Una descripción general de la seguridad funcional en la industria de procesos

Este libro blancos explora varios estándares, definiciones y productos que pueden ayudarle a lograr una mayor seguridad funcional en las aplicaciones de procesos.

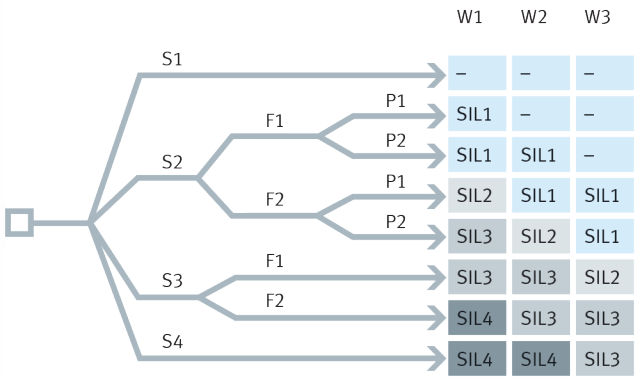
La implementación de la seguridad funcional es fundamental en las industrias de procesos, que incluyen aplicaciones químicas, petroleras y petroquímicas peligrosas. Los sistemas en estas industrias, hasta el nivel práctico más bajo, deben diseñarse para reducir los peligros contra las personas, la propiedad y el medio ambiente, especialmente en caso de mal funcionamiento o falla. Para explorar más este tema, este documento le proporciona una descripción general útil de lo siguiente:

- Niveles de Integridad de Seguridad (SIL, por sus siglas en inglés), incluyendo cómo asignar un nivel a su sistema.
- Los estándares, definiciones y valores característicos para el cálculo de SIL.
- Los diversos productos, incluyendo las válvulas a prueba de fallas y las arquitecturas redundantes, que pueden ayudarle a implementar la seguridad funcional de una manera fácil y rentable.

Cómo determinar y asignar SIL

Una métrica importante para la industria de procesos, SIL mide el nivel de seguridad o riesgo esperado para un sistema en términos de PFD, o la probabilidad de falla bajo demanda. Hay cuatro niveles distintos, donde SIL1 representa el riesgo más bajo y SIL4 representa el riesgo más alto aceptable. En general, a medida que aumentan los niveles, también aumenta el nivel de seguridad asociado. Al mismo tiempo, la probabilidad de que el sistema no funcione correctamente es menor. Por lo general, la complejidad del sistema y los costos de instalación y mantenimiento también aumentan con los niveles. Una vez que un nivel se ha asignado a un sistema, se deben observar principios de instalación específicos, como el diseño de circuitos redundantes, para minimizar los riesgos de seguridad en caso de un mal funcionamiento.

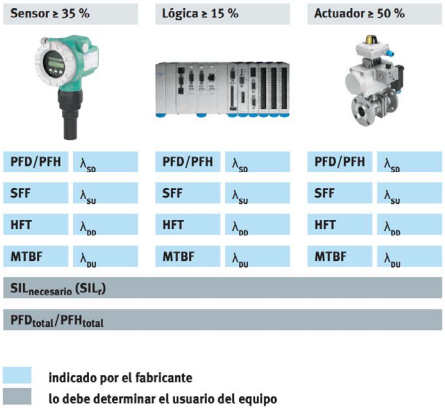
SIL (Safety Integrity Level, nivel de integridad de seguridad)



S	Grado del daño	
	S1	Lesiones leves de una persona
	S2	Lesiones graves de varias personas, incluida la muerte de una persona
	S3	Muerte de varias personas
	S4	Consecuencias catastróficas con numerosos muertos
F	Frecuencia y tiempo de exposición	
	F1	Poco frecuente hasta ligeramente frecuente
	F2	Frecuente hasta permanente
P	Protección/prevención contra riesgos	
	P1	Posible en determinadas condiciones
	P2	Raramente posible
W	Probabilidad del peligro	
	W1	Relativamente alta
	W2	Baja
	W3	Muy baja

Además del PFD, el cálculo del SIL depende de varios valores característicos, como la probabilidad de falla por hora (PFH, por sus siglas en inglés) o la probabilidad de que una función de seguridad falle durante el uso continuo. Otros valores importantes incluyen:

- **Fracción de falla segura (SFF, por sus siglas en inglés):** la proporción de fallas seguras respecto al toral de fallas.
- **Tiempo medio entre fallas (MTBF, por sus siglas en inglés):** el tiempo medio entre dos fallos sucesivos.
- **Tolerancia a fallas de hardware (HFT, por sus siglas en inglés):** la capacidad de un sistema para continuar ejecutando la función requerida en caso de fallas o desviaciones. Para HFT0, una sola falla puede eliminar la función de seguridad. Para HFT1, deben ocurrir al menos dos fallas simultáneamente para eliminar la función de seguridad. Y para HFT2, deben ocurrir al menos tres fallas simultáneamente para eliminar la función de seguridad.
- **Tipos de dispositivo A y B:** el tipo A significa que podemos determinar adecuadamente el comportamiento de falla y las características de todos los componentes del sistema. El tipo B significa que no podemos determinar el comportamiento de falla de al menos un componente del sistema.
- **Tasa de falla (λ):** la tasa de falla es la variable que determina la confiabilidad de un componente. Hay muchos tipos, entre otros:
    - Fallas seguras, o λ_S
    - Fallas identificables seguras, o λ_{SD}
    - Fallas seguras no identificables, o λ_{SU}
    - Fallas peligrosas, o λ_D
    - Fallas identificables peligrosas, o λ_{DD}
    - Fallas peligrosas no identificables, o λ_{DU}



Distribución típica del PFD/PFH entre los subsistemas de una función de seguridad en sistemas monocanal.

Estándares de seguridad funcional para aplicaciones de proceso

El estándar básico para la seguridad funcional es IEC 61508, que abarca los sistemas eléctricos, electrónicos y electrónicos programables relacionados con la seguridad. También describe los métodos para evaluar los riesgos de seguridad utilizando un gráfico de riesgo, así como el diseño de funciones de seguridad adecuadas para sensores, circuitos lógicos, actuadores y otros dispositivos. Tenga en cuenta que los requisitos de IEC 61508 solo se aplican a los Sistemas Instrumentados de Seguridad (SIS, por sus siglas en inglés) completos y no a los componentes individuales. Un SIS generalmente consta de lo siguiente:

- Sensores, por ejemplo, sensores de presión y temperatura, así como medidores de nivel de llenado;
- Unidades de evaluación y salida como Controladores Lógicos Programables (PLC) de seguridad;
- Válvulas de proceso automatizadas, que comprenden la válvula solenoide, el actuador y la válvula de proceso.

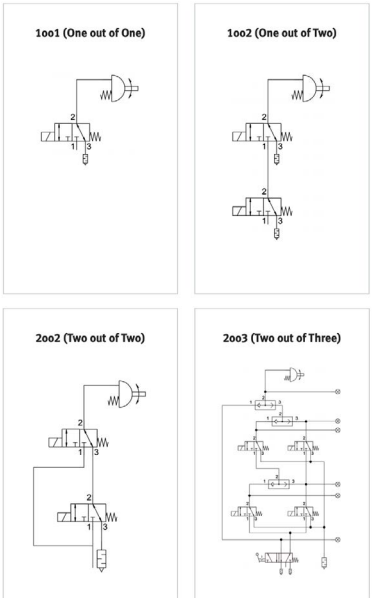
El estándar IEC 61511 describe cómo implementar IEC 61508 para la industria de procesos con un enfoque en aplicaciones con un modo de baja demanda. A diferencia de las funciones de seguridad de alta demanda, que se espera que ocurran más de una vez al año, las funciones de baja demanda tienen una tasa de demanda esperada de menos de una vez al año. Cualquier empresa que implemente u opere un sistema que represente un peligro potencial para los empleados, los residentes locales o el medio ambiente debe minimizar los riesgos del proceso en condiciones de falla. Para hacerlo, el IEC 61508 y el IEC 61511 describen los siguientes pasos:

- Definir y evaluar los riesgos de acuerdo con las probabilidades de falla detalladas para sensores, controladores, actuadores y otros componentes;
- Definir e implementar medidas para minimizar los riesgos residuales;
- Utilizar solo dispositivos evaluados o certificados;
- Realizar pruebas periódicas para garantizar el cumplimiento de las funciones de seguridad.

Una inmersión profunda en arquitecturas de SIS redundantes

El IEC 61508 y el IEC 61511 recomiendan diversas redundancias para aumentar la integridad de seguridad de los sistemas electrónicos programables. Estas arquitecturas, que colocan la seguridad y la confiabilidad de los procesos a la vanguardia del diseño de hardware, desempeñan un papel fundamental en las aplicaciones que procesan petróleo crudo, gases naturales, productos químicos y otras sustancias peligrosas. Estas incluyen:

- **1oo1 (Uno de uno):** Testa arquitectura presenta un solo elemento. Si el contacto no se abre en caso de emergencia, el sistema podría sufrir una falla peligrosa.
- **1oo2 (Uno de cada dos):** este diseño mejora la seguridad del sistema al agregar redundancia. Debido a que solo se requiere un contacto para iniciar un apagado seguro, el PFD es más bajo.
- **2oo2 (Dos de dos):** Testa configuración agrega redundancia para una mejor confiabilidad del proceso. Debido a que las salidas están cableadas en paralelo, ambos contactos deben estar en operación para iniciar un apagado del proceso, reduciendo la tasa de disparos falsos pero aumentando el PFD.
- **2oo3 (Dos de tres):** este diseño, en el que dos de los tres canales deben coincidir en la salida, agrega redundancia avanzada para una mejor seguridad y confiabilidad del proceso. Involucra más componentes, aumenta los requisitos de entrada/salida (E/S) y el consumo de energía, y se ve comúnmente en aplicaciones como turbinas de gas, compresores y calentadores. Esta arquitectura reduce tanto la tasa de disparos falsos como el PFD promedio.

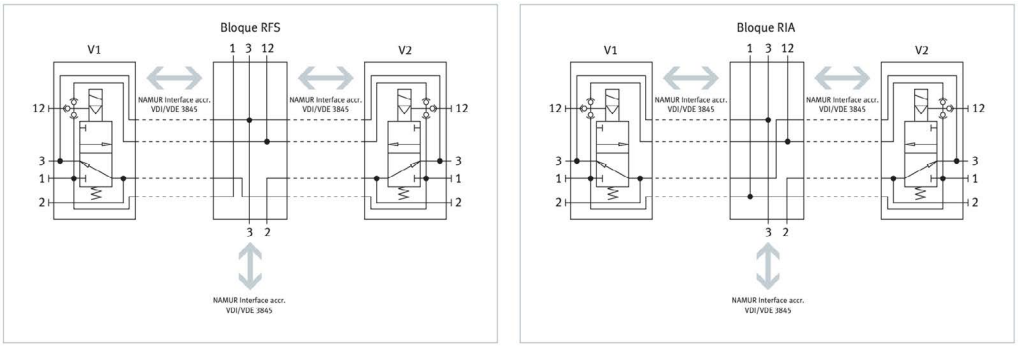


Arquitecturas SIS básicas y avanzadas.

Los sistemas redundantes más comunes a nivel de campo son 1oo2, que aumenta la seguridad, y 2oo2, que aumenta el tiempo de actividad. En una configuración 1oo2, dos válvulas se conectan en serie y son energizadas durante el funcionamiento. Si una válvula o solenoide falla, todo el sistema se vacía para protegerlo de daños. Las líneas transportadoras de medios con frecuencia requieren 1oo2 por el mayor nivel de seguridad que logra. En una configuración 2oo2, dos válvulas se conectan en paralelo y se energizan durante el funcionamiento. Si una válvula o solenoide falla durante el funcionamiento, todo el sistema permanecerá activo y continuará funcionando. Los circuitos de refrigeración, que requieren este tiempo de actividad constante, suelen utilizar la arquitectura 2oo2.

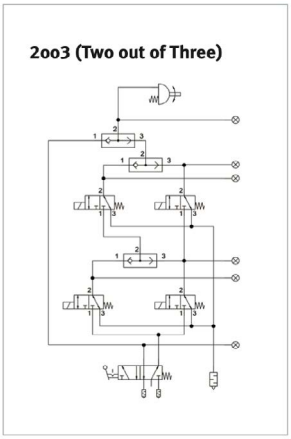
Redundancia a nivel de campo

Para visualizar cómo funcionan varias arquitecturas de SIS redundantes en la práctica, exploremos algunos ejemplos. Este primer escenario implica un bloque NAMUR redundante, que permite a los usuarios instalar dos válvulas de solenoide de la serie VOFC o VOFD de Festo. Estas válvulas están interconectadas, proporcionando redundancia para las válvulas de proceso automatizadas. Además, la interfaz NAMUR hace que la redundancia sea fácil de implementar, reduce los costos de almacenamiento y hace que el reemplazo de la válvula sea rápido y fácil. Los bloques están disponibles con una función a prueba de fallas (1oo2) o con mayor tiempo de actividad (2oo2), y los usuarios pueden montar el bloque directamente en actuadores de cuarto de vuelta utilizando la interfaz estandarizada. Con una configuración 1oo2 y usando una terminal de alimentación auxiliar adicional, el bloque NAMUR también se puede usar con válvulas solenoides con piloto en actuadores que tienen un posicionador para funcionamiento a prueba de fallas. Esta solución ofrece a los usuarios altos niveles de flexibilidad, gracias a las numerosas opciones de protección contra ignición, certificaciones y conexiones globales.



Configuraciones de bloque NAMUR para redundancia a prueba de fallas (1oo2) y mayor tiempo de actividad (2oo2).

Nuestro siguiente ejemplo involucra válvulas en línea redundantes para las arquitecturas 1oo2 y 2oo2. Con estos sistemas compactos, dos válvulas de la serie VOFD se combinan en una misma carcasa. Gracias a su recubrimiento especial, estas válvulas cumplen con los más altos estándares de seguridad en la ingeniería de procesos y pueden soportar condiciones de clima difíciles. Además, sus circuitos redundantes garantizan un funcionamiento a prueba de fallas (1oo2) o logran un mayor tiempo de actividad (2oo2) para las válvulas de proceso automatizadas. Al igual que la opción de bloque NAMUR, esta solución ofrece a los usuarios altos niveles de flexibilidad, gracias a las numerosas opciones de protección contra ignición, certificaciones y conexiones globales.ility, thanks to the many ignition protection options, global certifications and connections.



NAMUR opción de redundancia en línea (2oo3).

Nuestro último ejemplo combina el bloque NAMUR y las válvulas en línea, creando un sistema 2oo3 que proporciona la máxima seguridad y disponibilidad del proceso al mismo tiempo. El bloque en sí es una variante en línea que los usuarios pueden integrar fácilmente en su sistema, con válvulas estándar montadas directamente en el bloque a través de la interfaz NAMUR. Este diseño 2oo3 ofrece varios beneficios:

- Los usuarios pueden reemplazar fácilmente válvulas individuales o desviar sus funciones. Esta derivación se puede desbloquear con una llave, lo que permite al personal realizar el mantenimiento durante la operación.
- Los usuarios pueden montar indicadores de presión mecánicos o manómetros directamente en el bloque de válvulas, proporcionando una indicación confiable de si una válvula está presurizada.
- Los usuarios pueden reemplazar los lectores mecánicos con sensores de presión electrónicos para reflejar el estado del sistema de control.

Más información sobre la seguridad funcional

La ingeniería de seguridad es uno de los requisitos más importantes de la industria de procesos. En Festo, ofrecemos productos y soluciones que son el requisito previo perfecto para implementar la ingeniería de seguridad de la manera más fácil y rentable posible. Para obtener más información, descargue nuestra Guía de seguridad funcional.

Otros productos para aplicaciones relacionadas con la seguridad

Los siguientes productos de Festo pueden ayudarle a mejorar la integridad de la seguridad en toda su aplicación de proceso:

- **Actuadores.** Ofrecemos actuadores de acción simple y doble, probados y listos para instalar en sistemas de seguridad. Nuestras válvulas de proceso automatizadas solo utilizan componentes certificados y podemos realizar evaluaciones SIL o ATEX de actuadores de acuerdo con la declaración del fabricante.
- **Redundancia PROFIBUS.** Nuestra solución PROFIBUS redundante aumenta la seguridad entre el sistema de control distribuido y las E/S remotas. Si se quita un cable PROFIBUS o el nodo está defectuoso, entonces un segundo cable PROFIBUS y el nodo se hacen cargo, enviando y recibiendo de manera confiable todos los protocolos del sistema de control.
- **Armarios de control.** Los armarios de control personalizables protegen los componentes de factores ambientales, fluidos y materias extrañas. Elija entre conexiones de tubo o de tubería. Y ya sea que utilice componentes neumáticos, eléctricos o electroneumáticos, recibirá un gabinete de control que cumpla con los requisitos únicos para su aplicación. Si lo solicita, podemos realizar una evaluación SIL del gabinete y, para su protección contra explosión, podemos fabricar armarios en un diseño 2GD o 3GD que cumpla con las normas internacionales y del Código Eléctrico Nacional (NEC, por sus siglas en inglés).

Modificado por:
Festo Corp.
1377 Motor Parkway
Islandia, NY 11749

Editor:
Festo SE & Co. KG.
Ruiter Strasse 82
D-73734 Esslingen
www.festo.com