciador) incluye a las tarjetas de entrada y los relés de entrada al resolvedor lógico.

- ***Sistema de control***
  Sistema que responde a las señales de entrada del proceso y/o de un operador y genera señales de salida que hacen que el proceso opere en la forma deseada.

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

- ***Sistema de Control Básico de Proceso (Basic Process Control System - BPCS)***
  Un sistema que responde a las señales de entrada del proceso, de su equipo asociado, de otros sistemas programables y/o de un operador y genera señales de salida haciendo que el proceso y su equipo asociado operen de la manera deseada pero que no se utilizan para funciones instrumentadas de seguridad.

- ***Validación***
  La actividad de demostrar que la función o las funciones instrumentadas de la seguridad y el sistema o los sistemas instrumentados de seguridad bajo consideración después de la instalación cumplen en todos los aspectos con la especificación de los requisitos de seguridad. Por lo tanto se valida el SIS.

- ***Verificación***
  La actividad de demostrar respecto de cada fase del ciclo de vida pertinente, mediante análisis y/o pruebas, que las entradas y las salidas específicas cum-

plen en todos los aspectos con los objetivos y requisitos establecidos para las fases específicas. Por lo tanto se verifican las fases del ciclo de vida de seguridad.

PARA NO OLVIDAR:

- Los *Sistemas Instrumentados de Seguridad* (SIS) son la formalización de las llamadas Buenas Prácticas.

CONSEJOS PRÁCTICOS

- Familiarizarse con los conceptos y definiciones incluidos en los estándares.
- Conseguir una visión global del sistema de seguridad que queremos estudiar.
- Saber identificar las SIF que forman parte del SIS.