

Análisis del diseño y verificación de los sistemas instrumentados de seguridad

Por
Pilar Ojeda Rodríguez,
Victoriano Macías Jaén
y Miguel Ángel Muñoz Aguilar
 División de Seguridad
 Industrial
 Inerco

Introducción

Las instalaciones industriales en las que se almacenan, procesan y generan sustancias peligrosas, son susceptibles de inducir consecuencias adversas debido a los riesgos que ello implica sobre receptores vulnerables como son personas, bienes materiales y medio ambiente. Por ello se requiere la adopción de medidas extras de seguridad que nos brinden protección adicional, para llevar el proceso a su estado seguro.

Estos riesgos exigen que las plantas adopten estrictos criterios de seguridad tanto en el diseño de instalaciones y equipos, como en la adopción de medidas de seguridad, medidas que se traducen en múltiples capas de protección, que trabajan en conjunto, con el objetivo de prevenir los accidentes y/o mitigar las consecuencias derivadas de los mismos.

Dichas capas de protección se dividen, principalmente, en dos grandes grupos:

- Capas de prevención, cuyo objetivo es prevenir posibles accidentes derivados de los riesgos inherentes a las instalaciones, como el sistema de control básico de procesos (BPCS) o los sistemas instrumentados de seguridad (SIS).

- Capas de mitigación, que se instalan con el objetivo de mitigar las consecuencias derivadas de dichos accidentes como, por ejemplo, los sistemas

fuego-gas, la respuesta de planta ante una emergencia o la respuesta de la población ante una emergencia.

Existen un gran número de técnicas de análisis de riesgos que se pueden utilizar para realizar la elección más adecuada de las capas de protección a utilizar para cada situación específica. De entre estas técnicas, las más empleadas son: bases de datos o análisis históricos de accidentes, análisis preliminar de riesgos, análisis *what-if*, listas de chequeo o *check-list*, análisis de modos de fallos y efectos (FMEA), estudios de riesgos y operabilidad (HAZOP), análisis mediante árboles de fallos (FTA), análisis mediante árboles de sucesos o análisis de causa-consecuencia. De entre todos ellos cabe destacar la metodología HAZOP como una de las más representativas, debido a su análisis estructurado y exhaustivo que suele constituir la última verificación de las condiciones de diseño, adecuación del proceso y materiales de la instalación previamente a su construcción.

Índice SIL (Safety Integrity Level)

Los sistemas instrumentados de seguridad (SIS) son los encargados de,

una vez vulneradas las condiciones de operación seguras, llevar el proceso a lugar seguro. Dichos sistemas suelen estar constituidos, básicamente, por tres elementos (en la figura 1 se muestra una posible configuración de estos SIS):

- Elemento sensor o grupo de sensores.
- Convertidor lógico.
- Actuador o elementos finales.

Estos tres elementos funcionan en conjunto y actúan como última medida de prevención antes de que se produzca alguna situación de peligro.

Para una mejor comprensión se va a analizar el fallo del lazo de control de nivel en un botellón de proceso. En la figura 2 se muestra la evolución normal de un suceso accidental, teniendo en cuenta las diferentes medidas de protección existentes.

Dicho control realizaría su función manteniendo el parámetro a controlar dentro de un rango normal de operación. Si este sistema fallara se activaría la alarma por alto nivel y se procedería a tomar las respectivas medidas por parte del operador para llevar el proceso de nuevo a su rango de operación normal. Si la alarma no se activara o el operador no llevara a cabo su función se produciría una nueva situación de peligro, don-



Arquitectura de un sistema instrumentado de seguridad

de no se dispone de más capas de prevención para evitar el posible accidente. Es ahí donde actuaría el sistema instrumentado de seguridad, siendo la última capa de prevención, antes de que se produzca una situación de peligro, en la que sólo nos quedarían medidas de mitigación para salvaguardar la seguridad de los receptores vulnerables.

Esta exigencia se traduce en unos niveles de seguridad, denominados niveles íntegros de seguridad (índice SIL, *Safety Integrity Level*) específicos que van desde 1 hasta 4 (tabla 1). En las normativas específicas sobre seguridad funcional existe una relación entre estos índices SIL, la probabilidad de fallo en demanda del sistema instrumentado (PFD) y el factor de reducción de riesgo (RRF). De esta manera se consigue reducir el riesgo a un nivel tolerable definido para cada instalación.

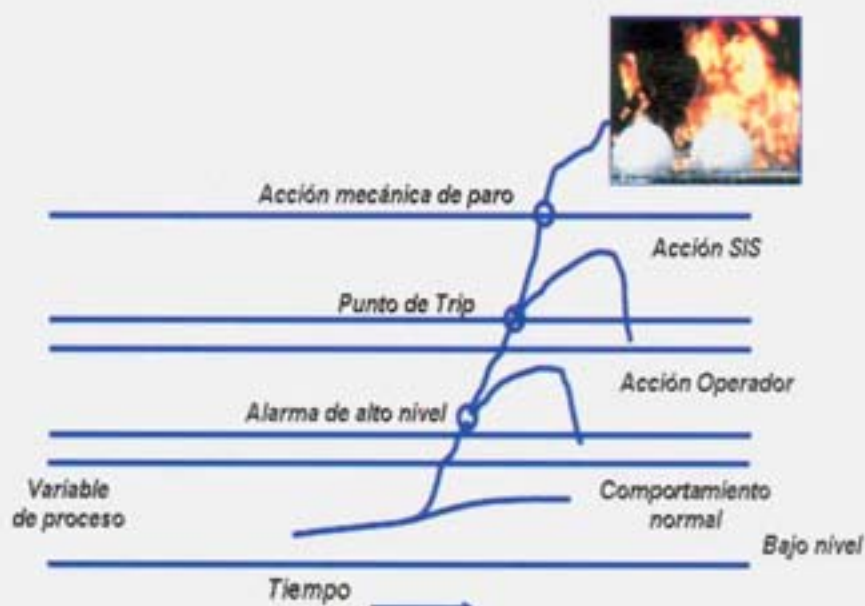
Normativas y estándares

En la actualidad existen multitud de estándares relacionados con la seguridad funcional. Los más utilizados en materia de sistemas instrumentados de seguridad, son:

1 ANSIIISA-S84.01-1996: "Application of safety instrumented systems for the process industries"

Es una norma del *American National Standards Institute* en la que se establece una base para el diseño de SIS en la industria de proceso, incluyendo tecnología eléctrica, electrónica y electrónica programable. Establece, asimismo, cuáles son los pasos en el ciclo de vida de un SIS desde su concepción inicial hasta el desmontaje del mismo. Está dirigida fundamentalmente al personal que participa en el desarrollo y fabricación de los SIS, en la instalación, en el comisionado y en las restantes fases del ciclo.

2 IEC 61508: "Functional safety of electrical/electronic/programmable electronic safety related systems"



Capas de protección instrumentadas en el control de una variable de proceso

Es un estándar de la *International Electrotechnical Commission* en el que se establece una base para el uso de dispositivos eléctricos y/o electrónicos programables en el diseño de SIS en aplicaciones médicas, de transporte, en industria de proceso, etc. Establece, asimismo, cuáles son los pasos en el ciclo de vida de un SIS desde su concepción inicial hasta el desmontaje del mismo. Está dirigida al personal involucrado en cualquier fase del proyecto desde el concepto hasta la explotación.

Se encuentra publicada la correspondiente norma europea UNE-EN 61508 equivalente a este estándar.

3 IEC 61511: "Functional Safety of electrical/electronic/programmable electronic safety related systems for the process industry sector"

Es un estándar de la *International Electrotechnical Commission* en el que se establece una base para el uso de dispositivos eléctricos y/o electrónicos programables en el diseño de SIS en la industria de proceso. Establece, asimismo, cuáles son los pasos en el ciclo de vida de un SIS desde su concepción inicial hasta el desmontaje del mismo. Está dirigida fundamentalmente al usuario final de los

sistemas de seguridad y constituye la aplicación del estándar IEC 61508 a la industria de procesos.

Se encuentra publicada la correspondiente norma europea UNE-EN 61511 equivalente a este estándar.

Ciclo de vida de un sistema instrumentado de seguridad. Diseño y verificación del SIS

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 (p.e., 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.

Una vez definido el listado de SIS y calculado el SIL correspondiente a

cada uno de ellos se debe verificar que su diseño, configuración, arquitectura e instalación está conforme con este SIL establecido, para cumplir con los requisitos de seguridad funcional.

Esto se consigue mediante el cálculo de la probabilidad de fallo en demanda (PFD) del sistema instrumentado de seguridad. Para ello, se calcula la PFD para cada elemento (sensores, lógica y actuadores) que forma parte del SIS y, mediante álgebra de Boole, se calcula la PFD del sistema global, para la arquitectura elegida. A esta PFD le correspondería un SIL determinado (tabla 1), que debe coincidir con el SIL establecido en la etapa previa de cálculo del mismo.

El cálculo de la PFD de cada elemento del SIS depende de una serie de factores:

- Tasa de fallos (λ), es el número de fallo 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.

Existen multitud de métodos de cálculo para hallar la PFD de cada elemento como, por ejemplo, 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 existen programas de cálculo comerciales que disponen de bases de datos de diferentes clases de elementos para poder verificar su diseño.

En la configuración de la arquitectura del SIS se debe tener en cuenta que su objetivo principal es llevar el proceso a un estado seguro cuando se vulneran unas condiciones predeterminadas. Por ello, un elemento im-

Tabla 1. Relación índices SIL con PFD y el RFF

NIVEL DE INTEGRIDAD DE SEGURIDAD (SIL)	PROBABILIDAD DE FALLO MEDIA OBJETIVO DE FALLO BAJO DEMANDA	FACTOR DE REDUCCIÓN DE RIESGO (RRF)
4 ¹	$\geq 10^{-5}$ A $<10^{-4}$	$>10\ 000$ A $\leq 100\ 000$
3	$\geq 10^{-4}$ A $<10^{-3}$	$>1\ 000$ A $\leq 10\ 000$
2	$\geq 10^{-3}$ A $<10^{-2}$	>100 A $\leq 1\ 000$
1	$\geq 10^{-2}$ A $<10^{-1}$	>10 A ≤ 100

¹ El índice SIL 4 sólo se contempla en los estándares IEC 61508/61511, pero no en el estándar ANSI/ISA-84

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 HARDWARE		
	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 HARDWARE		
	SFF < 60%	SFF 60% A 90 %	SFF > 90%
1	0	0	0
2	1	1	0
3	2	2	1
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 HARDWARE		
	0	1	2
SFF < 60%	SIL 1	SIL 2	SIL 3
60% \leq SFF \leq 90%	SIL 2	SIL 3	SIL 4
90% \leq SFF \leq 99%	SIL 3	SIL 4	SIL 4
SFF \geq 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 HARDWARE		
	0	1	2
SFF < 60%	NO PERMITIDO	SIL 1	SIL 2
60% \leq SFF \leq 90%	SIL 1	SIL 2	SIL 3
90% \leq SFF \leq 99%	SIL 2	SIL 3	SIL 4
SFF \geq 99%	SIL 3	SIL 4	SIL 4

portante es la independencia de este sistema con cualquier otra capa de protección que impida su funcionamiento o que pueda provocar el fallo de éste, reduciendo así la probabilidad de que el sistema de control y las funciones de seguridad no estén disponibles al mismo tiempo.

En este aspecto, las normativas IEC 61508/615011 son muy exigentes y sólo permiten en casos especiales la dependencia del sistema instrumentado de seguridad con el sistema de control básico de proceso, BPCS. En estos casos se debe fundamentar y demostrar que no se compromete la integridad de las funciones de seguridad.

En cambio, la normativa ANSI/ISA-S84, es menos restrictiva en este aspecto:

- 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 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.

Además de la independencia del sistema instrumentado de seguridad con otras capas de protección, si nos regimos por los estándares IEC 61508/61511, éstos establecen 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 peligro 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).

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

Así, si en el desarrollo de la arquitectura de un SIS hemos elegido un elemento sensor para configurar un SIL 2 y optamos por basarnos en la normativa IEC-61511, necesitaríamos utilizar una tolerancia mínima a los defectos del hardware de 1, por lo que nos llevaría a una votación de 1oo2, 2oo3, etc... Por tanto, la conclusión es que con un único sensor no alcanzaríamos el objetivo buscado de SIL 2. En el caso de que optemos por guiarnos por la normativa IEC-61508 y nuestro sensor sea, por ejemplo, mecánico de tipo A, debemos de comprobar que rango de SFF posee para clasificar su nivel SIL. Ello nos puede conducir a que si su SFF está comprendida entre el 60 por 100 y 90 por 100 con un único sensor se podría alcanzar el nivel de seguridad de SIL 2.

Todo esto nos muestra que la configuración de SIS no sólo es elegir los elementos en función de su probabilidad de fallo en demanda, sino que debemos de cerciorarnos que cumplimos con las restricciones recogidas en las normativas IEC-61508 o IEC-61511. A la hora de elegir los elementos que van a formar parte del SIS debemos de exigir al fabricante el certificado de conformidad con

respecto a las normativas IEC-61508 e IEC-61511.

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 de este sistema.

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 debemos 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. ■