

Se

SEGURIDAD

P. Ojeda Rodríguez
V. Macías Jaén
M.Á. Muñoz Aguilar
División de Seguridad
Industrial
Inerco, S.A.



Diseño y verificación de los SIS en instalaciones de procesos

Se destacan los sistemas instrumentados de seguridad (SIS) entre las medidas de prevención de accidentes en instalaciones industriales, los cuales llevan el proceso a un estado de seguridad cuando se vulneran unas condiciones predeterminadas. Estos sistemas no controlan, sino que actúan bajo demanda en caso de fallo de las demás sistemas de prevención que existen en la instalación.

A LA HORA DE DECIDIR CUÁL ES LA seguridad existente en las instalaciones, hay que tener en cuenta que cualquier fallo de control, mal mantenimiento o incluso fallos debido a factores ambientales pueden ser motivo de riesgo y, por lo tanto, de accidente. Es por ello que, desde hace tiempo, se han llevado a cabo estudios para conseguir reducir los riesgos existentes en las instalaciones industriales; más aún, después de todos los accidentes importantes ocurridos en las últimas décadas, como los ocurridos en Seveso o Flixborough.

Los diferentes sistemas de control hacen que una instalación opere de forma óptima, dentro de unos límites establecidos, lo cual no significa que dicha operación se realice de forma segura. Para tratar de certificar esta situación de seguridad, existen medidas de mitigación (por ejemplo, los sistemas de alivio, las repuestas de la planta y de la población ante una emergencia o los sistemas fuego&gas) que impiden el desarrollo de las consecuencias de un accidente. Pero, ¿por qué no actuar antes de que se produzca el accidente? Ante esta pregunta surge una respuesta inmediata: la introducción en la industria de

UNA DE LAS PRINCIPALES CARACTERÍSTICAS DE LOS SIS ES SU INDEPENDENCIA DE CUALQUIER OTRO SISTEMA DE CONTROL O CAPA DE PREVENCIÓN

las medidas de prevención. Estas medidas lo que buscan es disminuir la probabilidad de ocurrencia de los accidentes previniendo las consecuencias de los mismos. Y entre estas medidas destacan sobre manera los sistemas instrumentados de seguridad (SIS) como última capa de prevención, llevando el proceso a un estado de seguridad cuando se vulneran unas condiciones predeterminadas. Este sistema no controla, sino que sólo actúa bajo demanda en caso de fallo de las demás capas de prevención existente en la instalación. Por ello, una de las principales características de los SIS es la independencia de cualquier otro sistema de control o capa de prevención.

1 CICLO DE VIDA DE UN SIS

Los sistemas instrumentados de seguridad están compuestos, básicamente, por tres grupos de elementos:

- Elemento primario o sensor(es).
- Unidad lógica.
- Elemento final o actuador(es).

Un esquema posible de este sistema se muestra en la Figura 1.

La vida de un sistema instrumentado de seguridad se analiza como un ciclo, desde su concepción inicial hasta su desmantelamiento. Las etapas de este ciclo de vida son:

- Diseño conceptual del proceso.
- Análisis de riesgos (por ejemplo, HAZOP).
- Cálculo del índice SIL.
- Desarrollo de las especificaciones de los requisitos de seguridad (SRS).
- Diseño conceptual del SIS y verificación del diseño.
- Diseño detallado del SIS.
- Instalación y comisionado.
- Operación y mantenimiento.
- Modificaciones.
- Desmantelamiento y retirada de servicio.

En las normativas existentes sobre seguridad funcional, IEC 61508/61511 y ANSI/ISA S84, se especifica que, para cada función que deben llevar a cabo los SIS, se debe cumplir con un nivel íntegro de seguridad (SIL, *Safety Integrity Level*) que se corresponde con un factor de reducción de riesgo, relaciona-

Figura 1
Arquitectura de un sistema instrumentado de seguridad



do con la probabilidad de fallo en demanda de cada función (Tabla 1).

Una vez calculado este índice SIL, se debe tener en cuenta una serie de características que influyen en su configuración e instalación para que se cumplan las prescripciones técnicas establecidas en las normativas y estándares sobre seguridad funcional. Todo ello se analiza en el punto del ciclo de vida correspondiente a la etapa de diseño y verificación del SIS.

2 DISEÑO Y VERIFICACIÓN DEL SIS

Esta etapa trata de verificar que el SIS se diseña con unos requisitos mínimos de exigencia en seguridad, verificando que cumple con el SIL calculado en la etapa previa del ciclo de vida correspondiente al cálculo del nivel SIL.

Para ello hay que realizar un diseño conceptual del sistema instrumentado de seguridad, eligiendo sensor(es), lógica y elemento(s) final(es) o actuador(es) disponibles en el mercado que realicen las funciones del SIS (SIF, *Safety Instrumented Functions*). Una vez elegida la arquitectura de cada SIF, hay que verificar que el SIL correspondiente con esa arquitectura es el mismo que el nivel SIL que previamente se ha obtenido en la etapa de cálculo. Si este SIL no alcanza el SIL establecido para cada función instrumentada de seguri-

TABLA 1

RELACIÓN DE LOS ÍNDICES SIL CON PFD Y RFF

Nivel de integridad de seguridad (SIL)	Probabilidad de fallo media objetivo de fallo bajo demanda	Factor de reducción de riesgo
4 ¹⁾	$\leq 10^{-11}$ a $< 10^{-10}$	> 10.000 a ≤ 100.000
3	$\leq 10^{-9}$ a $< 10^{-8}$	> 1.000 a ≤ 10.000
2	$\leq 10^{-7}$ a $< 10^{-6}$	> 100 a ≤ 1.000
1	$\leq 10^{-5}$ a $< 10^{-4}$	> 10 a ≤ 100

¹⁾ El índice SIL 4 sólo se conforma en los estándares IEC 61508-61511 y no en el estándar ANSI/ISA S84

SE DEBEN COMPROBAR LAS RESTRICCIONES QUE NOS IMPONEN LAS NORMATIVAS PARA EL ADECUADO CUMPLIMIENTO DE LA ARQUITECTURA DE LOS SIS

dad, hay que modificar la configuración hasta que cumpla con este último.

Para comprobar qué índice SIL le corresponde a esa arquitectura debemos de calcular la probabilidad de fallo en demanda (PFD) para cada SIS. Esta PFD depende de una serie de conceptos que influyen en el diseño del SIS, como son:

- Tasa de fallos (λ): es el número de fallos del elemento por unidad de tiempo.
- Tasa de autodiagnósticos (C): es el porcentaje de fallos que serían detectados en pruebas autodiagnósticas.
- Frecuencia del intervalo de pruebas (T): es el intervalo de tiempo en el que se comprueba que el elemento funciona correctamente.
- MTTR (*Mean Time To Repair*): es el tiempo medio que se necesita para reparar el sistema una vez que ha fallado.

TABLA 2

TOLERANCIA MÍNIMA A LOS DEFECTOS DE *HARDWARE* DE LAS UNIDADES LÓGICAS DE ELECTRÓNICA PROGRAMABLE (PE). IEC 61511

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

TABLA 3

TOLERANCIA MÍNIMA A LOS DEFECTOS DE *HARDWARE* DE LOS SENSORES Y ELEMENTOS FINALES Y DE LAS UNIDADES LÓGICAS DISTINTAS DE LAS PE. IEC 61511

SIL	Tolerancia mínima a los defectos del <i>hardware</i>
1	0
2	1
3	2
4	Se aplican requisitos especiales (véase la norma IEC 61508)

TABLA 4

FRACCIÓN DE FALLO SEGURO IEC 61508 TIPO A

Fracción de fallo seguro	Tolerancia a fallo del <i>hardware</i>		
	0	1	2
SFF < 60%	SIL 1	SIL 2	SIL 3
60% < SFF < 90%	SIL 2	SIL 3	SIL 4
90% < SFF < 99%	SIL 3	SIL 4	SIL 4
SFF > 99%	SIL 3	SIL 4	SIL 4

TABLA 5

FRACCIÓN DE FALLO SEGURO IEC 61508 TIPO B

Fracción de fallo seguro	Tolerancia a fallo del <i>hardware</i>		
	0	1	2
SFF < 60%	No permitido	SIL 1	SIL 2
60% < SFF < 90%	SIL 1	SIL 2	SIL 3
90% < SFF < 99%	SIL 2	SIL 3	SIL 4
SFF > 99%	SIL 3	SIL 4	SIL 4

Existen técnicas de cálculo de esta PFD como son: árboles de fallo (FTA), técnica RBD (diagramas de bloques de fiabilidad), modelos de Markov o mediante fórmulas basadas en simplificaciones algebraicas del modelo de Markov. Además, existe la posibilidad de calcularla mediante programas comerciales, que poseen amplias bases de datos de elementos que componen los sistemas instrumentados de seguridad.

Una vez calculada la PFD de cada elemento, mediante álgebra de Boole, se calcula la PFD global para el sistema instrumentado de seguridad, cerciorándonos de que cumple con el SIL establecido (Tabla 1).

Además de la PFD, influyen otros factores para verificar el diseño del SIS. Los estándares de seguridad funcional IEC 61508/61511 incorporan restricciones en la arquitectura del SIS. En dichos estándares vienen reflejados unos requisitos mínimos de tolerancia a los defectos del *hardware* de los elementos que conforman el SIS en función del índice SIL y la fracción de fallo seguro (SFF, *Safety Failure Fraction*), que es la proporción de la tasa de fallos aleatorios de *hardware* de un dispositivo que da lugar a un fallo seguro o a un fallo peligroso detectado. Esta relación se muestra en las Tablas 2, 3, 4 y 5, en función del tipo de elemento (sensor, lógica o actuador) y de la normativa que adoptemos (IEC 61518 o IEC 61511).

Según la IEC 61511, la tolerancia a los defectos del *hardware* se define como "...la capacidad de un componente para continuar siendo capaz de ejecutar la función instrumentada de seguridad requerida en presencia de uno o más defectos peligrosos en el *hardware*". Por ejemplo, una tolerancia a los defectos del *hardware* de 1 significa que hay dos dispositivos y la arquitectura es tal que el fallo peligroso de uno de

Figura 2
Independencia del SIS



los elementos no impide que se produzca la acción de seguridad.

A continuación se presenta un ejemplo para comprobar la aplicación de dichas restricciones. La PFD calculada para un sensor corresponde, según la Tabla 1, a un SIL 2. Ahora hay que verificar si tiene alguna restricción según las normativas IEC 61508/61511. Si la tolerancia a los defectos del *hardware* es cero (quiere decir que sólo disponemos de un elemento), y nos regimos por la norma IEC 61508, la fracción de fallo seguro debe de estar entre el 60 y 90%, si se trata de un dispositivo de tipo A (mecánico), o de entre el 90 y 99% si se trata de un dispositivo tipo B (electrónico), para que le corresponda un SIL 2.

Por ello, hay que verificar que los sistemas instrumentados de seguridad cumplen con las restricciones recogidas en las normativas. En caso de que no cumplan, debemos de modificar la arquitectura del SIS, utilizando elementos más fiables (con menores tasas de fallo o menores tiempo de reparación), elementos redundantes con lógica de votación NooM (1oo2, 2oo3, 1oo3...) para aumentar la tolerancia a fallo del *hardware*, etc.

Además de comprobar que los SIS cumplen con las normativas, existe otra característica muy importante a considerar, como es la independencia del sistemas instrumentado de seguridad con respecto al sistema de control básico de procesos (BPCS) (Fig. 2). Se debe considerar esta independencia como algo indispensable a la hora de configurar el SIS para evitar motivos de fallo de causa común.

Esta independencia se trata de forma diferente según la normativa o estándar que se esté aplicando. Así, si aplicamos la normativa ANSI/ISA S84, los criterios que exigen son los siguientes:

- Para sensores de campo con SIL 1, puede usarse el mismo sensor para el BPCS y el SIS, siempre que prevalezca éste último sobre el BPCS. Para elementos con SIL 2 o SIL 3, deben de ser completamente independientes.

- Para lógicas de actuación, si el SIL es 1, se puede usar la misma para el BPCS y el SIS. Para lógicas con SIL 2, también se puede usar la misma, pero siempre

EL OBJETIVO DE LA CERTIFICACIÓN PERSONAL ES ACREDITAR Y ESTABLECER LA COMPETENCIA DE AQUELLAS PERSONAS DEDICADAS A LA PRÁCTICA DE APLICACIONES DE LOS SISTEMAS DE SEGURIDAD EN LAS INDUSTRIAS DE PROCESOS

que prevalezca la función del SIS sobre la del BPCS. Para SIL 3, se requiere independencia completa.

- Para elementos finales con SIL 1 o SIL 2, se puede usar el mismo, siempre que prevalezca la acción del SIS sobre la del BPCS. En cambio, para SIL 3, se requiere que sean independientes.

En cambio, los estándares IEC 61508/61511 son más restrictivos en este aspecto. Exigen independencia total, salvo excepciones puntuales en las que se debe de justificar el por qué de esa dependencia. En esos casos se deberá de fundamentar y demostrar que no se compromete la integridad de las funciones de seguridad.

Todo esto nos muestra que la configuración de un SIS no sólo es elegir los elementos en función de su probabilidad de fallo en demanda, sino que debe de cerciorarse que cumplimos con las restricciones recogidas en las normativas IEC-61508 o IEC-61511. Un aspecto fundamental a la hora de elegir los elementos que van a formar parte del SIS es exigir el certificado de conformidad con respecto a dichas normativas.

A todo lo anterior hay que añadir que debe existir un personal adecuado con conocimientos suficientes para garantizar el cumplimiento de las normativas sobre seguridad funcional de los procesos. En este sentido, existen dos tipos de certificaciones:

- De personal (experto en seguridad funcional).
- De equipos o componentes (programas de certificación y manuales de seguridad).

El objetivo de la certificación personal es acreditar y establecer formalmente la competencia de aquellas personas dedicadas a la práctica de aplicaciones de los sistemas de seguridad en las industrias de procesos. En las certificaciones de equipos o componentes se especifican valores correspondientes a:

- SIL.
- Tolerancia a fallo del *hardware* (HFT).
- Fracción de fallo seguro (SFF).
- Probabilidad de fallo en demanda (PFD).
- La tasa de fallos peligrosos no detectados (λ_{nd}).
- La tasa de fallos peligrosos detectados (λ_{dd}).
- La tasa de fallos seguros no detectados (λ_{ns}).
- La tasa de fallos seguros detectados (λ_{sd}).

La certificación puede ser auditada por cuerpos notificados y autorizados, como el grupo TÜV Rheinland Europeo, autorizado a certificar Directivas de la Unión Europea (maquinarias, equipos de presión, etc.) o el *Nationally Recognized Test Laboratory* (NRTL), acreditado por la OSHA para certificar a la UL (primera organización de certificados de seguridad funcional de los EE.UU.) y otros estándares de los EE.UU. y otros estados canadienses.

Estos grupos realizan aprobaciones para asegurarse de que el producto incluye suficiente seguridad funcional según los niveles previstos de seguridad (SIL).

La emisión de un certificado SIL para un componente puede dar lugar a una percepción falsa de que comprar equipos con "certificados SIL" asegura la seguridad de la planta sin necesidad de mayores ni posteriores verificaciones.

De esta forma, aún disponiendo de los componentes o equipos con certificación SIL, puede ocurrir que el SIS no cumpla con el nivel SIL requerido. En todos los casos, la verificación de la PFD del sistema integrado y la arquitectura del sistema deberán ser comparadas con el nivel SIL requerido y con las restricciones establecidas en las normativas sobre seguridad funcional.

Con todo esto, una vez configurado y verificado el sistema instrumentado de seguridad, se procederá a cumplimentar el resto de las etapas del ciclo de vida.

3 CONCLUSIONES

La presencia de elementos que puedan constituir un riesgo de accidente en cualquier instalación industrial requiere la adopción de medidas de seguridad con criterios exigentes para, cuando se vulneren condiciones predeterminadas, poder llevar el proceso a un estado de seguridad tanto para las personas como para el medio ambiente o bienes materiales. Esto se traduce en la necesidad de implementar sistemas especiales, independientes de cualquier otro sistema, para que, en caso de fallo del resto de capas de prevención, pueda actuar y llevar el proceso a un estado seguro.

Por este motivo aparecen los sistemas instrumentados de seguridad (SIS) como última capa de prevención, con el objetivo de evitar situaciones de riesgo para los receptores vulnerables.

El diseño de estos sistemas requiere medidas especiales de configuración, como la independencia o la redundancia de los elementos, en función del SIL requerido, y se rigen con estrictos criterios recogidos en las diferentes normativas de seguridad funcional. Los estándares IEC 61508/61511 establecen restricciones en la arquitectura del SIS que hay que tener en cuenta a la hora del diseño y verificación para poder así cumplir con el SIL establecido.

Como conclusión final cabe destacar que, no sólo se trata de comprar elementos muy fiables con bajas tasas de probabilidad de fallo en demanda, sino que se deben comprobar las múltiples restricciones que nos imponen las normativas IEC-61508 o IEC-61511 para el adecuado cumplimiento de la arquitectura de los sistemas instrumentados de seguridad. ■