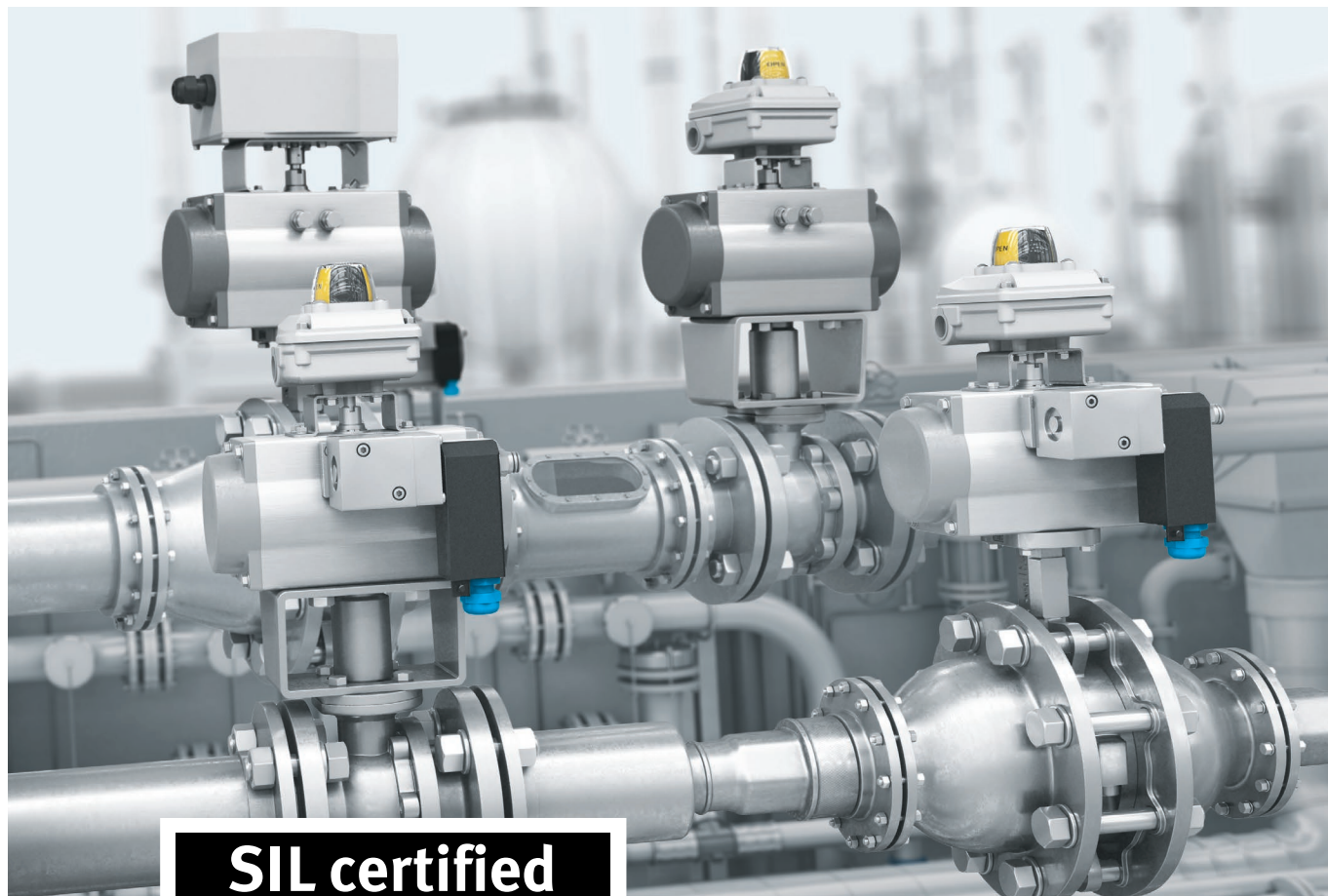


Riesgo minimizado

SIL para la Industria Química

FESTO



Este white paper trata los siguientes temas:

- ¿Qué es SIL, por qué es relevante este tema para los operadores de la planta y qué malentendidos comunes existen en este contexto?
- ¿Qué significan los certificados y cómo se leen correctamente?
- ¿En qué sentido son los componentes duraderos una ventaja útil?

Resumen ejecutivo

Los dispositivos de seguridad en los equipos de la Industria de Procesos deben reducir los riesgos causados por el equipo a las personas y al medio ambiente al nivel más bajo posible. Cuanto más altos son los riesgos que pudiera generar el equipo, menor debe ser la probabilidad de fallo de la cadena de seguridad. Según el potencial de riesgo, el equipo se clasifica en un nivel Safety Integrity Level (SIL)/Nivel de Integridad de Seguridad.

Para lograr el Safety Integrity Level exigido hay que considerar tanto los componentes como el circuito de seguridad al completo. Los valores de seguridad de los componentes se identifican en sus certificados. No obstante, pueden darse malentendidos, porque, por ejemplo, algunos detalles específicos de normas no se mencionen en un certificado. Por tanto, poder leer e interpretar correctamente los certificados es un importante requisito.

La frecuencia con la que debe comprobarse un componente depende del SIL exigido y de la probabilidad de fallo. No obstante, esto es para muchas empresas un importante argumento económico. Los productos con un bajo riesgo de fallo aumentan la productividad. A fin de cuentas, deben comprobarse con mucha menos frecuencia o incluso no necesitar comprobaciones en absoluto. Esto también implica que la producción ya no debe detenerse temporalmente para la realización de comprobaciones. Un claro ejemplo de componentes eficientes en circuitos SIL es una válvula de asiento de émbolo de Festo, que se utiliza en todo el mundo en la industria química.

Seguridad, riesgo y reducción de riesgos

La seguridad tiene muchas facetas. El fallo de dispositivos de seguridad pueden ser costoso en muchos sentidos: los fallos en instalaciones pueden ocasionar daños materiales, pero también, según el sector, daños a personas y perjuicios al medio ambiente. Al mismo tiempo, una desviación en el proceso, por pequeña que sea, también tiene siempre un aspecto económico. La instalación se debe desconectar y revisar. Los dispositivos de seguridad en los equipos de la industria de procesos deben reducir estos riesgos al riesgo residual más bajo posible aceptable.

Según el potencial de peligro, el equipo o partes del equipo se clasifican en un Safety Integrity Level: el SIL. SIL1 es el riesgo más bajo y SIL4, el más alto que se puede asumir con consecuencias catastróficas con eventuales averías. Es importante saber que SIL no describe la idoneidad de componentes, sino que guarda relación con un circuito de seguridad completo, también llamado SIS (Safety Instrumented System) / Sistema Instrumentado de Seguridad. Este incluye todo, desde toda la tecnología de sensores, pasando por la lógica, hasta toda la variedad de actuadores. No obstante, los aparatos y componentes empleados para el circuito de seguridad deben ser aptos para el nivel correspondiente.

En principio, es válido lo siguiente: cuanto más alto es el riesgo residual del proceso, con mayor fiabilidad deben funcionar los dispositivos de seguridad en caso necesario. Si una parte de la instalación está clasificada con un determinado nivel SIL, deberán cumplirse las medidas de protección pasivas y activas requeridas para ello. De este modo se minimiza el riesgo de un proceso no seguro. Mediante dispositivos de protección se reduce el riesgo hasta un riesgo residual aceptable.

➤ El Safety Integrity Level (SIL) describe el potencial de peligro de una planta o de una parte de la planta. Establece la medida con la que debe reducirse un riesgo. No solo hace referencia a componentes individuales, sino más bien a un circuito de seguridad completo. Para ello, a su vez, es necesario emplear los componentes adecuados.

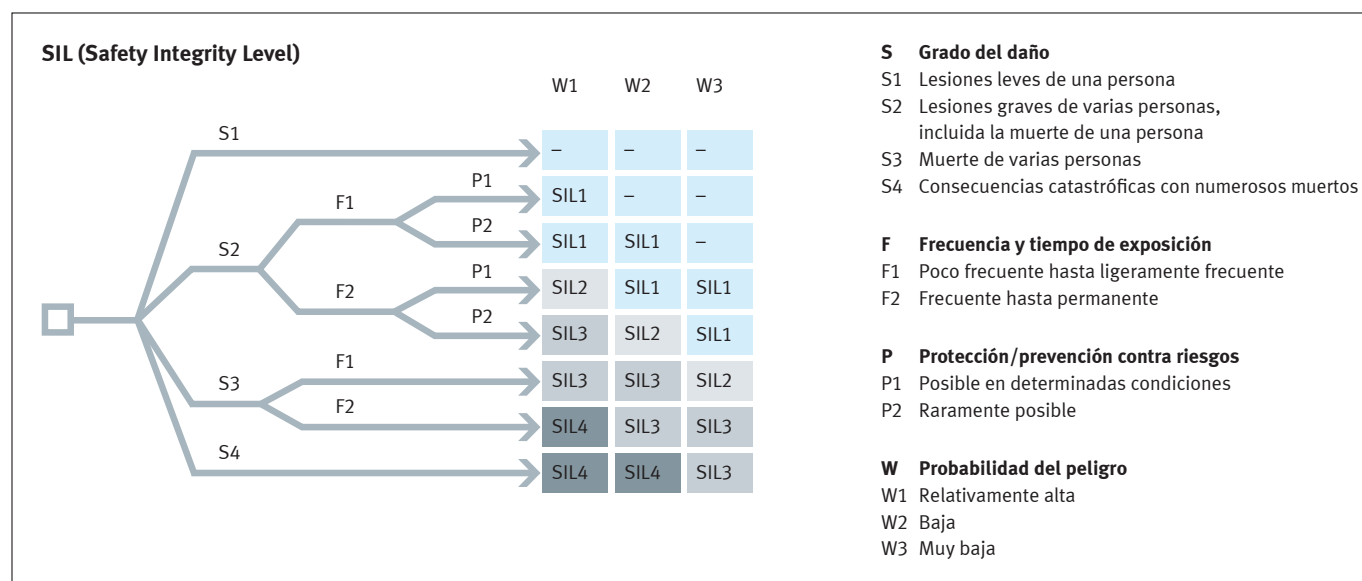


Ilustración: gráfico de riesgos para la evaluación SIL

Normas, reglas y principios

“Siempre existirá un riesgo residual”, afirma Reiner Laun, Gerente del Segmento Industrial de Química en Festo. Los expertos coinciden en que no puede existir un riesgo nulo absoluto. Por tanto, lo determinante es reducir el riesgo a un nivel generalmente aceptable.

Para lograr un estándar internacional y permitir una clara comparación existen diferentes normas. Los operadores de las plantas deben poder tener claro y reconocer fácilmente cómo alcanzar la fiabilidad requerida y deseada de los dispositivos de seguridad

En este sentido, la norma IEC 61508 determina tanto la clase de evaluación de riesgos como la medida para las correspondientes funciones de seguridad de sensores o del procesamiento lógico interno. Lo decisivo a este respecto es que se eviten errores sistemáticos y que puedan tenerse bajo control los errores que se producen de manera fortuita. La norma es un estándar que es independiente de la aplicación. Por tanto, también está designada como norma básica y sirve en todo el mundo de base para las especificaciones, la concepción y la operación de sistemas técnicos de seguridad.

A su vez, de ella se derivaron normas industriales específicas como, por ejemplo, la IEC 61511 para explotadores de instalaciones en la automatización de procesos: esta norma establece criterios de diseño para componentes de las funciones de seguridad. Esto incluye también, por ejemplo, lo que se conoce como validación de operación de sensores y actuadores. Un producto está “validado para la operación” si, de forma probada y documentada, ha funcionado con fiabilidad en las condiciones especiales de la correspondiente operación durante un largo periodo de tiempo conforme a NE 130 ¹.

Para comprender con qué precisión regulan el riesgo y la seguridad estas normas, vale la pena analizar a fondo un ejemplo. En principio, rige lo siguiente: en un proceso de producción pueden producirse fallos. “Los componentes eléctricos, mecánicos y electromecánicos pueden fallar, ya que, entre otras cosas, están expuestos al desgaste y a los efectos atmosféricos”, indica Carsten Schindler, Key Account Manager de la Industria Química en Festo: “O el proceso de producción puede entrar en un estado crítico”. Lo determinante es que se vuelva a alcanzar luego un estado seguro mediante protección y contramedidas.

➤ Siempre existe un riesgo residual: lo determinante es reducirlo hasta un nivel aceptable. Las normas determinan tanto la clase de evaluación de riesgos como medidas para las correspondientes funciones de seguridad. Una medida habitual para alcanzar SIL 3 es el uso de sistemas redundantes.

¹ Recomendación de NAMUR 130:
Equipos de funcionamiento probado para dispositivos de protección en el control de procesos y cálculo de SIL simplificado.

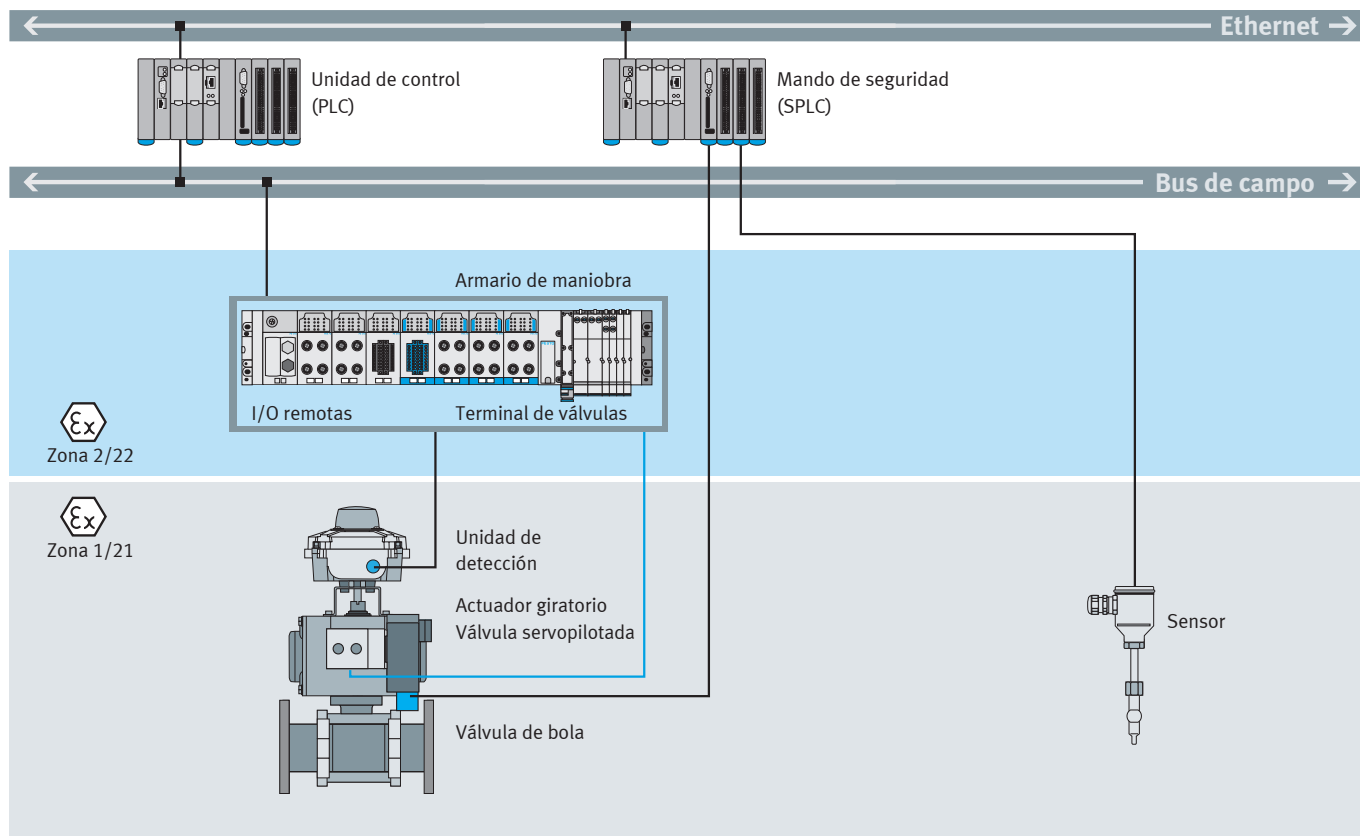


Ilustración: ejemplo de circuito de seguridad SIL-2

La ilustración muestra un circuito de seguridad habitual con el que, por ejemplo, se puede automatizar una mezcladora. La mezcladora se llena con flúidos a través de líneas de alimentación. Los medios fluyen mediante una válvula de proceso. Aparte de la detección de posición, esta válvula normalmente no tiene una función de diagnóstico y, con esta conexión, alcanza como máximo un SIL 2. El controlador lógico programable (PLC) determina cuándo se abre o cierra la válvula de proceso. Existe un riesgo de seguridad si la señal del PLC no llega correctamente a la válvula: por ejemplo, por que la terminal de válvulas no hace la desconexión de un puerto a causa de suciedad en la línea de aire comprimido y, por tanto, no cierra la válvula que tiene conexión con el proceso. Entonces, el líquido vuelve a fluir sin impedimento a la mezcladora.

La contramedida apropiada: un sensor en la mezcladora indica que se ha alcanzado un nivel de llenado crítico. Envía una señal al PLC de seguridad (SPC), este, a su vez, desconecta una válvula servopilotada que actúa como válvula de seguridad y que solo se utiliza para este caso. El proceso se pone en estado seguro. No obstante, el anterior ejemplo no ofrece medidas de protección adicionales en caso de que el accionamiento al completo o la propia válvula de proceso estén defectuosos. Entonces solo habrá un mensaje de error y un empleado realizará la comprobación in situ.

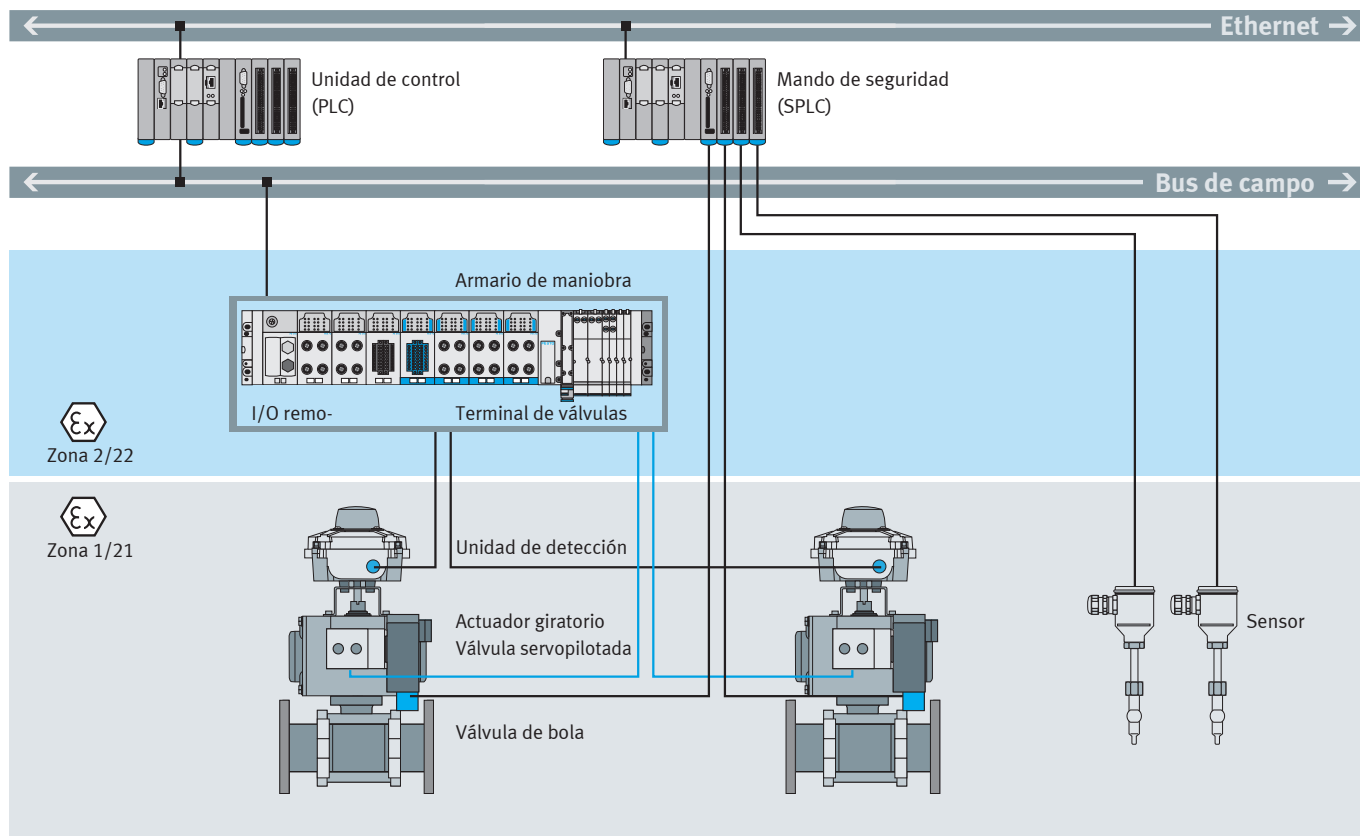


Ilustración: ejemplo de circuito de seguridad SIL-3

Si el circuito SIL-2 arriba mostrado no fuera suficiente porque un rebose del depósito tendría consecuencias muy graves, será necesaria una estructura que minimice sucesivamente este riesgo: la redundancia.

En lugar de una única válvula de proceso aquí hay dos válvulas de proceso conectadas en serie. La probabilidad de que ambas válvulas fallen al mismo tiempo es sumamente baja. A su vez, el riesgo puede minimizarse instalando sensores adicionales para que la técnica de sensores esté realizada de forma redundante. En caso de demanda, un sensor puede iniciar medidas de protección. De este modo también puede alcanzarse un SIL 3 con componentes sin función de diagnóstico.

No obstante, en este caso, un error sistemático que afecte por ejemplo a toda la sensórica podría hacer que ambas válvulas no se reconectasen. Fallos sistemáticos son aquellos fallos que existen ya sea en el momento de suministro del producto (p. ej. errores de software) o que se producen a causa de materiales incorrectos, eventualmente también porque el producto empleado no es adecuado para la tarea prevista o las condiciones ambientales existentes. Una contramedida posible es emplear componentes diversos, es decir componentes de diferentes principios de funcionamiento o construcción.

Consejo: Leer correctamente los certificados

Los operadores de la planta necesitan una demostración de la idoneidad de los componentes empleados, preferentemente mediante una declaración de fabricante o un certificado de una organización independiente como TÜV y Exida. No obstante, los certifica-

dos solo indican la idoneidad de los componentes individuales en un circuito de seguridad, pero la arquitectura necesaria a menudo no está clara a primera vista. El ejemplo anterior ha mostrado que con componentes sin función de diagnóstico, SIL 3 solo es posible mediante un circuito redundante. Solo de ese modo se puede compensar el fallo de un componente. Esto está claramente descrito en la IEC 61511, pero a menudo se interpreta erróneamente debido a las formulaciones de palabras en las declaraciones de los fabricantes y los certificados. A esto hay que sumar que hay en circulación certificados que todavía no están estandarizados en cuanto al texto, lo cual puede dar lugar también a malentendidos.

1. Un certificado SIL-4 no es forzosamente el mejor

Cuando se emitieron los primeros certificados SIL para componentes a principios de los años 90, no se incluían todavía todos los grados de riesgo hasta SIL 4. Como consecuencia del elevado riesgo, en la realidad se evita construir piezas de instalaciones que harían necesarios los circuitos de seguridad SIL-4. Simplemente serían demasiado peligrosos para las personas y el medio ambiente y demasiado costosos en la instrumentación de los circuitos SIL con el mantenimiento y la comprobación posteriores. En consecuencia, todavía siguen emitiéndose únicamente certificados con SIL 3. No obstante, todavía hay en circulación certificados SIL-4 emitidos en el pasado. Esto significa que si alguien encuentra certificados hoy que documentan “Estos componentes son adecuados en sistemas hasta SIL 4”, mientras que otro certificado solo establece la idoneidad de SIL 3, puede tratarse realmente del mismo producto. En el segundo caso solo con un certificado actual que deliberadamente ya no considera el SIL 4. En este contexto, debe recordarse que SIL hace referencia al potencial de peligro de una instalación; las medidas de protección que se definan siempre dependen de ello.

2. Un certificado que hace muchas restricciones no es peor

En la actualidad, en el mercado existen diferentes variantes y formulaciones de palabras de certificados que, básicamente, expresan lo mismo. En los certificados más recientes se trata de formular con palabras detalladamente la idoneidad de la aplicación respectiva. “Esto probablemente se convertirá gradualmente en el estándar”, aprecia Schindler. Hasta entonces, habrá en el mercado variantes muy diversas.

Los equipos en la serie de tipos arriba indicada son adecuados para su utilización en sistemas de seguridad hasta SIL 3, inclusive, según IEC 61508.

Ilustración: expresión antigua en el certificado

En su declaración “hasta SIL 3”, este certificado da lugar a confusiones: como se muestra, una válvula individual sin función de diagnóstico solo puede utilizarse hasta SIL 2. SIL 3 solo es posible si se utiliza un circuito redundante. No obstante, el certificado se refiere indirectamente a esto con la nota “conforme a IEC 61511”, porque el estándar define claramente esta relación. Sin embargo, sigue siendo una fuente potencial de conclusiones incorrectas. Además, un componente SIL-2 con una configuración redundante no es automáticamente indicado para circuitos SIL-3. Esta idoneidad se deduce del valor de probabilidad de fallo (valor PFD) indicado en el certificado.

➤ Lo decisivo es que los errores, cuando se producen, se detecten y se puedan iniciarse contramedidas adecuadas. Las normas hacen que esté claramente regulado qué componentes y procesos se requieren para ello. Para alcanzar un Safety Integrity Level 3 se requiere, por ejemplo, una redundancia de las válvulas (“válvula doble”).

Los certificados más recientes son más detallados:

Las válvulas son indicadas para el uso en sistemas de seguridad hasta SIL 2 en modo de baja y alta demanda. Considerando la tolerancia a fallos de hardware mínima requerida $HFT = 1$, pueden utilizarse tanto en ejecución redundante como hasta SIL 3.

Ilustración: nueva expresión inequívoca en el certificado

En comparación con el certificado anterior, el texto “pueden utilizarse en sistemas orientados a la seguridad hasta SIL 2” tiene el efecto de degradar el producto en términos de idoneidad SIL. En rigor, se trata exactamente de la misma declaración: ambas formulaciones de palabras quieren decir lo mismo, aunque la segunda fórmula es más transparente y describe con claridad las posibilidades de uso y el SIL resultante.

3. El certificado no lo dice todo, itenga en cuenta el “Manual de seguridad”!

La frase “Consulte el manual de seguridad” se encuentra en todos los certificados como indicación estándar. Esto es algo más que la referencia acostumbrada para muchos productos a un manual o un folleto de instrucciones. Por lo menos por una razón vale la pena mirar el manual de seguridad: para comparar los valores y los intervalos de comprobación especificados.

Para una mayor uniformidad y una comparabilidad más rápida, en el certificado siempre asume un intervalo de comprobación necesario de un año. Con ello se calcula la probabilidad de fallo. De hecho, hay, por ejemplo, componentes que deben comprobarse con más frecuencia. Sobre todo, también hay productos para los que la comprobación no es necesaria con tanta frecuencia. Especialmente en la industria química, muchos clientes están justificadamente interesados en desconectar sus sistemas lo menos posible para realizar comprobaciones. Un único día improductivo a causa de mantenimiento puede suponer por sí solo para una refinería una pérdida de producción por valor de un millón de euros. Lo determinante es si un componente está certificado para que siga cumpliendo las exigencias SIL en el segundo o el quinto año. La probabilidad de fallo (valor PDF) cambia con el intervalo de comprobación: cuanto más largo es el intervalo de comprobación mayor es la probabilidad de fallo. “El intervalo de comprobación de un año indicado en el certificado también puede contener un valor oculto que puede tener sobre todo efectos económicos. Esto puede ser ventajoso o desventajoso y, por lo tanto, debe considerarse por separado”, afirma Reiner Laun.

Qué dicen y qué no dicen los certificados

Los tres ejemplos ponen de manifiesto que un certificado sirve, entre otras cosas, para unificar estándares y que mediante un certificado los operadores de las instalaciones pueden saber de forma rápida y clara si un componente es adecuado para una determinada función de seguridad en un dispositivo de seguridad PLT (Prozessleittechnik Sicherheitseinrichtung -dispositivo de seguridad en el control de procesos). Sin embargo, en determinadas circunstancias, los componentes certificados por sí solos pueden no ser suficientes para alcanzar el SIL requerido. Según la evaluación de riesgos de la instalación parcial también deberá comprobarse con precisión la arquitectura.

Quienes ignoran este obstáculo podrían incurrir en costes adicionales: si la autoridad comprobadora considera que, a pesar de los componentes certificados, existe un riesgo de seguridad inadmisibles, estos deberán readaptarse. Esto cuesta tiempo y también dinero.

➤ Los certificados proporcionan información sobre si un componente es básicamente adecuado para un determinado SIL. No obstante, pueden darse malentendidos, porque no se mencionen algunos detalles o porque haya en circulación diferentes variantes que expresan lo mismo. Una comprensión del tema ahorra tiempo y dinero.

La ventaja de los componentes duraderos

Es claro que los ciclos de comprobación pueden ser caros. La rentabilidad depende, de manera decisiva, de la fiabilidad de los diferentes elementos de la instalación. Por tanto, los operadores de las plantas quieren componentes que, de ser posible, nunca tengan que comprobarse, ya que las instalaciones modernas a menudo se optimizan en gran medida en términos de tecnología de proceso. Una mayor producción solo es posible si la instalación opera de un modo altamente productivo y funciona de manera fiable de modo que se consigan unos tiempos de inspección o unos tiempos improductivos mínimos. Por ejemplo, válvulas servopilotadas: la humedad o la suciedad provocan en la junta de una válvula envejecimiento y desgaste del mismo modo que la temperatura o el simple uso regular. “Una válvula es un producto finito porque, por ejemplo, las juntas pueden volverse porosas”, comenta Carsten Schindler: “La antigüedad desempeña el papel más decisivo, seguido de las condiciones ambientales. A menudo se utilizan válvulas de corredera que emplean hasta seis juntas. Esto incrementa el riesgo de un efecto stick-slip (efecto de saltos en el avance)”. Pero, ¿qué pasaría si una válvula en la pieza central estuviera completamente sin junta? La serie VOFC de Festo ofrece por ejemplo: una electroválvula con tecnología de válvula de asiento de émbolo, que no requiere una junta dinámica. Esto significa que el envejecimiento debido al desgaste de las juntas se elimina aquí por completo. De este modo, la probabilidad de fallo se reduce enormemente.

No obstante, ¿cómo se adapta la válvula para que pese a la ausencia de una junta blanda exista una hermeticidad equivalente? Esto requiere ingeniería: el asiento de las electroválvulas VOFC está sellado de manera rígida, el poliuretano sustituye a la junta blanda convencional.

En conformidad al ensayo de TÜV Rheinland y la certificación SIL, las electroválvulas VOFC garantizan que con un uso correcto solo se produzca como máximo una conexión incorrecta cada 2.410 conexiones. Asumiendo un caso de necesidad por año, esto supone una única conexión errónea en 2.410 años. En pocas palabras: gracias al principio de construcción es sumamente improbable que la válvula no se desconecte en caso de necesidad.

Ejemplo práctico: Planta Multipropósito de Bayer CropScience

La válvula demuestra su idoneidad de uso, entre otros lugares, en la instalación multipropósito de Bayer en el sitio de Dormagen. Se montó en el año 2002. La empresa agrupa aquí diferentes procesos en un mismo sitio: desde el desarrollo de nuevos principios activos para la protección fitosanitaria, pasando por el tratamiento de laboratorio y la gestión de proyectos, hasta la producción. Por este motivo, las instalaciones y los equipos deben estar conectados y operar de la manera más flexible posible en diferentes configuraciones: secadoras, centrífugas, aparatos de destilación o recipientes de agitador se utilizan en diferente secuencia según la tarea: un total de 67 sistemas de automatización son responsables de esto.

Estos procesos se protegen mediante numerosos dispositivos de seguridad con tecnologías de medición, mando y regulación eléctrica: de este modo, en caso de emergencia, las válvulas dosificadoras, las válvulas de escape o las válvulas de vapor se colocan en posiciones a prueba de fallo. Para que estas válvulas de proceso puedan cerrarse con la suficiente rapidez en caso de emergencia, entre el posicionador y el actuador hay normalmente válvulas servopilotadas que controlan el actuador (véase también a este respecto el capítulo “Normas, reglas y principios”).

En total, Bayer ha montado en la planta multipropósito más de 1,500 de estas válvulas. En los 15 años desde la puesta en marcha de la instalación no se ha producido ningún fallo inseguro en las electroválvulas. Finalmente, en 2015, 14 de las electroválvulas se retiraron de la instalación multiusos y fueron comprobadas minuciosamente por Festo.

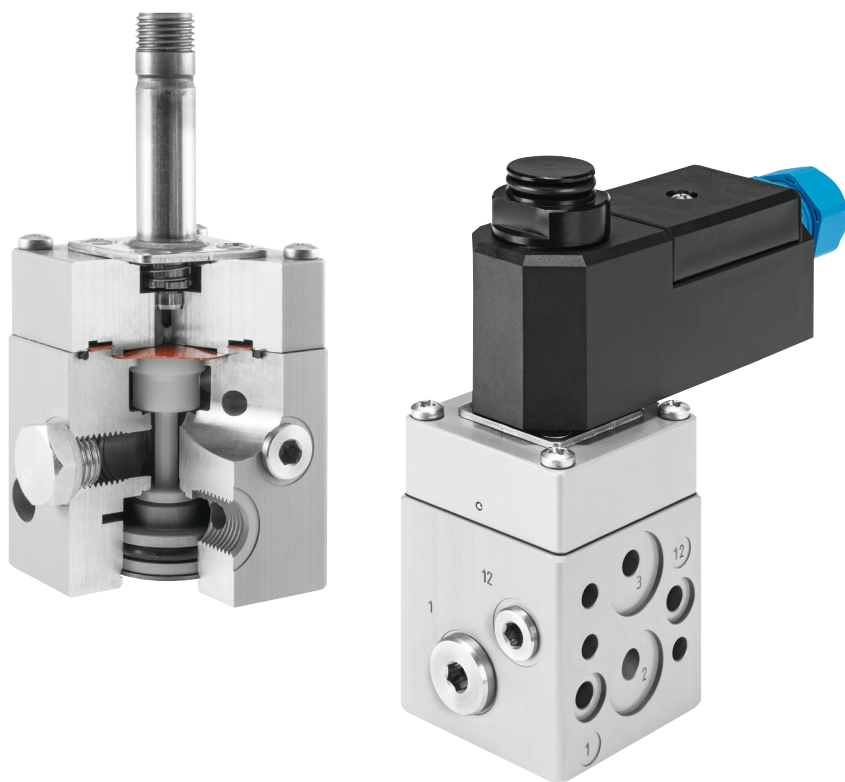


Ilustración: serie de electroválvulas VOFC de Festo

A la vista de los 15 años de funcionamiento probado, una comprobación de laboratorio realizada ya en 1998 y la satisfactoria comprobación sucesiva, TÜV Rheinland emitió un certificado: para la válvula solo se requiere una realización de pruebas cada siete años. No obstante, como es lógico, el explotador es el responsable del montaje, la operación y el mantenimiento correctos y profesionales. Con ello, sin embargo, puede ampliar considerablemente los intervalos de comprobación de las electroválvulas.

Conclusiones

SIL es un tema que puede ser relevante no solo para la seguridad, sino también para los costes: los errores en la planificación y la construcción de un circuito de seguridad pueden llevar a la necesidad de una costosa reconversión. Cualquier comprobación regular o incluso el fallo de un componente puede implicar considerables costes a causa de la pérdida de producción. A este respecto, es particularmente importante prestar la debida consideración a unos componentes duraderos y certificados. Al mismo tiempo, en la misma fase de diseño se debería considerar el sistema al completo y examinarse distintos enfoques de solución.

➤ Los operadores de la planta desean tiempos de inspección o improductivos mínimos. No obstante, componentes como juntas blandas son, en principio, productos finitos. Mediante un desarrollo innovador de componentes es posible desarrollar válvulas que no utilizan juntas blandas y que, por tanto, son más duraderas. Las electroválvulas VOFC de Festo, por ejemplo, funcionan de forma probada y certificada desde hace más de 15 años en una instalación de Bayer.

Publicado por:
Festo AG & Co. KG

process@festo.com
→ www.festo.com/process

Personas de contacto:
Reiner Laun
Reiner.Laun@festo.com

Carsten Schindler
Carsten.Schindler@festo.com