



## CICLO DE VIDA DE LOS SIS EN INSTALACIONES DE PROCESO

*Los SIS o sistemas instrumentados de seguridad representan un avance en materia de seguridad funcional de las instalaciones donde se manejan sustancias peligrosas. Forman parte de las denominadas capas de protección que se implantan en las instalaciones, y más concretamente, de las denominadas capas de prevención. Con el presente artículo, esta revista se ocupa nuevamente de este tema, tan importante en el control de la seguridad de las plantas de proceso, en el que la autora analiza las etapas fundamentales que se deben cubrir en el ciclo de vida de estos sistemas.*

**LAS INSTALACIONES INDUSTRIALES** de proceso que almacenan, procesan y generan sustancias peligrosas, tienen asociado un determinado nivel de riesgo sobre las personas, sobre los bienes materiales y sobre el medio ambiente.

Dichos riesgos potenciales exigen que estas plantas adopten estrictos criterios tanto en el diseño de las instalaciones y equipos, como en la adopción de medidas de seguridad. Éstas últimas se traducen en las múltiples capas de protección existentes en las instalaciones.

Cada capa de protección está compuesta de equipos y/o procedimientos de control que actúan conjuntamente con otras capas de protección para controlar y/o mitigar los riesgos de los procesos (Figura 1).

**Figura 1**  
Definición de riesgo y ejemplos de unidades de riesgo

<b>RIESGO</b>	=	<b>FRECUENCIA</b>	×	<b>SEVERIDAD DE LAS CONSECUENCIAS</b>
N° muertes/año € pérdidas/mes Kg sustancia fugada/hora Alto/Medio/Bajo		Año <sup>-1</sup> Mes <sup>-1</sup> Hora <sup>-1</sup> Alto/Medio/Bajo		N° muertes Pérdida económica (€) Kg de sustancia fugada Accidente categoría 1/2/3

# 1

## LAS CAPAS DE PROTECCIÓN

Las capas de protección (Figura 2) se pueden dividir en:

- Capas de prevención: Son aquellas que tienen el propósito de detectar y evitar los sucesos que dan lugar al accidente, o lo que es lo mismo, son las que han de actuar antes de la pérdida de contención de materia o energía (reducen el riesgo disminuyendo la frecuencia del accidente). Las más comunes son:

- El sistema básico de control de procesos (basic process control system - BPCS).
- Las alarmas críticas e intervención humana.
- Los sistemas instrumentados de seguridad (SIS).
- La protección física ante sobrepresiones o vacío: válvulas de seguridad (*pressure safety valves* - PSV), discos de ruptura (*rupture disk* - RD) y válvulas rompedoras de vacío.

- Capas de mitigación: Son aquellas diseñadas para minimizar la severidad de las consecuencias del accidente, es decir, han de actuar después de la pérdida de contención de materia o energía (reducen el riesgo disminuyendo las consecuencias del accidente). Dentro de éstas se incluyen entre otras:

- Protección física (pasiva): cubeto, aislamiento ignífugo, paredes anti-explosiones/búnker.
- Sistemas instrumentados de mitigación: sistemas fire & gas, sistemas de paro de emergencia, válvulas de aislamiento de accionamiento remoto manual, sistemas de aislamientos de deflagraciones, etc.
- Respuesta de la planta ante emergencia.
- Respuesta de la comunidad ante emergencia.

Un sistema instrumentado de seguridad (Figura 3) es un sistema compuesto por sensor, convertidor lógico y elementos de control finales o actuadores con objeto de llevar el proceso a un estado seguro cuando se vulneran unas condiciones predeterminadas.

Dado que los sistemas instrumentados de seguridad constituyen una medida de seguridad o capa de pro-

**Figura 2**  
Capas de protección en instalaciones de proceso "figura de la cebolla"



## Arquitectura de los SIS



tección que debe actuar en caso de fallo del control de proceso y de una actuación incorrecta por parte del operador, dichos sistemas deben disponer de unas condiciones de seguridad y fiabilidad suficiente que garanticen su correcto funcionamiento cuando se les demanden. El análisis SIL permitirá evaluar cuál es el nivel de seguridad, mediante el cálculo del índice SIL (safety integrity level) o nivel íntegro de seguridad exigible a estos sistemas, así como verificar que éstos están conformes a dicho nivel.

Por otro lado, una función instrumentada de seguridad se define como una función, a ser implementada por un SIS, la cual tiene por finalidad el lograr o mantener el proceso en un estado seguro frente a un elemento peligroso específico.

## 2

### ETAPAS EN EL CICLO DE VIDA DE LOS SIS

Las normativas y estándares sobre seguridad funcional ANSI-ISA-S84 e IEC-61511/61508 establecen las distintas etapas a cubrir en el ciclo de vida de seguridad de un sistema instrumentado de seguridad, desde la concepción inicial del mismo hasta su desmontaje. Las distintas etapas a considerar se esquematizan en la Figura 4 y son las siguientes:

- Diseño conceptual del proceso. Desarrollo de ingeniería básica y de detalle.
- 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.

A continuación, se describen cinco fases fundamentales a cubrir dentro del ciclo de vida de los sistemas instrumentados de seguridad.

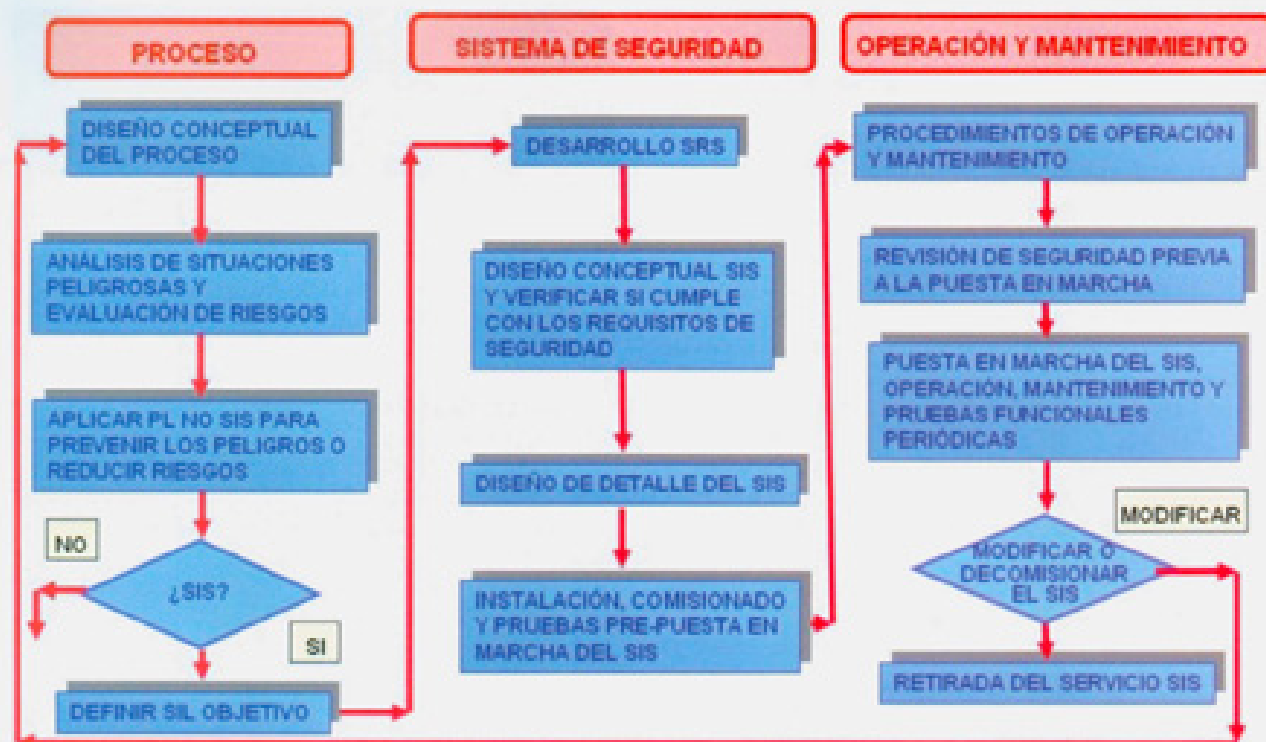
### 2.1

#### Análisis de riesgos de los procesos

Las medidas de seguridad más adecuadas a adoptar en las instalaciones se derivarán de la elaboración de un análisis de riesgos específico en las mismas, mediante la aplicación de una o varias técnicas de identificación de riesgos.

Existe una gran variedad de técnicas de identificación de riesgos, tales como bases de datos de accidentes,

Figura 4  
Ciclo de vida de un sistema Instrumentado de seguridad



análisis de peligros y operatividad (HAZOP), análisis what if?, listas de chequeo, análisis de los modos de fallo, efectos y consecuencias (FCMEA), análisis mediante árboles de fallo y árboles de suceso, etc. La técnica de identificación seleccionada dependerá de los propósitos perseguidos con la identificación de riesgos, así como de los datos y recursos disponibles.

En este sentido, la metodología HAZOP es a día de hoy la más comúnmente aceptada y está recomendada por las normativas sobre seguridad funcional. Se presenta como una de las técnicas más rigurosas y estructuradas para la identificación de los peligros asociados a una planta de proceso. La aplicación principal de esta técnica se encuentra en la identificación de riesgos en las primeras etapas del diseño, al ser el mejor momento para introducir cambios o modificaciones, dado que los resultados son recomendaciones de mejora que modificarán el diseño final de los equipos o sistemas.

## 2.2

### Cálculo o definición del índice SIL objetivo

Dentro de las etapas del ciclo de vida, debe realizarse la asignación o definición del índice SIL para todas las funciones instrumentadas de seguridad de las instalaciones, considerando no sólo las definidas en la ingeniería básica y de detalle, sino también las que se introducen nuevas como consecuencia del estudio HAZOP desarrollado para las instalaciones en cuestión.

De acuerdo a las citadas normativas, existen varias metodologías para la elaboración y desarrollo de análisis SIL, que pueden ser de carácter cualitativo, semicualitativo, semicuantitativo o cuantitativo:

- Cualitativas
  - Gráfico de riesgo.

- Semicualitativas

- Gráfico de riesgo calibrado.
- Matrices de riesgo.

- Semicuantitativas

- Análisis LOPA o análisis de las capas de protección.

- Cuantitativas

- Análisis de Markov.
- Análisis cuantitativo de riesgos (ACR).

## 2.3

### Diseño conceptual del SIS en función del SIL calculado

Una vez asignado o calculado el índice SIL para los sistemas instrumentados de seguridad, debe verificarse que el diseño de los mismos se adapta al nivel de seguridad establecido, de acuerdo a los requerimientos de las normativas sobre seguridad funcional.

En las normativas específicas sobre seguridad funcional existe una relación entre estos índices SIL, la probabilidad de fallo en demanda (PFD) y el factor de reducción de riesgo (RRF) del sistema instrumentado. En este sentido, los distintos componentes del SIS (sensor, lógica y actuador) deben tener una PFD tal que la PFD del sistema global sea inferior a la recogida en la Tabla 1, obteniéndose de esta forma reducir el riesgo a un nivel tolerable definido para cada instalación.

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

- Tasa de fallos ( $\lambda$ ): 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.

TABLA 1

## RELACIÓN DE LOS ÍNDICES SIL CON LA 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 <sup>1</sup>	$\geq 10^{-5}$ 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 $\leq 100$

<sup>1</sup> El índice SIL 4 sólo se contempla en los estándares IEC 61508/61511, pero no en el estándar ANSI/ISA-S84

- 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 importante 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.

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 de 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).

En definitiva, a la hora de instalar el sistema instrumentado de seguridad se debe verificar que los elementos reales instalados en el proceso cumplen con las especificaciones de seguridad requeridas y el SIL calculado en la etapa de determinación del índice SIL.

## 2.4

### Desarrollo y requerimientos de seguridad (SRS)

En este paso se debe desarrollar la especificación de los requerimientos de seguridad, esencialmente la filosofía

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
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 hardware		
	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 hardware		
	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

de operación del sistema. Cada función de seguridad debe tener un requerimiento de SIL asociado y requerimientos de confiabilidad para disparos en falso. Se deben incluir todas las condiciones de operación del proceso, desde el arranque hasta el paro, incluyendo el mantenimiento para cada modo de operación del proceso.

Los requerimientos del SIS deben ser expresados y estructurados, de tal modo que sean claros, precisos, verificables, sostenibles, factibles y escritos de modo que puedan ser comprendidos y aplicados. La especi-

cación de los requerimientos de diseño para el SIS debe incluir:

- La función del sistema o componente del sistema.
- Acciones que el sistema o componente debe realizar bajo circunstancias establecidas (especificación funcional).
- Integridad requerida (confiabilidad y disponibilidad) para operar en dichas circunstancias (especificación de integridad).

La información requerida para el desarrollo de la especificación de los requerimientos de seguridad, debe incluir:

- Lista de las funciones instrumentadas de seguridad requeridas y el SIL de cada función de seguridad.
- Diagramas de proceso e instrumentación, hojas de datos de proceso.
- Información del proceso (filosofía de operación, elementos finales, entre otros) e información del análisis de riesgo (causa y secuencia de cada evento potencial de peligro que requiera un SIS).
- Consideraciones de fallos de causa común del proceso, tales como corrosión, taponamiento, etc.
- Requerimientos regulatorios que aplican al SIS.
- Consideraciones de confiabilidad, calidad y ambientales.
- Lista de consideraciones operacionales y de mantenimiento.

Los requerimientos y desarrollos de seguridad se dividen en:

- Requerimientos generales.
- Especificación funcional.
- Especificación de integridad.

La especificación constituye la guía para definir los requerimientos de diseño, razón por la cual se debe incluir toda la información requerida como un paquete completo. Además de la información requerida y citada con anterioridad, debe incluirse para integrar el paquete de documentos de la especificación funcional y de integridad:

- Los diagramas o matrices causa-efecto, o
- Los diagramas lógicos.

## 2.5

### Procedimientos de operación y mantenimiento para pruebas funcionales

La realización de pruebas funcionales de operación y mantenimientos al SIS constituye otro paso fundamental e imprescindible en todas aquellas instalaciones que contengan un sistema instrumentado de seguridad.

Cuando el sistema instrumentado de seguridad entra en servicio es necesario asegurar que el SIL requerido para cada función instrumentada se mantenga durante la operación de la planta.

Los sistemas instrumentados de seguridad compuestos por un conjunto de funciones instrumentadas de seguridad no son sistemas en demanda continua. La función de cada SIF es actuar en caso de aparecer el evento potencialmente inseguro para el que fue diseñada, con el fin de evitar las consecuencias que podían derivarse del mismo. Esta característica hace imprescindible un seguimiento de los componentes que constituyen cada función instrumentada.

Las pruebas pueden llevarse a cabo con el proceso en operación (pruebas *on-line*) o con el proceso en parada (*off-line*), dependiendo de múltiples factores, como: las características del proceso, las sustancias presentes, los riesgos asociados al proceso, los elementos redundantes, el tiempo de parada de planta o la presencia de bypass.

Cada función instrumentada de seguridad presenta características totalmente distintas al resto de funciones que componen el SIS. Por ello, las pruebas deben individualizarse para cada una de ellas. Los procedimientos deberán recoger paso a paso las acciones a seguir y la responsabilidad del personal encargado para las mismas. De modo que deben comprobarse los elementos iniciadores, el PLC, los elementos finales y las alarmas asociadas.

## 3

### CONCLUSIONES

Los riesgos originados por el manejo, transporte, utilización y manipulación de sustancias consideradas peligrosas, conlleva la utilización de un mayor avance en dispositivos de seguridad que eviten los posibles peligros derivados de un mal funcionamiento de dichos dispositivos. Es por eso por lo que en materia de seguridad funcional se intenta mejorar y avanzar con los denominados sistemas instrumentados de seguridad (SIS). La seguridad funcional persigue que los SIS operen correctamente y que, por tanto, sean altamente confiables.

La implementación de estos sistemas instrumentados de seguridad en instalaciones de proceso, así como el desarrollo de un análisis SIL que garantice la correcta instalación y gestión de dichos sistemas, permite al industrial obtener los siguientes beneficios o ventajas:

- Adecuarse a las recomendaciones del seguro, obteniéndose de esta forma una disminución de las primas en la contratación de pólizas de seguros.
- Cumplir requisitos de la licenciataria del proceso con objeto de no perder garantías y mantener las condiciones de seguridad del proceso.
- Adaptarse a las normativas sobre seguridad funcional, Normas ANSI-ISA84 e IEC-61511/61508, que constituyen una guía de buenas prácticas de ingeniería para el diseño conceptual de los sistemas instrumentados con criterios de seguridad.
- Incrementar la seguridad de las instalaciones mediante la implementación de medidas de prevención con fiabilidad demostrada.
- Verificar los niveles de seguridad de las distintas capas de protección (prevención y mitigación) para cumplir con los criterios de aceptabilidad del riesgo establecidos por la corporación.
- Diseñar un ciclo de vida para todas las funciones de seguridad instrumentadas que permita cubrir todas las etapas desde la concepción inicial del sistema hasta el posible desmontaje del mismo.
- Diseñar e implantar un plan de mantenimiento y prueba de los SIS con criterios de seguridad.
- Adquirir los distintos elementos del SIS con especificaciones de seguridad y fiabilidad.
- Disminución de pérdidas financieras, por costes materiales propios, lucro cesante y responsabilidad civil derivados de accidentes graves en las instalaciones. ■