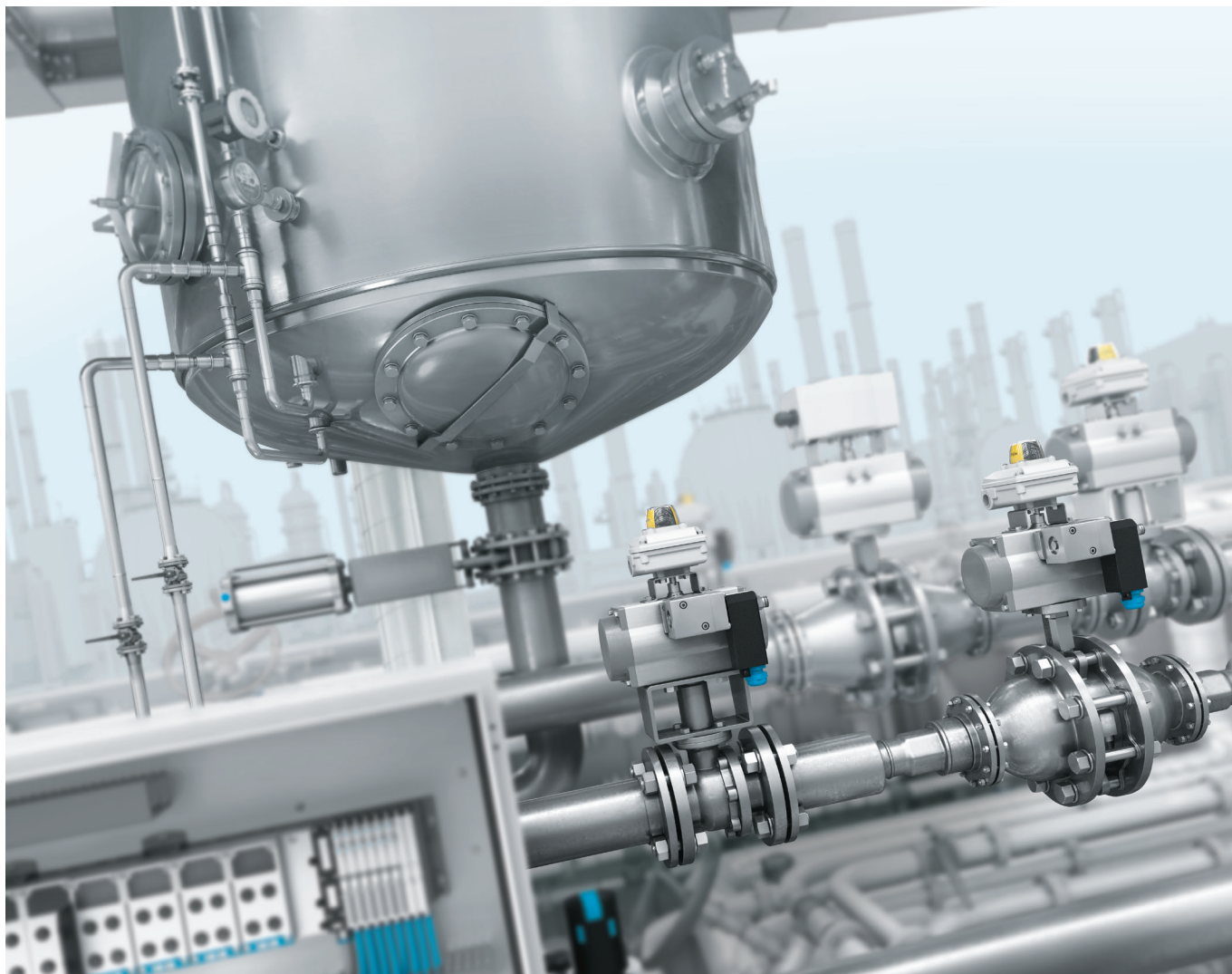


Libro blanco

Control de válvulas de proceso teniendo en cuenta la seguridad funcional (SIL)



Desde la entrada en vigor de la norma IEC 61508, el tema "Seguridad funcional" en la industria de procesos ha ganado en importancia. A menudo, solo se utiliza el término SIL. Pero ¿qué es exactamente SIL y qué soluciones existen para controlar las válvulas de proceso?

En este libro blanco encontrará la siguiente información:

- ¿Qué es SIL (Safety Integrity Level)?
- Parte normativa
- El análisis de riesgos
- Certificados y declaraciones del fabricante
- Dispositivo de protección con ejemplo de un reactor de tanque agitado
- Funcionamiento y prolongación de la vida útil con ejemplo de electroválvula
- Accionamientos redundantes de actuadores sobre el terreno

1. ¿Qué es SIL (Safety Integrity Level)?

La tarea de las funciones de seguridad (Safety Functions) consiste en minimizar los riesgos de los procesos que supongan riesgos para las personas, los bienes y el medioambiente. SIL (Safety Integrity Level) describe la dimensión de dicha reducción de riesgos a un nivel razonable. La norma IEC 61508 explica tanto el tipo de evaluación de riesgos (gráfico de riesgos) como las medidas para instalar las correspondientes funciones de seguridad de sensores, procesamiento lógico y actuadores en relación a la "Prevención de errores" (errores sistemáticos) y el "Control de errores" (errores ocasionales). Esta norma básica independiente de la aplicación describe los requisitos de componentes y sistemas para las funciones de seguridad y contribuye a la elaboración de normas específicas del sector, como la norma IEC61511-1 "Seguridad funcional: Sistemas de seguridad para el sector de las industrias de procesos". Entre otros aspectos, la norma IEC 61511-1 determina los criterios de selección para componentes de funciones de seguridad como, por ejemplo, el funcionamiento de sensores y actuadores.

Sensor ≥35 %	Lógica ≥15 %	Actuador ≥50 %			
					
PFD/PFH	λ_{SD}	PFD/PFH	λ_{SD}	PFD/PFH	λ_{SD}
SFF	λ_{SU}	SFF	λ_{SU}	SFF	λ_{SU}
HFT	λ_{DD}	HFT	λ_{DD}	HFT	λ_{DD}
MTBF	λ_{DU}	MTBF	λ_{DU}	MTBF	λ_{DU}
SIL _{necesario} (SIL _r)					
PFD _{total} /PFH _{total}					
indicado por el fabricante					
lo debe determinar el usuario del equipo					

Qué debe saber

La demanda de la probabilidad de fallos según la norma IEC 61508 se refiere siempre a un dispositivo de protección completo y no a componentes individuales. Por lo tanto, un componente por sí solo puede no tener un nivel SIL, sino solo el circuito de seguridad completo, denominado SIS.

Por norma general, un circuito de seguridad está formado por los siguientes componentes:

- Sensores, p. ej., sensor de presión, temperatura y nivel de llenado
- Unidad de evaluación y unidad de salida, p. ej. PLC de seguridad
- Válvulas de proceso automatizadas compuestas por electroválvula, actuador y válvulas de proceso

Asignación habitual del PFD/PFH a sistemas parciales de una función de seguridad en sistemas monocanal

2. Parte normativa

Las normas sobre la temática de "Seguridad funcional" son variadas y no siempre resulta sencillo distinguirlas, incluso para usuarios experimentados. En este libro blanco nos centramos en la implementación práctica, así como en la interpretación de dichas normas, y, por tanto, no profundizamos en la parte normativa.

Por norma general, resultan relevantes las siguientes normas:

- Norma IEC 61508 "Seguridad funcional de los sistemas eléctricos/electrónicos/electrónicos programables, relacionados con la seguridad"
- Norma básica para la temática de seguridad funcional
- Norma IEC 61511 "Seguridad funcional. Sistemas de seguridad para el sector de las industrias de procesos"
- válida para la automatización de procesos

3. El análisis de riesgos

Para minimizar los riesgos, la norma IEC 61508 y la norma IEC 61511 prescriben principalmente los siguientes pasos:

- Definición y evaluación de los riesgos según las probabilidades de fallo detalladas desde el sensor, el controlador y hasta el actuador, y durante toda la vida útil de los componentes.
- Determinación y aplicación de las medidas para minimizar los riesgos residuales
- Utilización de equipos adecuados (evaluados o certificados)
- Inspección periódica para asegurar el correcto funcionamiento de las funciones de seguridad

3.1. Análisis HAZOP y otros procesos

Se denominan riesgos a aquellas posibles desviaciones graves de los planes sobre el proceso de fabricación. Los riesgos también son peligros que representan una amenaza real o potencial. HAZOP ("Hazard and Operability Study") sirve para identificar, de forma sistemática, los errores y fallos de funcionamiento que reducen la productividad (Operability Problems). Actualmente, esta tecnología se utiliza de forma universal en equipos de todo tipo que fabrican de forma continua o discontinua. Los pasos básicos para un análisis HAZOP son:

- 1) Pronóstico de un posible resultado
- 2) Determinación de las causas
- 3) Valoración de los efectos
- 4) Medidas correctoras

Otros procedimientos utilizados durante en análisis de riesgos son, por ejemplo, el análisis modal de fallos y efectos (AMFE), el análisis de árbol de eventos (ETA, por sus siglas en inglés) o el análisis del árbol de fallos (FTA, por sus siglas en inglés). El procedimiento puede

dividirse en tres grupos: procedimiento inductivo como AMFE, en el que se conocen las causas del fallo pero no las consecuencias resultantes; procedimiento deductivo como FTA, en el que se conocen las consecuencias pero no las causas, y el procedimiento explorativo, en el que no se conocen las causas ni las consecuencias de las desviaciones, como HAZOP. La información que falta debe determinarse mediante la implementación de los métodos.

Además, puede realizarse una distinción en la búsqueda de abajo hacia arriba (Bottom-Up) y de arriba hacia abajo (Top-Down). Hacia abajo significa que se parte de un error crítico y se intentan determinar las consecuencias (AMFE). En la búsqueda hacia arriba, se parte de las consecuencias peligrosas y se intentan determinar las causas (FTA).

SIL (Safety Integrity Level)

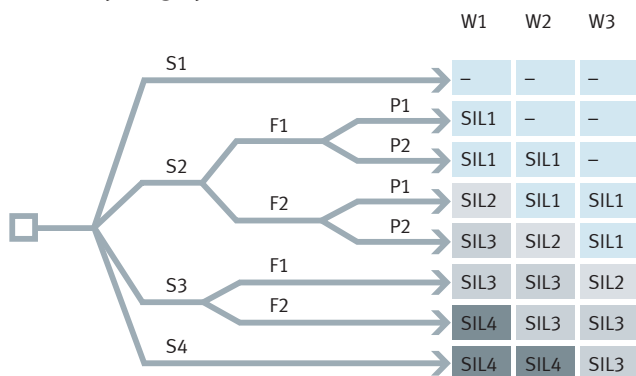


Gráfico de riesgos: cuatro niveles discretos (SIL1 a SIL4). Cuanto mayor sea el nivel SIL de un sistema relacionado con la seguridad, menor es la probabilidad de que el sistema no pueda efectuar las funciones de seguridad necesarias.

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

3.2. Términos y factores relevantes

HFT

La Hardware Failure Tolerance (HFT) describe la capacidad de implementar funciones de seguridad en caso de (varios) errores y desviaciones. Si no se alcanzase el nivel SIL necesario debido a dichos valores, cabe la posibilidad de alcanzar dicho nivel SIL mediante redundancias.

SFF

La Safe Failure Fraction determina la proporción de fallos seguros del número total de fallos. Se denomina error seguro a aquellos errores que no conllevan un estado peligroso del equipo o que podrían conllevar un estado peligrosos del equipo, pero son detectables.

La idoneidad del producto para el nivel SIL necesario se determina mediante varios parámetros:

Low Demand

Modo de funcionamiento con frecuencia baja de demanda en el sistema de seguridad. El sistema de seguridad no puede solicitarse más de una vez al año.

→ PFD (probability of failure on demand) = la probabilidad de fallos en la demanda está relacionada con los eventos

High Demand

Modo de funcionamiento con frecuencia elevada de demanda o demanda continua en el sistema de seguridad. El sistema de seguridad funciona de forma continua y se solicita más de una vez al año.

→ PFH (probability of failure per hour) = la probabilidad de fallo por hora está relacionada con el tiempo

Tipo de equipo A/B

Tipo A: se describe de forma suficiente el comportamiento en caso de avería de todos los componentes. Por lo tanto, los equipos sencillos (nuevos) y los equipos de funcionamiento garantizado forman parte de este tipo de equipos.

Tipo B: no se conoce totalmente el comportamiento en caso de avería de, como mínimo, un componente. Por lo tanto, los equipos complejos y productos innovadores forman parte de este tipo de equipos.

Objetivo: $SIL \geq SIL_r$

Nivel SIL			Tipo de equipo A				Tipo de equipo B					
			Safe Failure Fraction (SFF)									
	High Demand Mode	Fallos máximos aceptables del sistema de seguridad	< 60%	60...90%	90...99%	> 99%	< 60%	60...90%	90...99%	> 99%	Low Demand Mode	Fallos máximos aceptables del sistema de seguridad
	$10^{-5} \leq PFH < 10^{-4}$	Riesgo de un fallo cada 10 000 horas										
1	$3 \times 10^{-6} \leq PFH < 10^{-5}$	Riesgo de un fallo cada 1 250 días	HFT 0				HFT 1	HFT 0			$10^{-2} \leq PFD < 10^{-1}$	una vez cada 10 años
	$10^{-6} \leq PFH < 3 \times 10^{-6}$	Riesgo de un fallo cada 115,74 años										
2	$10^{-7} \leq PFH < 10^{-6}$	Riesgo de un fallo cada 115,74 años	HFT 1	HFT 0			HFT 2	HFT 1	HFT 0		$10^{-3} \leq PFD < 10^{-2}$	una vez cada 100 años
3	$10^{-8} \leq PFH < 10^{-7}$	Riesgo de un fallo cada 1 157,41 años	HFT 2	HFT 1	HFT 0	HFT 0		HFT 2	HFT 1	HFT 0	$10^{-4} \leq PFD < 10^{-3}$	una vez cada 1 000 años
4	$10^{-9} \leq PFH < 10^{-8}$	Riesgo de un fallo cada 11 574,1 años		HFT 2	HFT 1	HFT 1			HFT 2	HFT 1	$10^{-5} \leq PFD < 10^{-4}$	una vez cada 10 000 años
					HFT 2	HFT 2		HFT 2				
(por hora)												

(por hora)

Cuadro general de las probabilidades de fallo y Hardware Failure Tolerance

4. Certificados y declaraciones del fabricante

Los usuarios del equipo deben presentar una prueba de la clasificación SIL de los componentes instalados por SIS (Safety Instrumented Systems). Conforme a IEC 61511, las declaraciones del fabricante son totalmente suficientes para ello. Los certificados no se exigen ni legalmente ni debido a la norma. Para poder elaborar una declaración del fabricante o un certificado, se requiere una valoración técnica de los componentes de seguridad que deben implementarse. A menudo, dicha valoración la realiza una organización independiente como, por ejemplo, TÜV o Exida. Tras una valoración satisfactoria, el fabricante puede elaborar una declaración del fabricante y, en caso necesario, hacer referencia al informe de ensayo de dicha valoración.

En contraposición a las declaraciones de los fabricantes, los certificados solo pueden ser expedidos por una organización acreditada (p. ej. TÜV).

Cuanto mayor sea la seguridad necesaria de un equipo, mayor debe ser la independencia de la organización que evalúa la seguridad funcional y expide la valoración:

Safety Integrity Level	Organización evaluadora
SIL 1	persona independiente
SIL 2	departamento independiente
SIL 3	organización independiente
SIL 4	organización independiente

5. Dispositivo de protección con ejemplo de un reactor de tanque agitado

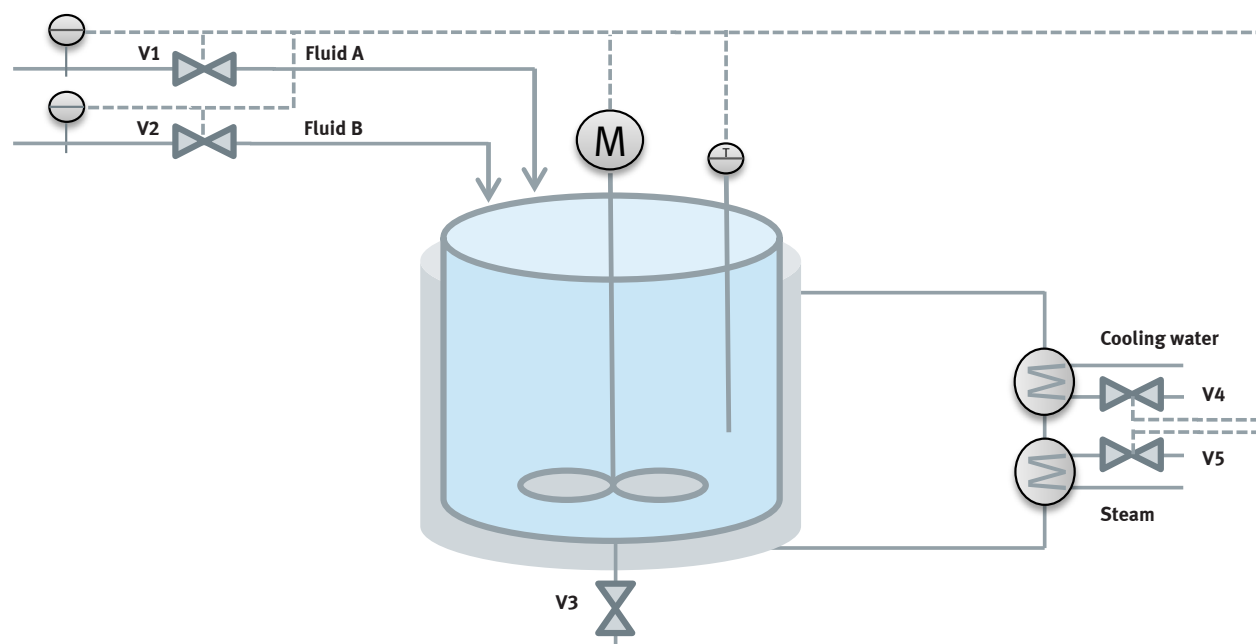
En un reactor de tanque agitado se combinan diferentes componentes (en el siguiente ejemplo mediante las válvulas V1 y V2) y dichos componentes reaccionan unos con otros debido al aporte de calor (reacción endotérmica) o durante la generación de calor (reacción exotérmica). Durante el proceso de agitación, se produce un mezclado intenso. En el caso de las reacciones exotérmicas, deben evitarse los sobrecalentamientos.

para un proceso de reacción. Si la presión en el reactor es demasiado elevada, se produce un error que impide el funcionamiento correcto de la disipación de calor. Como consecuencia de esto, la proporción de mezcla no sería la adecuada.

Esta situación conlleva la siguiente demanda de un dispositivo de protección: cerrar las válvulas de entrada V1, V2 y la válvula de vapor V5, y abrir, al mismo tiempo, la válvula de refrigeración V4 para refrigerar el reactor.

Un ejemplo del esquema representado a continuación, para el que se necesita un dispositivo de protección, es la regulación de presión

Para solucionar la problemática citada anteriormente, existen diferentes posibilidades en función del nivel de riesgo:



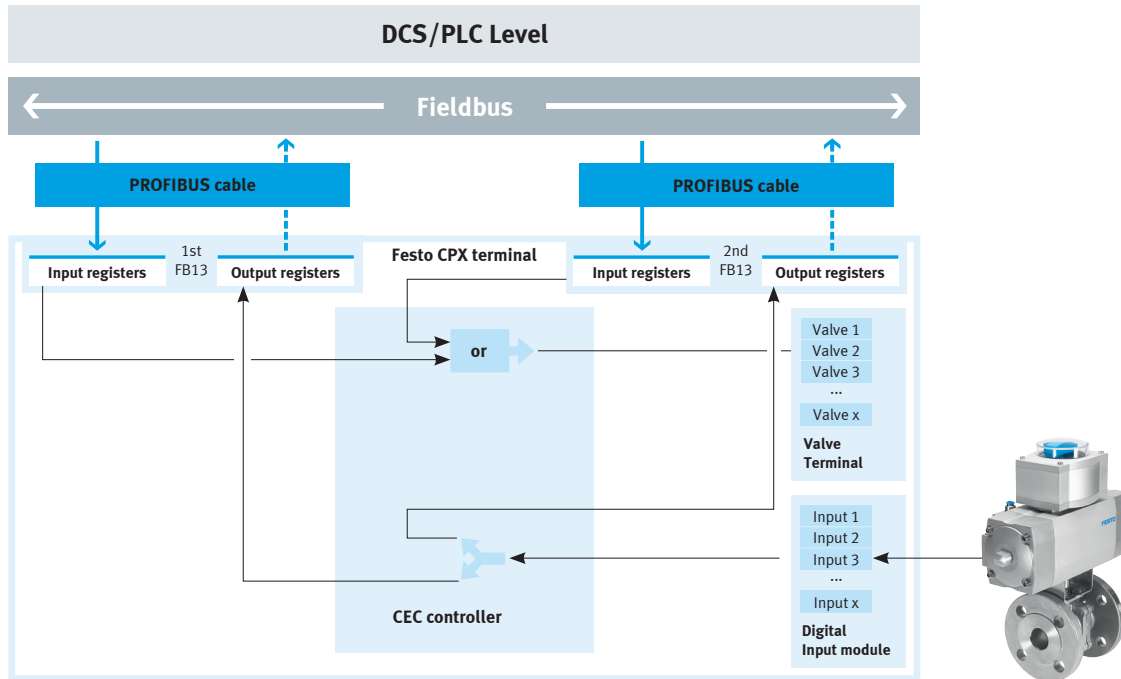
Representación esquemática de un reactor de tanque agitado

5.1. Aumento de la seguridad mediante una solución PROFIBUS redundante entre el sistema de control distribuido (DCS) y la entrada/salida remota.

Si se debe retirar un cable PROFIBUS o un nodo de red PROFIBUS está defectuoso, el segundo cable/nodo de red PROFIBUS asume las funciones. Este envía y recibe de forma fiable los protocolos desde el sistema de control distribuido.

Ventaja adicional:

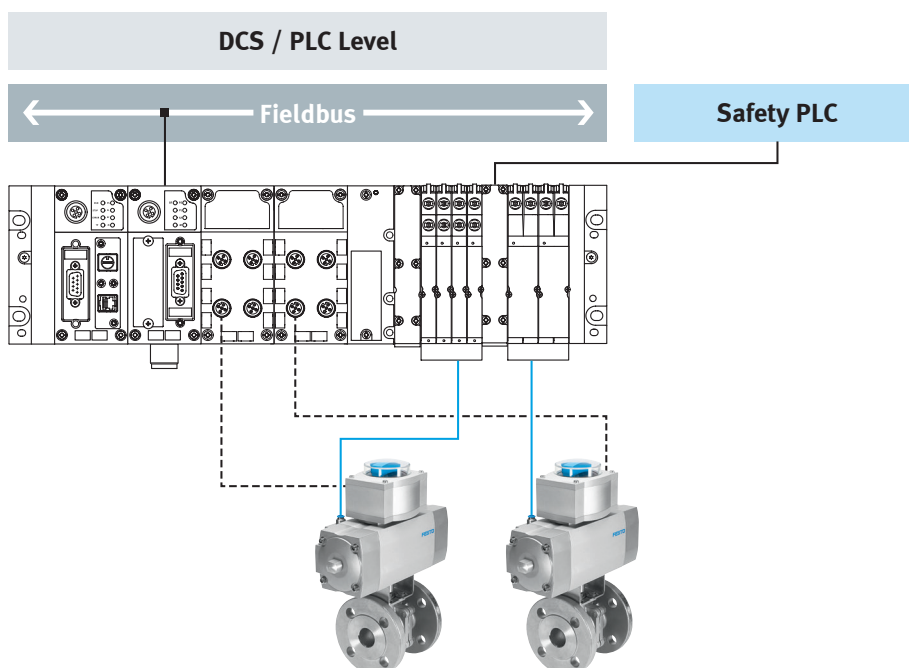
Mediante un controlador adicional con interfaz Ethernet, puede conectarse in situ a la entrada/salida remota y puede llevarse a cabo la parametrización o pueden implementarse procesos adicionales. La tecnología probada de entrada/salida remota asume de forma fiable las funciones del nivel de control con sus módulos de entrada para conectar los sensores NAMUR. Los terminales modulares, junto a la terminal de válvulas evaluada y disponible conforme a SIL2, constituyen una alternativa compacta.



5.2. Terminal de válvulas con desconexión de seguridad integrada

El modo de funcionamiento se lleva a cabo mediante los módulos de bus de campo y el terminal de válvulas con actuadores dispuestos en línea. El terminal de válvulas dispone de una alimentación independiente del Safety PLC, que controla las válvulas de forma autónoma.

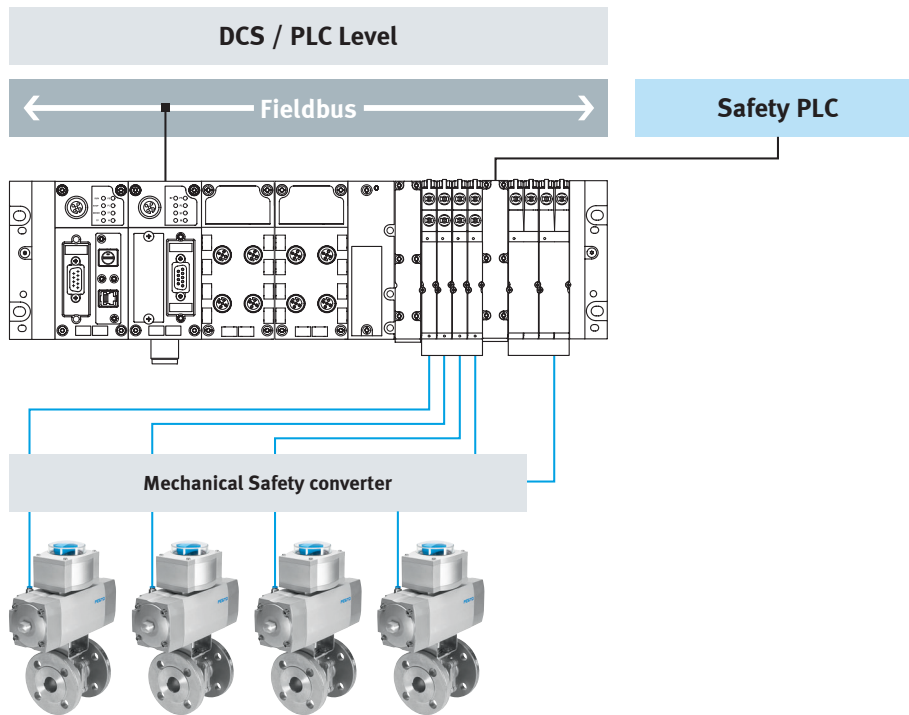
De esta forma, se conectan los actuadores para desconectar el proceso de forma segura. Esta solución es adecuada para circuitos SIL2. Con objeto de aumentar el nivel de seguridad, existe la posibilidad de interconectar las válvulas de forma redundante.



5.3. Terminal de válvulas con desconexión de seguridad integrada

En el modo de funcionamiento se controla el terminal de válvulas mediante un bus de campo y activa los actuadores del proceso. Además, el terminal de válvulas dispone de una alimentación independiente del Safety PLC, que controla las válvulas del terminal de válvulas para la desconexión de seguridad. El escape de aire se realiza mediante una válvula de 3/2 vías adicional, que se conecta en servicio normal y, de esta forma, impide que se abran las válvulas de

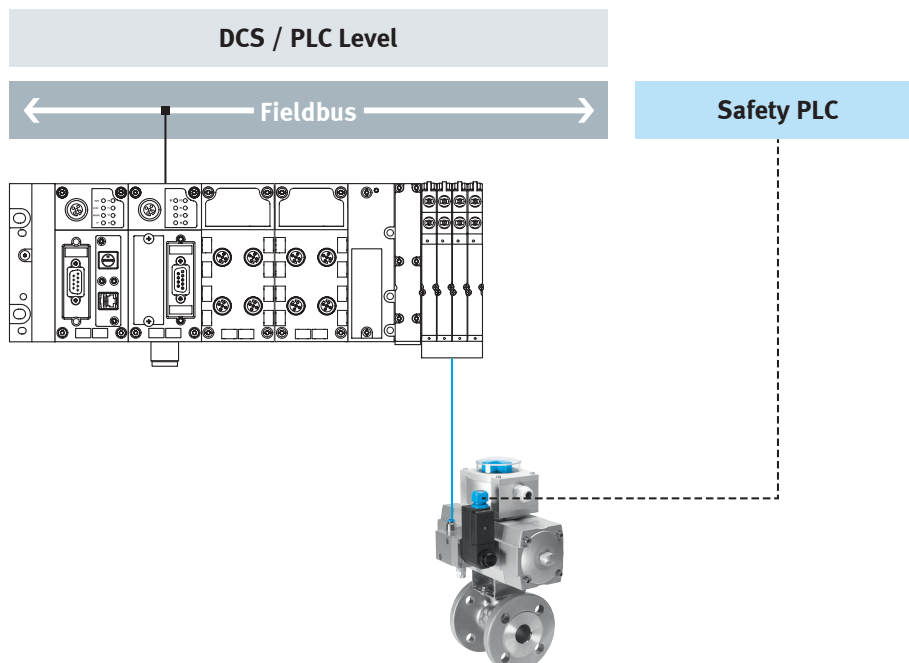
antirretorno montadas en las derivaciones intermedias. Además, se garantiza la posición de conmutación de la válvula mediante el control de la presión. Para ello, se conectan los mismos actuadores para desconectar el proceso de forma segura. Esta solución es adecuada para circuitos SIL2. Con objeto de aumentar el nivel de seguridad, existe la posibilidad de interconectar las válvulas de forma redundante.



5.4. Terminal de válvulas y válvula individual para la desconexión de seguridad

El modo de funcionamiento se controla mediante el bus de campo y el terminal de válvulas y activa los actuadores de campo. La válvula indi-

vidual certificada y montada en el mismo actuador se controla directamente mediante el Safety PLC y se desconecta de forma segura en caso necesario. Estas válvulas se pueden emplear en circuitos orientados a la seguridad hasta un nivel SIL3.



6. Funcionamiento y prolongación de la vida útil con ejemplo de electroválvula

La globalización, especialmente en la industria química, obliga a las empresas a sacar el máximo provecho a sus equipos. Sobre todo, para compensar la caída de los precios en el mercado y para continuar siendo competitivas. Esto solo puede lograrse con un equipo sin tiempos de parada que funcione con fiabilidad y sea altamente productivo, ya que se sigue optimizando la tecnología de procesos en los equipos modernos. Esto implica la reducción de los ciclos y tiempos de revisión, así como la prevención de tiempos de parada de máquinas debido a reparaciones fuera de las revisiones y paradas programadas.

Una posibilidad de garantizarlo, la ofrece la implementación de componentes de funcionamiento probado de la tecnología electrónica de regulación, control y medición (EMSR, por sus siglas en alemán), como las electroválvulas, certificados según la norma IEC 61508.

Sin embargo, en las electroválvulas certificadas también existe una gran diferencia apreciable en su rendimiento y en su índice de seguridad. Existen numerosas soluciones de electroválvulas en el mercado para el modo Low Demand, es decir, para dispositivos de seguridad. Muchos de dichos dispositivos presentan una vida útil limitada o tienen especificaciones en relación al tiempo de parada o el número de conexiones que deben realizarse anualmente para poder satisfacer los índices de seguridad.

El aumento de la fiabilidad constituye un requisito para prolongar los intervalos entre ensayos. De esta manera, es posible ahorrarse grandes importes. En las refinerías de petróleo es costumbre, desde hace

ya tiempo, realizar paradas solo cada cinco años. En ellas se ha alcanzado una alta fiabilidad, sobre todo, mediante la "filosofía dos de tres" (2003) y al apoyo ofrecido por los equipos y aparatos redundantes. Este costoso recorrido resulta rentable gracias a las grandes capacidades de estos equipos. Esto no siempre es válido con las instalaciones químicas. En ellas, actualmente se intenta alcanzar la misma fiabilidad elevada que con componentes redundantes, mediante equipos de alta fiabilidad certificados (motores eléctricos, transmisores, controles, electroválvulas o, incluso, válvulas de proceso).

Las electroválvulas servopilotadas en la tecnología de válvulas de asiento con certificados TÜV conforme a la norma IEC 61508 están disponibles en el mercado hasta el nivel SIL 3 incluido. Estas válvulas garantizan, según la clasificación SIL, una tasa de disfunción del $2,41 \times 10^{-4}$, es decir, utilizando correctamente las válvulas se puede producir, como máximo, una conmutación defectuosa cada 2410 conmutaciones.

Desde el año 2002, en las máquinas solo se utilizan electroválvulas con certificado SIL. Los valores iniciales de seguridad, alcanzados mediante las pruebas de laboratorio, se han confirmado mediante las electroválvulas utilizadas desde entonces y procedentes de dicha época. Esto significa que, durante este tiempo, existen electroválvulas con certificado SIL que no requiere limitación temporal en el certificado. En los ensayos realizados en el laboratorio, dichas electroválvulas han demostrado que las electroválvulas en la tecnología de válvulas de asiento, incluso tras más de 12 años de uso y en comparación con las válvulas nuevas, presentan tiempos de conmutación breves y casi inalterables. De esta forma, se garantiza la estanqueidad hacia fuera, así como a través del asiento de la junta.



Válvula de asiento de émbolo de 3/2 vías con conexión NAMUR ampliada y certificado TÜV según IEC 61508

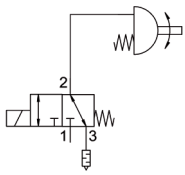
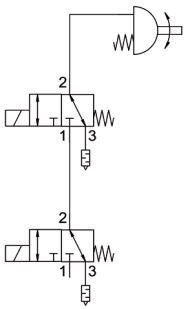
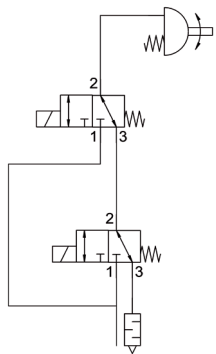
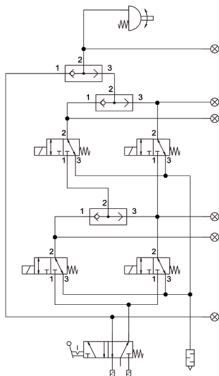
7. Accionamientos redundantes de actuadores sobre el terreno

Si las medidas citadas en "6. Funcionamiento y prolongación de la vida útil con ejemplo de electroválvula" no son suficientes, existe la posibilidad, ya mencionada anteriormente, de establecer una interconexión de las electroválvulas (HFT1 o HFT2).

La seguridad del proceso y la fiabilidad son siempre la prioridad cuando se usan redundancias. Las interconexiones de seguridad habituales en la técnica de procesos son 1oo2 (One out of Two), 2oo2 (Two out of Two) y 2oo3 (Two out of Three). Estas se aplican en extracción y procesamiento de materiales de alto valor y peligrosos como petróleo, gas natural, productos químicos....

7.1. Las funciones del esquema de conexiones

Con el fin de proporcionar redundancia en el caso de un fallo de una válvula, se instalan los sistemas en equipos críticos para la seguridad o los procesos. Gracias a la construcción compacta reducen el esfuerzo del sistema de tuberías y, al mismo tiempo, disminuyen posibles fugas en su sistema, lo que permite ahorrar en costes en el montaje y el funcionamiento del equipo.

1oo1 (One out of One)	1oo2 (One out of Two)	2oo2 (Two out of Two)	2oo3 (Two out of Three)
			
Un único error puede causar una pérdida de la seguridad.	Seguridad Si se detecta un error de una válvula, purgar el sistema completo. Esto causa una pérdida de la seguridad y el equipo pasa a la posición de seguridad.	Disponibilidad Cuando se produce un fallo de las dos válvulas, el funcionamiento ya no está garantizado y causa una pérdida de la seguridad.	Seguridad y disponibilidad Se deben producir al menos tres fallos simultáneos para provocar una pérdida de seguridad. Función, véase 7.5.2

Cuadro general de accionamiento redundante de actuadores sobre el terreno

7.2. Seguridad aumentada (1oo2)

Con el aumento de la seguridad (1oo2) se activan dos válvulas en serie. Estas reciben energía durante el funcionamiento. Si una válvula o una de las dos señales de mando sufren un fallo durante el funcionamiento, se descarga el sistema completo para proteger al equipo frente a daños. Las tuberías de transporte de medios precisan con frecuencia esta seguridad aumentada.

7.3. Disponibilidad aumentada (2oo2)

Con el aumento de la disponibilidad (2oo2) se activan dos válvulas en paralelo. Estas reciben energía durante el funcionamiento. Si una válvula o una de las dos señales de mando sufren un fallo durante el fun-

cionamiento, el equipo sigue estando activo y el sistema completo sigue funcionando. Por ejemplo, los circuitos de refrigeración precisan esta disponibilidad aumentada.

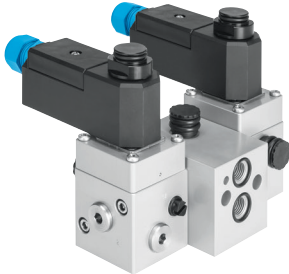
7.4. Seguridad y disponibilidad aumentadas (2oo3)

En una interconexión 2oo3, se combina la seguridad aumentada y la disponibilidad aumentada. Dicha combinación presenta la ventaja de que puede comprobarse el funcionamiento de las válvulas individuales sin conmutar el accionamiento. Esta combinación de válvulas aparece en múltiples aplicaciones importantes en la industria del aceite y el gas, así como en refinerías.

7.5. Soluciones disponibles

7.5.1. Seguridad aumentada del bloque NAMUR (1oo2) y disponibilidad aumentada (2oo2)

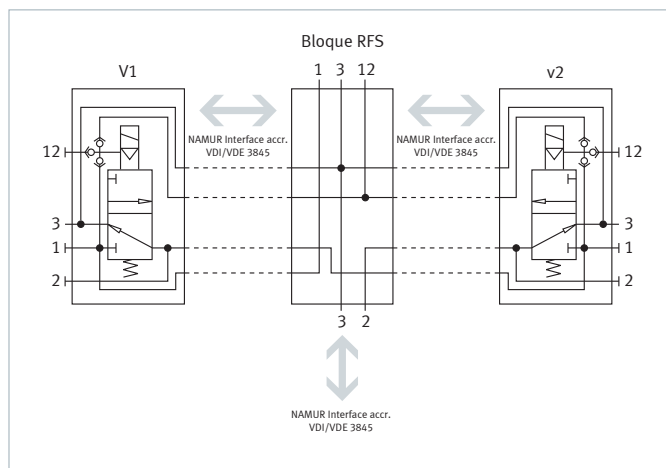
El bloque NAMUR permite la instalación de dos electroválvulas con distribución de conexiones según NAMUR. Mediante las interfaces NAMUR se simplifica la redundancia que se va a realizar. Las ventajas son la reducción de los costes de almacenamiento y la simplificación de la sustitución de las electroválvulas.



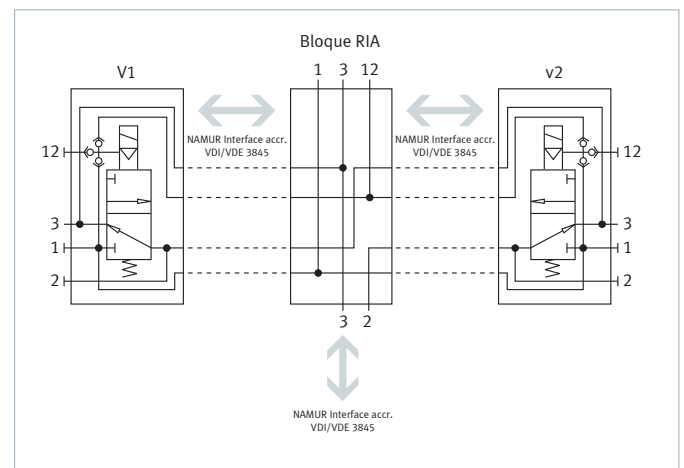
Bloque NAMUR redundante

El bloque NAMUR se puede montar mediante la interfaz NAMUR directamente en un actuador giratorio. Asimismo, es posible una instalación separada con el sistema de tuberías correspondiente.

Con la conexión de energía auxiliar adicional, el bloque NAMUR también puede utilizarse con electroválvulas servopilotadas en accionamientos con posicionadores para funciones Fail-Safe.



Redundant Fail Safe – 1oo2



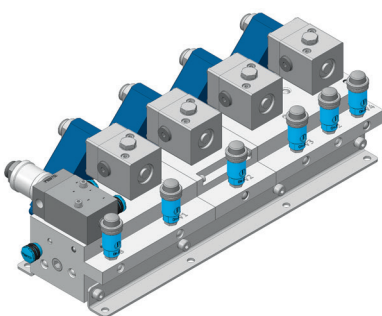
Redundant Increased Availability – 2oo2

7.5.2. Seguridad y disponibilidad en línea/Namur (2oo3)

Existe una combinación para una seguridad y disponibilidad máximas simultáneas. El sistema denominado 2oo3 aúna ambas tecnologías y satisface los mayores requisitos de un equipo.

El bloque de válvulas es una variante en línea y se inserta en el equipo. Las válvulas estándar integradas en el bloque están montadas y definidas mediante la interfaz NAMUR conforme a VDI/VDE 3845. Mediante esta combinación, el bloque se monta de forma única

y las válvulas solo se cambian mediante la interfaz NAMUR en caso necesario conforme al plan Service-Life/Safety-Lifecycle. En los sistemas 2oo3 se pueden evitar también las funciones de las cuatro válvulas mediante un bypass. Esto se puede desbloquear con una llave, de modo que el mantenimiento se pueda llevar a cabo en el funcionamiento en curso. Las indicaciones de presión montadas directamente en el bloque señalizan siempre de forma fiable y rápida si en una válvula hay presión.



Ejemplo para un bloque funcional - 2oo3

Autor:

Reiner Laun
Dirección del sector industrial

Festo AG & Co. KG
Rechbergstr. 19
73770 Denkendorf
Tel.: +49 711 347 76585
reiner.laun@festo.com