Julio Rivas, Pedro Manuel Redondo

3310.05 Ingeniería de procesos

SISTEMAS INSTRUMENTADOS DE SEGURIDAD (SIS):CICLO DE VIDA

Recibido: 10/05/07
Aceptado: 05/06/07

SAFETY INSTRUMENTED SYSTEMS (SIS): SERVICE LIFE

Julio Rivas Escudero
Ingeniero Técnico Industrial
Asesor de grandes proyectos de **Petronor**

Pedro Manuel Redondo Sobrado
Ingeniero Químico
Jefe del Dep. de Control Avanzado e Instrumentación
Dirección de Tecnología e Ingeniería **Repsol YpF**

RESUMEN

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.

El SIS constituye la última capa de Seguridad preventiva y su correcto diseño, instalación, pruebas y mantenimiento (ciclo de vida) son la garantía de su adecuado funcionamiento cuando, bajo demanda, le sea requerido. Si esta capa falla, el evento peligroso se desencadenará produciendo fugas, explosiones, incendios, etc. con las consecuencias que esto puede acarrear en costes y/o pérdidas humanas. Después de esta última capa preventiva, sólo aparecen las de mitigación que intentan minimizar las consecuencias (sistemas de fuego y gases, planes de emergencia, etc.).

Un sistema instrumentado de seguridad (SIS) puede ser definido 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"

Es, por tanto, crítico y fundamental que las Empresas de Proceso tengan en consideración en sus Proyectos que la Seguridad industrial de sus instalaciones pasa por el cumplimiento estricto de cada paso del ciclo de vida que las modernos estándares internacionales (ISA e IEC) definen y procedimentan.

Este artículo trata de exponer no sólo qué es un SIS sino también significar su importancia, enumerar los mejores estándares, así como describir cada uno de los pasos de su ciclo de vida dando finalmente unas recomendaciones de aplicación y una relación de los acrónimos utilizados.

Palabras clave: Sensores, seguridad, emergencia, mantenimiento.

ABSTRACT

An Safety Instrumented System (SIS) is a new term used in the standards that normally also have been and are known by the majority like: Emergency Shutdown System (ESD), Safety Shutdown System, Interlock System, Emergency tryps System, Security systems, etc.

The SIS constitutes the last layer of preventive security and their correct design, installation, tests and maintenance (life cycle) are the guarantee of their suitable operation when, under demand, it is required. If this layer fails the dangerous event will be triggered producing leakages, explosions, fires, etc with the consequences that this can carry in costs and/or human lost. After this last single preventive layer they appear those of mitigation that try to diminish the consequences (fire and gases systems, plans of emergency, etc.).

An Safety Instrumented System (SIS) can be defined as: "A System made up of sensors, final logic and elements in order to take to the determined process to a safe state when pre-established conditions are violated"

It is therefore critical and fundamental that the Companies of Process have in consideration in their Projects that the industrial safety of its facilities happens through the strict fulfillment of each step of the life cycle that the modern international standards (ISA and IEC) define.

This article tries to expose not only that is a SIS but also to mean its importance, to enumerate the best standards, as well as to as much describe each one of the steps of its life cycle giving finally recommendations and identification acronyms.

***Key words**: Sensors, safety, emergency, maintenance.*

1.-INTRODUCCIÓN

Sistema de enclavamientos, Sistema Instrumentado de Seguridad, Sistema de parada en emergencia, etc., la variedad de nombres parece algo ilimitado.

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. Ello afecta al propio diseño 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:

- 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'S redundantes? Algunos prefieren no usar sistemas basados en *software* en aplicaciones de seguridad. ¿Es una buena recomendación?

- 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?

- Elementos de campo

¿Deberían los elementos sensores iniciadores ser de tipo transmisor o interruptor (*switch*)? Si usamos transmisores, ¿analógicos o digitales? ¿Reducción 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 trabajo es tratar de dar respuestas a estas preguntas y de clarificar la confusión general que sobre estos sistemas se está produciendo.

2.-CAPAS DE SEGURIDAD: PREVENCIÓN Y MITIGACIÓN

La figura es (con ligeros matices) la que se representa en la mayoría de los estándares para separar las diferentes capas de seguridad que deben tenerse en cuenta en cualquier diseño y desarrollo de un proyecto.

Varias de esas capas son preventivas y otras, de mitigación. Algunas de ellas necesitan instrumentos y otras, no. En cualquier caso, el concepto de separar en capas la Seguridad de una planta responde a un concepto básico y simple: "*No poner todos los huevos en la misma cesta*".

2.1. Capas de prevención

Son aquéllas 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:

2.1.1. Diseño de la planta

El diseño de cualquier planta de proceso debe, por sí mismo, realizarse teniendo siempre en cuenta la Seguridad. Además de un correcto diseño conceptual y básico, la realización de un estudio de riesgos y operabilidad, tendente a identificar, evaluar y controlar los riesgos (accidentes e incidentes) de procesos es algo que se considera básico al inicio de la Ingeniería de detalle de cualquier proyecto (Ej. HAZOP).

2.1.2. Sistema de Control de procesos

El sistema de control de procesos es el siguiente paso en las capas de Seguridad. Es el encargado de mantener las variables de operación en sus puntos de consigna y dentro de márgenes seguros.

2.1.3. Sistemas de alarmas

Si el sistema de control falla y, por cualquier razón, no realiza su función, el siguiente nivel corresponde a las alarmas, que alertan al operador y le posibilitan para una intervención manual.

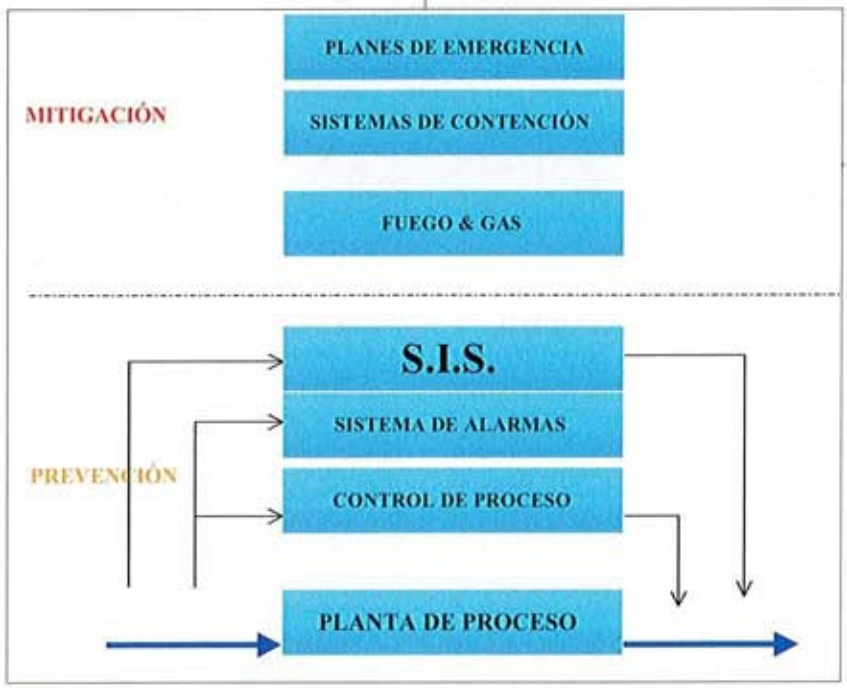

Fig. 1

2.1.4. Sistemas Instrumentados de Seguridad

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 los sensores y válvulas de campo.

2.2. Capas de mitigación

Son aquéllas que se diseñan para paliar o limitar las consecuencias de un peligro una vez que éste realmente ha sucedido. Las más importantes son:

2.2.1. Fuego y gas

Si el sistema instrumentado de seguridad falla y el accidente tiene lu-

gar (explosión, fuga, incendio, etc.), los sistemas de fuego y gas pueden ser usados para mitigar o minimizar las consecuencias del mismo.

En EEUU., estos sistemas sólo son usados como alarma, no tomando ninguna acción automática; Fuera de EEUU., sí suelen tomar acción automática y normalmente están integrados en las mismas plataformas que los SIS.

Una diferencia interesante entre los sistemas de fuego y gas y los SIS es que estos últimos están normalmente energizados (se desenergizan para producir la parada) y los de fuego y gas están normalmente desenergizados (se energizan para tomar acción).

2.2.2. Sistemas de contención

Ejemplos de estos sistemas son los pocetos de los tanques de productos, los edificios contenedores de reactores nucleares, etc.

2.3. Planes de emergencia

En el caso de un evento catastrófico, se debe disponer de procedimientos y planes de emergencia internos y externos que se activen en función de la gravedad de dicho evento. Aunque esta capa no dispone de sistemas físicos (instrumentos y equipos), salvo las sirenas, se considera una capa más de mitigación de seguridad.

3.-ESTÁNDARES Y NORMATIVAS

Ante todo, conviene clarificar la diferencia existente entre lo que es de obligado cumplimiento por ley y lo que simplemente es una buena práctica de diseño y trabajo recogido en especificaciones, estándares y normas. También es posible que lo que puede ser obligatorio en un país, puede no serlo en otros o viceversa.

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*". Otro es de Directiva *ATEX*.

Referente a los Sistemas Instrumentados de Seguridad (SIS), no hay ninguna Directiva ni R.D. que obligue a su cumplimiento. Sí 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, se enumeran los estándares y normas más importantes a tener en cuenta en el diseño y desarrollo de los mismos. A estos efectos, se separan en dos grupos: en el primero se enmarcan los Organismos que definen los mejores estándares y prácticas de diseño e Ingeniería de SIS y en el segundo, aquéllos cuyos estándares y guías deben ser integrados con los anteriores.

En el primer grupo está la ISA (**Sociedad Internacional de Instrumentación, Sistemas y Automatización**) y la I.E.C. (**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 enfocado sólo 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 2003) y, ya que dentro de la IEC está representando a EEUU 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 84.01/2003 es básicamente idéntico al IEC 61511 con la inclusión de una cláusula de salvaguarda (abuelo-*grandfather*) que afecta a modificaciones en instalaciones existentes.

IEC tiene dos estándares relacionados con los sistemas instrumentados de seguridad: IEC 61508 "*Seguridad funcional: Sistemas relacionados con la seguridad*" versión actual de 1999 y próxima en 2005, 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 sólo 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.

En el segundo grupo se encuentran una serie de Organismos que disponen de estándares y normas cuyas guías son de suma utilidad para complementar los anteriores de **ISA** e **IEC**. Entre ellos se encuentran:

- AICHE (**American Institute of Chemical Engineers**), con varios libros entre los que destaca el relativo a "*Guías de automatización segura en procesos químicos*".
- API (**American Petroleum Institute**). Con su práctica de recomendación RP14C de "*Sistemas de parada en plataformas petrolíferas*".
- NFPA (**National Fire Protection Association**). Este Organismo dispone de estándares que aplican a calderas, hornos y sistemas de control de quemadores.
- OSHA (**Occupational Safety and Health Administration**). Con su OSHA de "*Gestión de la Seguridad en el proceso de plantas químicas altamente peligrosas*".
- ASME, ISO, etc.

4.-TERMINOLOGÍA Y DEFINICIONES

Algunas terminologías y definiciones más usadas:

4.1.- 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 Pa-

rada de Emergencia (ESD), Sistema de Parada de Seguridad, Sistema de enclavamientos, Sistema de disparos de emergencia, Sistemas de seguridad, etc.

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"*

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*".

4.2.- SIL (Safety Integrity Level) o Nivel de Integridad de Seguridad.

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*".

Especificar la integridad de la seguridad no consiste sólo en definir 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, %
1	90,00 – 99,00
2	99,00 – 99,90
3	99,90 –99,99
4	> 99,99

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 sólo se pueden considerar de forma cualitativa.

4.3.- Probabilidad media de fallo de funcionamiento a la demanda (PFDMEDIA)

Para calcular de una forma numérica el SIL, uno de los parámetros más utilizados es la PFD_{MEDIA}, que 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.

La relación de la PFD_{MEDIA} con los SIL es la siguiente:

SIL	Disponibilidad, %	PFD_{MEDIA}
1	90,00 – 99,00	$10^{-2} – 10^{-1}$
2	99,00 – 99,90	$10^{-3} – 10^{-2}$
3	99,90 –99,99	$10^{-4} – 10^{-3}$
4	> 99,99	$10^{-5} – 10^{-4}$

Matemáticamente, el cálculo de la PFD_{MEDIA} es muy complejo si se intenta hacer sobre la función de Seguridad en su conjunto.(Fig. 2).

Fig. 2

Para simplificarlo, se hace 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:

4.4.-Ciclo de vida de Seguridad

Es uno de los conceptos básicos de la norma. Según cita ésta, el ciclo de vida de seguridad comprende aquellas *"actividades necesarias implicadas en la instalación de sistemas relacionados con la Seguridad, que se presentan durante un periodo de tiempo que empieza en la fase de diseño conceptual de un proyecto y termina cuando todos los sistemas E/E/PE relacionados con la Seguridad, o los sistemas relacionados con la Seguridad de otra tecnología e instalaciones de reducción del riesgo externo ya no se encuentran disponibles para su utilización"*.

Incluye todas las actividades relacionadas con un SIS desde la concepción del proceso o del propio SIS hasta su desinstalación.

Como un sistema de seguridad no es un componente simple, requiere la participación de un equipo multidisciplinar y de una sistemática precisa para evitar los fallos. Lo que la Norma intenta es que el objetivo de la Seguridad guíe todas las fases del diseño, la construcción, la operación y el mantenimiento de un proceso. Los datos demuestran que, aunque está sistemática aumenta los costes iniciales a la larga produce un sistema más seguro y,

por lo tanto, un aumento en la producción.

Según ANSI / ISA S84.01-1996, el ciclo de vida contempla, de forma resumida, las siguientes fases (Fig.3):

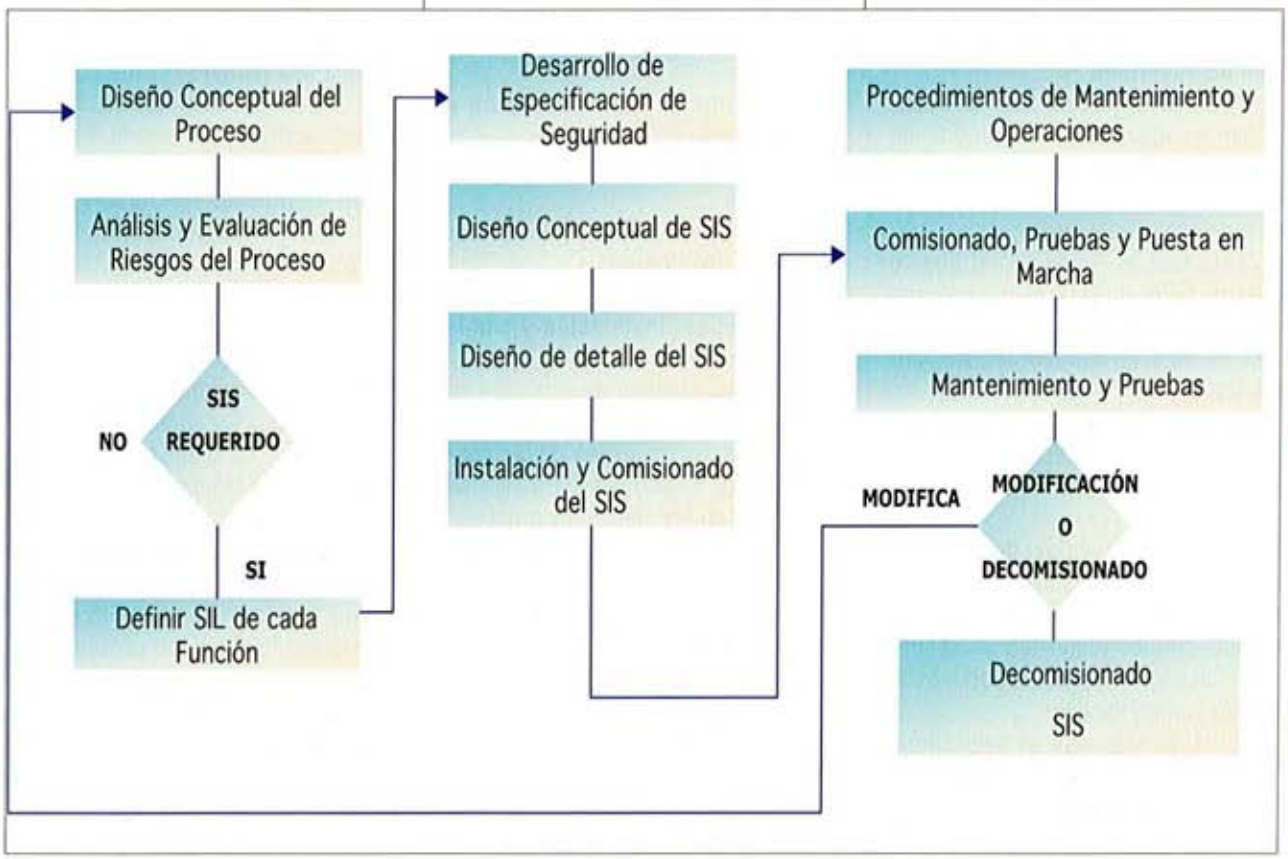

Fig. 3

El significado de las fases es el siguiente:

a. Diseño conceptual del proceso

El objetivo de esta fase es diseñar una planta que sea inherentemente segura. Para ello será necesario conocer el proceso, los equipos y el entorno en suficiente profundidad. En general, esta fase suele quedar fuera del alcance del especialista en Control y depende fundamentalmente del especialista en procesos.

b. Análisis y evaluación de riesgos del proceso

El primer objetivo de esta fase es entender todos los riesgos asociados al proceso, ya tengan impacto sobre el personal, la producción, los equipos el medio ambiente o la imagen de la compañía. Existen varias técnicas de Análisis de riesgos, aunque una de las más utilizadas es el análisis HAZOP.

El segundo objetivo de esta fase es evaluar los riesgos identificados en el análisis anterior para establecer un *ranking*. La evaluación de los riesgos puede ser:

- Cualitativa.
- Cuantitativa.

En esta fase estarán implicados especialistas de varias disciplinas: Control, Procesos, Operaciones, Instrumentación, Electricidad, etc.

c. Aplicación de capas de protección de Sistemas de Seguridad no Instrumentados

El objetivo de esta fase es evaluar qué tipo de capa de protección es la adecuada para lograr una disminución del riesgo hasta niveles aceptables (ALARP = *As Low As Reasonably Practical* o Tan bajo como sea razonablemente práctico).

Las capas de protección seleccionadas siempre en primer lugar, deben ser siempre las más sencillas (preferiblemente no-instrumentadas). Si esto fuera posible, aquí se pararía el proceso y sólo en el caso de que no sea suficiente con la aplicación de capas de protección sencillas, se debe elegir el uso de Sistemas Instrumentados de Seguridad (SIS).

Esta fase típicamente se realiza inmediatamente después de la anterior, por lo que están implicados los integrantes del mismo equipo interdisciplinario.

d. Definición del SIL objetivo de cada función

El objetivo de esta fase es definir el SIL requerido para cada SIS para conseguir la adecuada reducción del riesgo hasta un nivel aceptable.

El cálculo del SIL requerido no es, por tanto, una medida directa del riesgo del proceso, sino una medida de la disponibilidad del sistema de Seguridad que es necesario para mantener los riesgos del proceso en el nivel que hemos fijado como aceptable.

Es seguramente una de las fases más complejas de realizar.

El cálculo del SIL requerido se puede hacer mediante:

- Métodos cualitativos.
- Métodos cuantitativos.

Esta fase típicamente se realiza inmediatamente después de la anterior por lo que están implicados los integrantes del mismo equipo interdisciplinario.

e. Desarrollo de la especificación de Seguridad

El objetivo de esta fase es desarrollar la especificación con todos los requisitos de Seguridad. Esencialmente consiste en especificar la lógica funcional del Sistema.

Esta fase es fundamental puesto que un fallo en esta especificación (fallo funcional o sistemático) no será fácil de detectar durante las siguientes fases.

En esta fase estarán implicados principalmente los especialistas en Procesos y en Control.

f. Diseño conceptual del SIS

El objetivo de esta fase es desarrollar un diseño inicial del SIS que cumpla con los requisitos de Seguridad y alcance el SIL requerido o establecido como objetivo.

Durante esta fase se seleccionarán la tecnología, la arquitectura, los intervalos de prueba, etc., teniendo en cuenta factores tales como el presupuesto, el tamaño de la aplicación, la complejidad, la velocidad de respuesta, la política de puenteos, los requisitos de comunicaciones, la interfaz con el operador, etc.

Este diseño se realizará de acuerdo a la especificación de requerimientos de Seguridad (SRS) y, una vez completado, deberá ser verificado que el SIL de cada función de Seguridad instrumentada (SIF) es el correcto para lo cual deberá comprobarse que la probabilidad de fallo en demanda del conjunto del sensor/res, lógica y elemento/os finales es la adecuada al SIL requerido.

En esta fase ya entra de lleno en la responsabilidad del especialista de Control.

g. Diseño de detalle del SIS

El objetivo de esta fase es desarrollar un diseño en detalle del SIS que cumpla con los requisitos de Seguridad y alcance el SIL requerido o establecido como objetivo.

El diseño debe incluir al menos la siguiente información:

- Documentos de Configuración de los equipos.
- Documentos de Prueba de los equipos.
- Documentos de Instalación de los equipos.
- Documentos de Operación / Mantenimiento de los equipos.
- Documentos de Verificación de los equipos.

Esta fase es responsabilidad del especialista de Control.

h. Pruebas, instalación y comisionado del SIS

El primer objetivo de esta fase es asegurar que el sistema se comporta conforme a los requisitos de la Especificación de Seguridad. Para ello, se deben realizar las siguientes pruebas:

- Pruebas FAT (*Factory Acceptance Test*). Típicamente serán pruebas del operador lógico en la fábrica del suministrador.
- Pruebas SAT (*Site Acceptance Test*). Típicamente serán pruebas del sistema completo (sensores, operadores lógicos, actuadores, servicios, etc.) en la propia planta.

El segundo objetivo de esta fase es asegurar que el sistema se instala de acuerdo a los procedimientos especificados.

Esta fase es responsabilidad del especialista de Control.

i. Realización de los Procedimientos de operación y mantenimiento del SIS

El primer objetivo de esta fase es asegurar que en los procedimientos operativos se documenten las respuestas específicas a las desviaciones en el proceso, las alarmas y las paradas. Los procedimientos operativos deben informar al operador de los riesgos del proceso y las consecuencias potenciales si las alarmas y las paradas no se activan.

El segundo objetivo de esta fase es asegurar que los procedimientos de mantenimiento sean detallados y escritos desde una perspectiva técnica con el suficiente detalle para asegurar que todos los dispositivos de los SIS sean totalmente comprobados y vuelven al servicio tras cada chequeo

j. Mantenimiento y Pruebas del SIS

El objetivo de esta fase es asegurar que cada una de las partes del sistema sea periódicamente comprobada según la frecuencia establecida durante el diseño de detalle. Por otra parte, también será necesaria la realización de pruebas funcionales periódicas del sistema completo (verificación) según la frecuencia establecida durante el diseño de detalle.

Es fundamental que toda la información de mantenimiento sea adecuadamente documentada para, en su caso, poder ser auditada.

Esta fase es responsabilidad del especialista de Mantenimiento.

k. Modificaciones del SIS

El objetivo de esta fase es asegurar que todo cambio en el SIS se realiza siguiendo el mismo procedimiento que en la primera implementación. La gestión del cambio implicará que, ante cada cambio, se deberá volver a la fase adecuada en el ciclo de vida del SIS.

Todo cambio será debidamente documentado. Por ello es fundamental tener un estricto control de toda la documentación.

Esta fase es responsabilidad del equipo multidisciplinar ya citado.

l. Decomisionado del SIS

Entiéndese como decomisionado a las tareas que hay que realizar para eliminar una o varias funciones instrumentadas de seguridad cuando se constata que no son necesarias.

El objetivo de esta fase es asegurar que el decomisionado de un SIS no tiene impacto ni en el proceso ni en otras unidades anexas.

5.- RELACIÓN ENTRE LOS SISTEMAS DE CONTROL Y LOS SIS

Los estándares de los SIS recomiendan la total separación e independencia de las funciones de los SIS y las funciones de los SCD para que la integridad de la Seguridad no se vea comprometida. En general, las ra-

zones de la separación son las siguientes:

• Reducir los efectos del SCD sobre los equipos compartidos.

• Facilitar las operaciones del SCD (flexibilidad en los cambios, mantenimiento, pruebas, documentación, etc.) para no tener que seguir procedimientos tan rígidos.

• Disminuir la complejidad del SIS para facilitar la validación de la Seguridad funcional.

La separación física de los diferentes elementos no es obligatoria siempre que la independencia asegure que el SIS no se verá afectado por:

• Fallos en el SCD.

• Operaciones (mantenimiento, configuración, operación, etc.) realizadas en el SCD.

La independencia de elementos del SIS y el SCD es muy compleja en aplicaciones muy interrelacionadas (por ejemplo, máquinas). Sin embargo, en sistemas con lógica sencilla y/o pocas actuaciones (por ejemplo, sistemas de fuego y gas) no suele presentar demasiadas complicaciones o incluso no ser imprescindible.

Las áreas donde es altamente recomendada la separación entre Sistemas de control y SIS son las siguientes:

a. Sensores de campo

Se recomienda el uso de sensores de campo independientes y preferiblemente utilizando conexiones al proceso independientes. Sin embargo, se pueden utilizar sensores comunes siempre que el fallo del propio sensor no produzca precisamente una situación peligrosa a través de la acción de control. En la práctica, esto solamente suele ser factible para funciones con SIL= 1. La conexión adicional de los sensores del SIS al SCD ofrece la posibilidad de contraste con los sensores del SCD y, por lo tanto, mejora la cobertura de los diagnósticos.

b. Plataformas de lógica

Se recomienda el uso de plataformas de lógica independientes (tanto en CPU como en tarjetas de E/S). Sin embargo, se pueden tener aplicaciones de Seguridad y de control en la misma CPU siempre que dichas aplicaciones sean estancas. En la práctica, las CPU del SCD no suelen alcanzar los requerimientos mínimos exigibles (tasa de fallos, cobertura de diagnósticos, fracción de fallos seguros, etc.) para aplicaciones con un SIL ≥ 1.

c. Elementos finales de control

Se recomienda el uso de actuadores independientes. Sin embargo, se pueden utilizar actuadores comunes siempre que el fallo del propio actuador no produzca precisamente una situación peligrosa a través de la acción de control y siempre que la señal al actuador procedente del SIS tenga preponderancia sobre la señal procedente del SCD. En la práctica esto solamente suele ser factible para funciones con SIL= 1.

d. Cableado

Se recomienda el uso de cajas y cables múltiples independientes para señales del SCD y del SIS. Esta recomendación se torna en obligatoria cuando se trata de SIS con configuración energizada para disparo.

Las bandejas, *conducto de cables* y similares pueden ser comunes.

6.-INTERFACES DE OPERACIÓN E INGENIERÍA / MANTENIMIENTO

6.1.-La interfaz de operación

Es el medio por el cual el operador se comunica con el SIS.

La interfaz de operación puede ser común para el SCD y los sistemas de seguridad instrumentados. Sin embargo, no deberán ser comunes aquellas interfaces en las que el operador sea una parte de la función de seguridad (por ejemplo, un disparo que necesite la autorización adicional del operador mediante un pulsador).

Interfaces de operación típicas son: pantallas, paneles de lámparas y pulsadores, anunciadores e impresoras.

La especificación de diseño del sistema de seguridad debe explicitar claramente las informaciones que, por su relevancia, deben ser mostradas al operador así como la forma de mostrarlas. Especial importancia tienen todas las señales informativas sobre el *status* de las diferentes partes del SIS. Es muy importante no sobrecargar de información al operador y proporcionar, si procede, programas estáticos y dinámicos que optimicen la misma.

6,2.-La interfaz de Ingeniería / mantenimiento

Es el medio por el cual se realizan las modificaciones en el SIS.

Debe ser una interfaz independiente para cada SIS y no debe usarse como interfaz de operación.

Debe tener unos protocolos de seguridad muy estrictos porque tendrá acceso a todos los parámetros de configuración del sistema (*hardware* y *software*).

7.-RESUMEN, CONCLUSIONES Y RECOMENDACIONES

7.1.-Resumen

a. ¿Cómo afectan los estándares de los SIS al diseño?

El análisis de riesgos y de las capas de protección debe realizarse en cuanto se tenga la primera revisión de los P&I D. Este análisis identificará los riesgos, seleccionará la capa de protección adecuada y asignará a cada una de ellas la reducción de riesgo requerida. Para las funciones instrumentadas de seguridad, la reducción de riesgo es equivalente al nivel de integridad de seguridad. El SIL suele requerir unas necesidades de redundancia y de pruebas funcionales (identificadas en la Especificación Funcional de Seguridad y en la Guía de diseño) que suelen ir más allá de las practicas actuales de las plantas. Las implementaciones exitosas, también implican unas bien planificadas y fiables comunicaciones con el SCD.

b. ¿Cómo afectan los estándares de los SIS a la operación?

En términos de procedimientos operativos, muchos procedimientos se centran en el control de la calidad y otros parámetros operacionales asociados. Los procedimientos operativos suelen verse más como un medio para conseguir una determinada calidad en un producto. Los estándares de los SIS requieren que en los procedimientos operativos se documenten las respuestas específicas a las desviaciones en el proceso, las

alarmas y las paradas. Los procedimientos operativos deben informar al operador de los riesgos del proceso y las consecuencias potenciales si las alarmas y las paradas no se activan. Los procedimientos operativos incluirán las respuestas apropiadas ante perturbaciones, mal funciones y alarmas del proceso y diagnósticos de fallos del SIS.

c. ¿Cómo afectan los estándares de los SIS al mantenimiento?

La importancia del mantenimiento y las pruebas funcionales esta bien documentado en los estándares de los SIS. Los procedimientos de mantenimiento proporcionarán procedimientos detallados y escritos desde una perspectiva técnica con el suficiente detalle para asegurar que todos los dispositivos de los SIS son totalmente comprobados y vuelven al servicio. Los procedimientos bien escritos suelen verse como una forma de garantizar la consistencia del comportamiento, que es el único camino de conseguir la integridad deseada del dispositivo. Los procedimientos de mantenimiento serán lo suficientemente detallados para asegurar que los dispositivos están apropiadamente probados y vueltos al servicio, garantizando el rendimiento del dispositivo SIS.

7.2.-Conclusiones

- Existencia de confusionismo en todo lo relacionado con estos Sistemas.
- Falta de clarificación y uniformidad de criterios en la aplicación de los estándares y normas.
- Insuficiente formación de los técnicos responsables de estos trabajos a lo largo del ciclo de vida de un SIS (diseño, montaje, mantenimiento, operación, etc.).

7.3.-Recomendaciones.

La importancia de los Sistemas Instrumentados de Seguridad (SIS) es vital para la Seguridad de funcionamiento de las Plantas de Proceso

Actualmente las empresas y compañías más importantes del mundo están decidiendo, con buen criterio, aplicar en esta capa preventiva las mejores prácticas que, al día de hoy, son las contempladas en los estandares ISA e IEC generando asimismo las normas y especificaciones complementarias a dichos estándares.

La correcta aplicación de estos estándares implica una serie de actividades las cuales requieren gran dedicación y conocimiento por parte de todos los implicados en todas y cada una de las fases que constituyen el Ciclo de Vida de un SIS.

Como resumen se recomienda en las empresas que decidan poner en práctica estos estándares lo siguiente:

- Creación grupos de trabajo de expertos para Sistemas de Seguridad que se encargue de:
  - Realizar una Especificación funcional fijando criterios tales como: tecnología utilizada, arquitectura, política de puenteos, requisitos de comunicaciones, interfaz con el operador, etc.
  - Definir los criterios mínimos de los documentos generados durante el diseño de detalle de los SIS. Entre otros, los documentos referentes a: Configuración, Pruebas (FAT y SAT), Instalación, Operación / Mantenimiento y Verificación de los equipos SIS.
  - Definir los criterios mínimos que, referentes a los SIS, deben incluirse en los Procedimientos de Operación y Mantenimiento.
  - Definir los criterios mínimos para asegurar la adecuación a las normas, que deben tenerse en cuenta en:
    - La gestión del Mantenimiento.
    - La gestión de las Verificaciones.
    - La gestión del Cambio.

    Todo ello en el ámbito de:
    - Nuevos proyectos.
    - Modificaciones de unidades existentes.
    - Y en SIS ya instalados y en funcionamiento.
- Formación / certificación de varias personas por centro en la norma IEC 61511.

ACRÓNIMOS UTILIZADOS

AICHE: American Institute of Chemical Engineers
ANSI: American National Standards Institute
API: American Petroleum Institute
ESD: Emergency Shutdown System
FAT: Factory Acceptance Test
HAZOP: Análisis Funcional de Operatividad
IEC: International Electrotechnical Commission
ISA: Sociedad Internacional de Instrumentación, Sistemas y Automatización
NFPA: National Fire Protection Association
OSHA: Occupational Safety and Health Administration
PLC: Programmable Logic Controller
SAT: Site Acceptance Test
SIF: Safety Instrumented Function
SIL: Safety Integrity Level
SIS: Safety Instrumental System
SRS: Safety Requirements Specification

8.-BIBLIOGRAFÍA

- ANSI/ISA SP84.01 Aplicación SIS para la Industria del Proceso.
- IEC 61508 Seguridad funcional: Sistemas relacionados con la Seguridad.
- IEC 61511 Seguridad funcional: SIS para el sector de la Industria del Proceso.
- GRUHN, Paul y CHEDDIE, Harry L. *Safety Shutdown Systems: Design, Analysis and Justification*
- RIVAS, Julio. *Master de Instrumentación y Control ISA/ISE* (Módulo 10)
- Especificaciones de diseño relacionadas con los SIS de Repsol. ■