

Sistemas instrumentados de seguridad

Fiabilidad a través de la seguridad funcional (SIL: Safety Integrity Level). Normas IEC 61508 / IEC 61511

Oliver Reher

Product Manager de Caudal y responsable implementación SIL & ATEX en E+H

En un gran número de procesos industriales el hecho de transformar materias primas o de utilizar equipos aporta cierto peligro. Las nuevas tendencias nos exigen garantizar un menor impacto en el entorno, eliminando aquellos peligros asociados a una actividad productiva.

La fiabilidad de los componentes individuales de un sistema es el principal factor relacionado con posibles funcionamientos defectuosos del dispositivo. Los procesos no se pueden controlar de manera correcta a menos que los componentes individuales definitivos presenten un funcionamiento fiable. El **Nivel de Integridad de Seguridad (SIL)** es un método de evaluación de la fiabilidad de cada uno de los componentes del proceso.

Una función de seguridad tiene el objetivo de prevenir, evitar y tratar situaciones peligrosas, en el fondo, reducir el riesgo manteniendo el proceso en un estado seguro.

La función instrumentada de seguridad es la función que, utilizando un nivel de integridad SIL, tiene la capacidad de efectuar una función de seguridad.

Un sistema instrumentado de seguridad es un conjunto de partes de diferentes características que permite instrumentar un lazo de control de forma automática y que, en caso de fallo, realice la función de seguridad requerida bajo todas las circunstancias establecidas y durante el periodo de tiempo especificado (Figura 1).

El objetivo final es eliminar el riesgo. Lograr un estado de absoluta seguridad es imposible: lo único que podemos hacer es reducir el riesgo hasta un nivel tolerable.

Cuando hablamos de la SIL debemos hacer mención a dos norma: IEC 61508, relacionada con el suministrador o fabricante, y la IEC 61511, relacionada con la seguridad de planta.

En esta última el responsable de seguridad se encargará de la gestión del ciclo de vida de la SIL, evaluación de riesgos, de-

finición de los requisitos de seguridad, medidas de protección, definición de las responsabilidades y competencias (Figura 2).

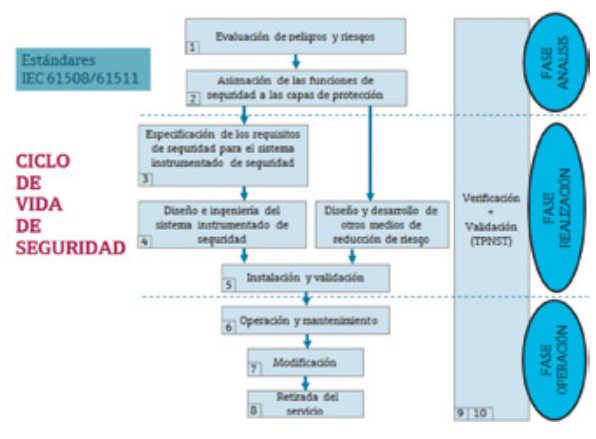
El ciclo de vida de la seguridad sigue unas fases lógicas y cronológicas, que empiezan por un análisis de riesgo deta-

Figura 1. Sistema Instrumentado de Seguridad (SIS)

- Un Sistema Instrumentado de Seguridad implementa una o más funciones de seguridad. Un SIS está compuesto por una combinación de: sensor(s), lógica, y elemento final



Figura 2. Ciclo de vida de seguridad



llado, donde se evalúan los diferentes riesgos como conjunto y se le asignan las funciones de seguridad necesarias para cada riesgo observado y analizado.

Seguidamente, se deben especificar los requisitos de seguridad y se deben diseñar los sistemas de seguridad, teniendo en cuenta tanto los sistemas instrumentados de seguridad, que son los que hacen referencia al SIL, como los sistemas de seguridad de otros medios, ya sean físicos, protocolos de actuación o protocolos de vigilancia. Una vez definidos y diseñados los sistemas instrumentados de seguridad, es preciso realizar la integración al sistema actual, y se debe pasar una verificación y una validación. Esta validación debe ser realizada por un organismo neutro e independiente, denominada "Tercera Parte Neutra", y debe validar el nivel de SIL de la parte hardware y la parte software de las funciones de seguridad, desde el análisis de riesgos hasta la integración de los SIS. Una vez operado, es preciso mantener el nivel de fiabilidad adquirido, mediante lo que se llama *Proof Test* o ensayo de la función de seguridad. La frecuencia de ensayos se debe determinar en el diseño de los SIS.

Pasamos a la siguiente fase, que significa que, en caso de modificación de cualquier parámetro inicial, deberemos realizar el ciclo completo del análisis de riesgos para verificar que sigue en vigor lo establecido o se debe modificar alguna de las cadenas de seguridad.

Al final del ciclo de vida de la seguridad se procede a la retirada de los sistemas establecidos.

Cualquier equipo de instrumentación considerado como crítico en el lazo de control debe ser verificado. Muchos fabricantes utilizan consolas externas para verificar el buen funcionamiento de los equipos en proceso, pero una tendencia al alza es que **el propio instrumento de medida se autoverifique**, generando a la vez un informe de esta verificación. Las principales ventajas de una autoverificación son:

- **Aumento de seguridad:** en ningún momento se pierde la señal proceso, incluso durante el periodo de autoverificación, ya que existe una multiplexación interna que permite realizar ambos procesos en el propio caudalímetro.
- **Mayor disponibilidad del punto de medida:** la autoverificación puede realizarse con el indicador local de campo, o bien remotamente a través de la comunicación HART.
- **Rapidez en la autoverificación:** un caudalímetro Coriolis puede tardar menos de cinco minutos en autoverificarse antes de un proceso discontinuo para poder garantizar la trazabilidad de la producción (Figura 3).

Como hemos descrito anteriormente, la adopción la seguridad funcional en la instrumentación de campo ha ayudado en el desarrollo de herramientas que hacen que estos instrumentos sean más seguros y fiables.

Figura 3. Ejemplo de informe de una autoverificación en un caudalímetro máscico Coriolis

