SIS 201

Diseño físico

15 minutos

Generalidades

Así como un sistema de control básico de proceso (BPCS) es más que un controlador, un sistema instrumentado de seguridad (SIS) es más que un PLC de seguridad. Sus componentes físicos principales son sensores, solucionadores lógicos y elementos finales de control.

En este curso se describe por qué estos componentes son considerados esenciales y otros no, así como la manera en que la diferencia puede afectar a sus decisiones de diseño. También veremos dos maneras de establecer que los componentes físicos son adecuados para aplicaciones de seguridad, el papel que juegan las pruebas para garantizar que los componentes funcionarán cuando se necesite, y cómo informar a las personas adecuadas cuando hay una indicación de que los componentes no están funcionando.

A lo largo del curso, estaremos viendo maneras de garantizar que su sistema instrumentado de seguridad cumpla con los requisitos sin que cueste más de lo necesario.

Al final del curso, usted puede usar el examen para confirmar lo que ha aprendido – y ganar valiosos Puntos de Recompensa.

Sugerencia

Preste especial atención a lo siguiente:

- Cómo se puede ahorrar tiempo y dinero al distinguir entre los componentes esenciales y los no esenciales.
- Qué se requiere para usar dispositivos de seguridad no certificados.
- Cómo afecta la probabilidad de falla en demanda (PFD, probabilidad de que el sistema falle cuando se le necesita) a la selección de los componentes
- Efectos potenciales de diferentes frecuencias de pruebas.

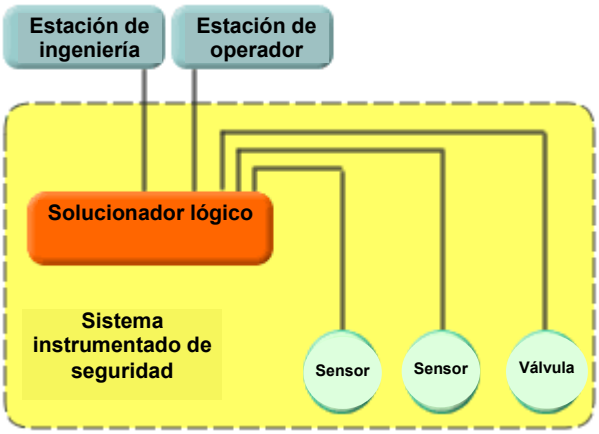
¿Listo(a) para comenzar? Sólo haga clic en el icono “>” a continuación para ir al primer tema.

Componentes y subsistemas esenciales

A menudo, cuando se diseña y se especifica un sistema de control básico de sistema (BPCS), se tiende a comprar tanta funcionalidad y capacidad – las características atractivas – para el BPCS como lo permite el presupuesto.

Sin embargo, cuando se diseña y se especifica un sistema instrumentado de seguridad (SIS) no se habla tanto sobre las características atractivas que sobre los componentes y subsistemas **esenciales** y **no esenciales**. Comprender la diferencia le ayuda a diseñar un sistema con el nivel de integridad de seguridad (SIL) correcto – sin exagerar el diseño de la solución.

Los elementos **esenciales** son los componentes SIS y los elementos asociados necesarios para llevar a cabo la función instrumentada de seguridad – incluyendo sensores, solucionadores lógicos, elementos finales de control, fuentes de alimentación y módulos de E/S. Estos son los elementos que deben cumplir con los requisitos definidos de nivel de integridad de seguridad (SIL).



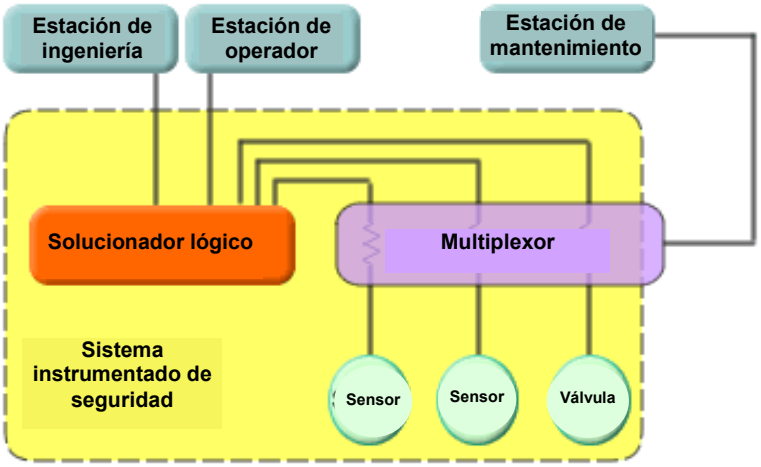
Componentes esenciales – en este ejemplo, los que se encuentran dentro del área amarilla – son los sensores, solucionadores lógicos, elementos finales de control y otro equipo necesario para llevar a cabo la función instrumentada de seguridad.

Componentes y subsistemas no esenciales

Como acabamos de aprender, los componentes y subsistemas SIS **esenciales** son los necesarios para llevar a cabo la función instrumentada de seguridad (SIF).

Los componentes **no esenciales** (conocidos también como "**no interferentes**") proporcionan soporte para diseñar y dar mantenimiento al sistema instrumentado de seguridad, pero su presencia o ausencia no interfiere con el funcionamiento del sistema instrumentado de seguridad. Los ejemplos incluyen estaciones de ingeniería, multiplexores HART, calibradores portátiles y estaciones de mantenimiento.

Aunque tales componentes pueden ***soportar*** la función de seguridad, no la ***ejecutan***. Como resultado, **no** tienen que cumplir con los requisitos de nivel de integridad de seguridad (SIL) – siempre y cuando usted pueda demostrar que éstos no introducir fallas peligrosas en el sistema instrumentado de seguridad.



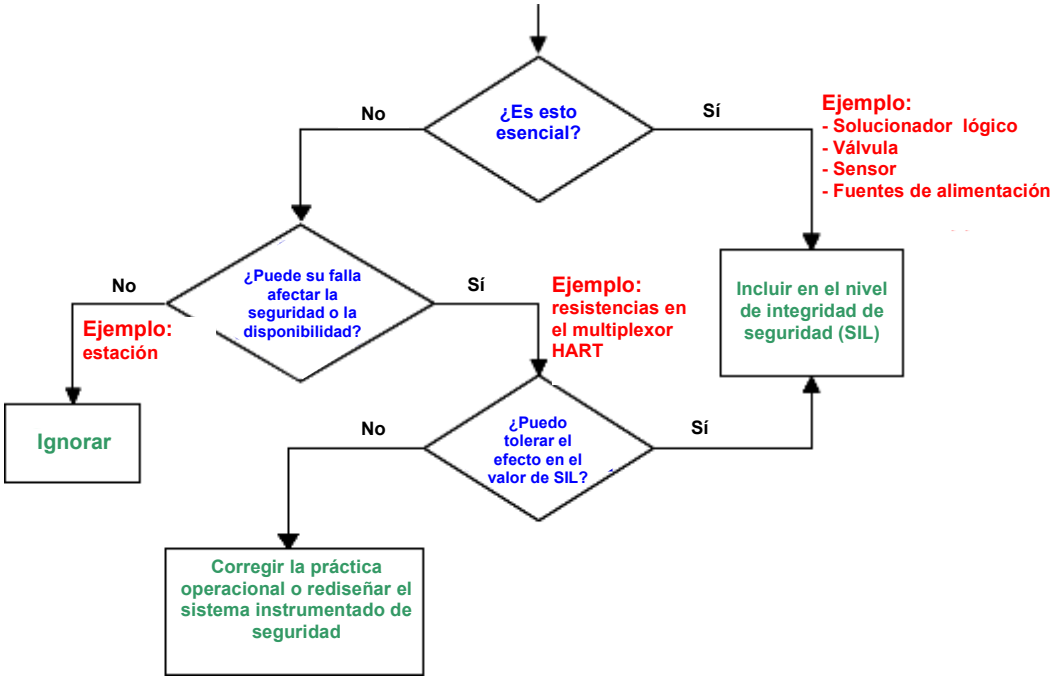
Los componentes no esenciales – como los que se encuentran fuera del área amarilla en este diagrama – no tienen que cumplir con los requisitos de nivel de integridad de seguridad (SIL).

En la mayoría de los casos, tal como en una estación de ingeniería, es obvio que el componente o subsistema no es esencial. Otros pueden ser menos obvios.

Vea otra vez la ilustración anterior. En la práctica, el multiplexor HART incluye un panel de terminales de E/S donde se usan resistencias para extraer la información digital de la señal del sensor de 4-20 mA. Debido a que la señal del sensor no pasa a través de la electrónica del multiplexor para llegar al solucionador lógico, la electrónica del multiplexor no se considera como parte del sistema instrumentado de seguridad, y por lo tanto no tiene que cumplir con los requisitos de nivel de integridad de seguridad. Una falla en las resistencias podría afectar la seguridad, entonces éstas *deben* ser incluidas en los cálculos de nivel de integridad de seguridad.

Usted puede usar el siguiente diagrama para ayudar a determinar si un componente o subsistema es esencial o no.

Haga clic en la imagen para ampliarla.



¿Certificado o comprobado en uso?

Las normas de sistemas de seguridad IEC y ANSI/ISA le proporcionan dos opciones cuando selecciona dispositivos de sistema de seguridad:

- Usar dispositivos que han sido certificados independientemente como conformes con las normas, *o*
- Producir documentación histórica que demuestre que un dispositivo no certificado puede ser usado en un sistema instrumentado de seguridad. Esta opción se llama comúnmente “uso anterior” o “comprobado en uso”.

Veamos cada una de estas opciones con más detalle.

¿Certificado o comprobado en uso?

Certificado

Certificado. Para lograr el estatus certificado, el fabricante del dispositivo lo envía para ser sometido a un amplio análisis por parte de un tercero para verificar que cumpla con IEC 61508. Estos terceros se conocen como organismos certificadores notificados.

La evaluación incluye pruebas y análisis del hardware, software y procesos de ingeniería y fabricación del dispositivo, y busca establecer

- cómo el dispositivo reacciona a una amplia gama de condiciones de falla potenciales
- si el dispositivo produce errores bajo esas condiciones
- si esos errores se pueden detectar en forma rutinaria
- si los errores son seguros o no seguros

Los dispositivos certificados siempre incluyen un *Manual de seguridad* que informa al usuario final cómo instalar, configurar y operar de manera segura el dispositivo certificado. El manual de seguridad también identifica las limitaciones de la funcionalidad del dispositivo – en otras palabras, qué cosa *no* hará. (Por esa razón, un pequeño manual puede ser una indicación de un buen dispositivo.)

Si usted no tiene un historial de uso anterior para el dispositivo funcionando bajo condiciones similares, el use de dispositivos SIS certificados es a menudo la solución con mejor relación costo-beneficio.

La ventaja PlantWeb

El controlador de válvula digital Fisher FIELDVUE DVC6000 de Emerson ha sido certificado por TÜV para usarse en aplicaciones SIL 3, y los transmisores de presión/presión diferencial 3051S y de temperatura 3144P de Rosemount han sido certificados por TÜV para usarse en aplicaciones SIL 2 (aplicaciones SIL 3 cuando se usan en forma redundante).

¿Certificado o comprobado en uso?

Comprobado en uso

Comprobado en uso. Para lograr la aprobación de comprobado en uso, el fabricante del dispositivo debe comprobar que tiene un sistema de calidad o de gestión de cambios para el dispositivo específico. Luego, **usted** tiene que documentar que tiene el mismo dispositivo funcionando bajo condiciones similares a las del sistema instrumentado de seguridad propuesto, tal como con un sistema de control básico del proceso (BPCS).

Además, usted debe documentar el historial de uso y fallas del dispositivo para determinar el tiempo medio entre fallas (TMEF o MTBF –por sus siglas en inglés). Esta documentación debe soportar

- Su declaración de que el dispositivo es capaz de cumplir con los requisitos SIL definidos, *y*
- Los números de probabilidad de falla en demanda (PFD) – descritos en el siguiente tema – que usted usa para calcular el nivel de integridad de seguridad (SIL) del lazo.

El uso anterior documenta el historial del dispositivo bajo condiciones de uso reales. Estas condiciones se deben extender más allá del dispositivo para incluir las conexiones del proceso, los elementos primarios y las prácticas de instalación. Para las plantas que tienen estos datos disponibles, el uso anterior puede a menudo cumplir con los requisitos de seguridad necesarios con una mejor relación costo-beneficio.

Como regla del pulgar, los dispositivos más complejos deben ser certificados. Si un dispositivo es programable, entonces es muy probable que sea complejo.

La ventaja PlantWeb

La colección y mantenimiento de datos de uso anterior puede ser desafiante y costoso. Eso es porque

- Los fabricantes cambian los diseños del producto, que puede impedir que usted confíe en la experiencia de usar un diseño anterior.
- Tradicionalmente, los proveedores no han dado a los usuarios manuales de seguridad que muestren cómo usar adecuadamente los productos en aplicaciones de seguridad y cómo hacerles pruebas de aceptación.
- Es posible que haya pocos o nada de datos de falla de seguridad disponibles sobre el producto.

Para muchos dispositivos de Emerson, sin embargo, Emerson puede ayudar a los usuarios a colectar y gestionar los datos que necesitan para construir su caso de uso anterior, incluyendo

- Efectos de modo de falla y análisis de diagnóstico (FMEDA) para mostrar los modos de falla (peligroso o seguro) y las tasas de falla
- Cálculos de beta para proporcionar probabilidades de falla de causa común
- Manuales de seguridad para proporcionar instrucciones sobre el uso adecuado y procedimientos de pruebas
- Prueba de la gestión de cambios
- Prueba de horas de operación
- Seguimiento en línea de los cambios de hardware y software
- Notificaciones de cambio de hardware y software

Probabilidad de falla cuando se necesita el sistema

Un sistema instrumentado de seguridad no puede ejecutar su función a menos que cada uno de sus componentes funcione adecuadamente cuando se le necesita. Pero la realidad es que *todo* el equipo tiene algún riesgo de falla. (Si no lo tuviera, usted no necesitaría un sistema instrumentado de seguridad, ¿o sí?)

Es por eso que cuando se diseña un sistema, es esencial que se comprenda la tasa de falla de cada uno de los componentes, o **probabilidad promedio de falla en demanda (PFD_{prom}),** para proporcionar un nivel dado de reducción de riesgo. Usted quiere componentes con una probabilidad de falla en demanda (PFD) que sea suficientemente baja para proporcionar el factor de reducción de riesgo correcto (FRR o RRF), pero no tan baja que usted termine con un diseño exagerado (y demasiado costoso).

Consideremos el ejemplo del tanque de amoniaco del curso SIS 101. Suponga que instalamos un sistema diseñado para evitar una ruptura en el tanque, y 1 vez de cada 10 no funciona cuando se necesita (PFD=1/10 ó 0.1). Sin un sistema, el tanque habría sufrido una ruptura 10 veces; con el sistema instalado, sufrirá una ruptura sólo una vez. Por lo tanto, hemos reducido el riesgo en un factor de 10 – y descubrimos que PFD=1/FRR.

Como usted vió en el curso SIS 101, cada nivel de integridad de seguridad (SIL) describe un rango de factores de reducción de riesgo objetivo. Ahora podemos agregar una tercera columna a la tabla que presentamos en ese curso:

Nivel de integridad de seguridad	Factor de reducción de riesgo objetivo	Probabilidad promedio de falla en demanda (PFD_{prom}) objetivo
4	>10,000 a ≤100,000	1/10,000 a 1/100,000
3	>1,000 a ≤10,000	1/1000 a 1/10,000
2	>100 a ≤1,000	1/100 a 1/1000
1	>10 a ≤100	1/10 a 1/100
Adaptado de IEC 61511-1 Tabla 3		

Al conocer el valor de PFD de un dispositivo usted podrá decidir si debe incluirlo en su diseño. ¿Pero qué sucede una vez que el sistema instrumentado de seguridad es operativo?

Pruebas de aceptación

Los componentes esenciales de un sistema instrumentado de seguridad deben ser probados periódicamente para comprobar que funcionarán cuando se necesite – o para descubrir problemas y restaurar el sistema a su funcionalidad de seguridad diseñada.

La frecuencia con la que se deben realizar estas pruebas depende de la probabilidad promedio de falla en demanda (PFD_{prom}) del componente. Entre más frecuentes sean las pruebas, mayor es la seguridad de que el componente funciona bien – lo que significa que la PFD_{prom} es menor y por lo tanto el factor de reducción de riesgo (FRR) es mayor.

La ejecución de una prueba de aceptación de todo el sistema generalmente es posible sólo cuando el proceso está parado. Aunque las pruebas completas del sistema se necesitan periódicamente, usted puede reducir la frecuencia de los paros requeridos conduciendo pruebas provisionales de lo que típicamente se considera mayores factores contribuyentes a la PFD_{prom}: los elementos finales de control.

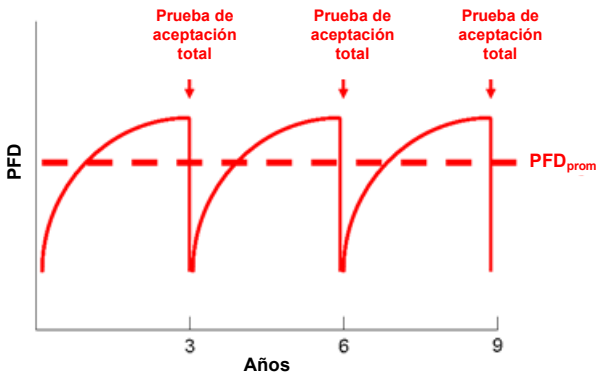
Por lo tanto, para mantener el sistema instrumentado de seguridad en cumplimiento se requiere escoger entre tres opciones:

1. Diseñar el sistema instrumentado de seguridad de manera que no necesite pruebas durante largos períodos entre paros de la planta. Con plantas operando dos, tres o más años entre paros programados, ésta puede ser una opción muy costosa – y podría ser imposible lograrla en la práctica.

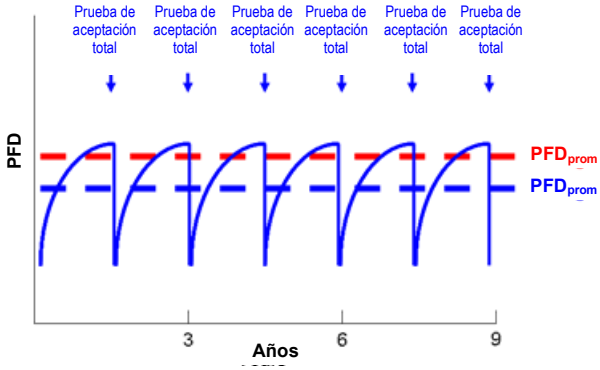
2. Instalar líneas de desviación alrededor de cada elemento final de control para facilitar la prueba de aceptación completa mientras el proceso permanece en operación. Ésta también es una opción costosa, y deja al proceso desprotegido durante los períodos de prueba. También existe el riesgo de que se dejen las líneas de desviación abiertas inadvertidamente después de que se completa la prueba.

3. Usar **pruebas de válvula de carrera parcial** manuales o automatizadas (que no requieren un paro de proceso) para reducir la PFD_{prom}. Los análisis de fiabilidad generalmente muestran que los problemas relacionados con las válvulas, tales como un vástago o tapón atascados, son los mayores contribuyentes a la PFD_{prom} del sistema instrumentado de seguridad total. Una prueba de carrera parcial puede detectar estos problemas – o comprobar que no existen.

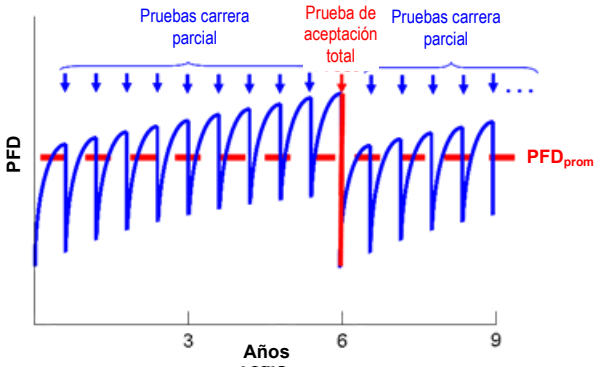
Los siguientes tres diagramas ilustran cómo las pruebas más frecuentes pueden reducir la PFD_{prom} o extender los intervalos entre pruebas de aceptación completas.



La probabilidad de falla en demanda (PFD) se incrementa en el tiempo pero regresa a su nivel original cuando una prueba de aceptación completa muestra que todo funciona correctamente – en este caso, durante un paro cada tres años.



La ejecución de la misma prueba dos veces a menudo reduce la PFD promedio. Como resultado, usted puede usar el mismo equipo para cumplir con un requisito SIL mayor, o puede usar equipo menos costoso para el mismo SIL.



Otro enfoque es ejecutar pruebas de aceptación completas sólo la mitad de la frecuencia, pero usar frecuentes pruebas de carrera parcial para mantener la misma PFD promedio.

Los solucionadores lógicos y controladores de válvula SIS inteligentes pueden trabajar juntos para automatizar las pruebas de carrera parcial, haciendo que sea más fácil y más económico realizar estas pruebas más a menudo. Estas pruebas automatizadas también evitan los riesgos de seguridad asociados cuando se envía a alguien al campo para ejecutar la prueba, y el riesgo de que la válvula de paro de emergencia no esté disponible si se necesita durante la prueba.

Los solucionadores lógicos y controladores de válvula inteligentes también facilita la detección de problemas potenciales al comparar los resultados de la prueba actual con respecto a los de la prueba anterior o cuando se instaló la válvula.

Para aprender más de este tema, vea el informe de Exida "The effects of partial-stroke testing on SIL levels" (Los efectos de las pruebas de carrera parcial sobre los niveles SIL) <http://www.exida.com/articles/Partial%20Valve%20Stroke%20Testing.pdf >

La ventaja PlantWeb

El sistema instrumentado de seguridad inteligente de Emerson está diseñado para **automatizar** las pruebas de carrera parcial, evitando los mayores costos y los riesgos potenciales de las pruebas manuales – incluyendo mayor mano de obra, exposición de los trabajadores a condiciones peligrosas, e incluso la reducción de la seguridad al no seguir los procedimientos adecuados.

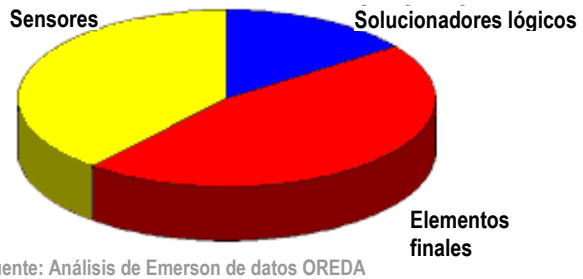
El controlador de válvula digital FIELDVUE, usado en combinación con el software AMS Device Manager, documenta la firma original de la válvula y otros datos, así como el tiempo de prueba de carrera parcial, la fecha y los resultados. El controlador de válvula FIELDVUE también es parte de la solución de actuador de válvula/controlador SIL-PAC disponible para aplicaciones SIS. El solucionador lógico SIS de DeltaV puede automatizar el inicio de la prueba de carrera parcial y colectar los resultados en datos pasa-falla.

Usted también puede reducir la frecuencia de las pruebas de aceptación escogiendo dispositivos con bajas tasas de falla – tales como los transmisores Rosemount y medidores de flujo tipo Coriolis de Micro Motion que también pueden ser componentes clave de nuestro sistema instrumentado de seguridad inteligente.

Diagnósticos

Otra manera de incrementar la fiabilidad de su sistema instrumentado de seguridad es escoger componentes con diagnósticos integrados. Esto es especialmente importante para sensores y elementos finales de control: más del 85% de los problemas que afectan a la operación de un sistema instrumentado de seguridad se relacionan con los dispositivos de campo, no con el solucionador lógico.

Fuentes de fallas en sistemas instrumentados de seguridad



Fuente: Análisis de Emerson de datos OREDA

Los dispositivos que brindan capacidades de diagnóstico usan microprocesadores incorporados en la tarjeta para monitorizar y reportar su propio estado. Algunos pueden incluso predecir problemas potenciales a tiempo para que usted tome la acción correctiva antes de que la seguridad se vea comprometida.

Mientras los dispositivos continúan haciéndose "inteligentes", las capacidades de diagnóstico se pueden extender más allá de su propia condición operativa hacia el proceso circundante. Por ejemplo, si un medidor de flujo simplemente reporta que hay un problema, el personal de mantenimiento podría reemplazarlo – pero eso no eliminaría una condición de slug-flow (densidad fuera de los límites), que es un problema del proceso. Los diagnósticos que le alertan sobre tales condiciones pueden permitirle resolver un problema del proceso antes de que se convierta en un problema de seguridad.

La ventaja PlantWeb

Los dispositivos inteligentes del sistema instrumentado de seguridad inteligente de Emerson brindan una amplia gama de diagnósticos avanzados. Por ejemplo, el controlador de válvula digital DVC6000 SIS puede diagnosticar problemas en el actuador y en la válvula así como en sí mismo. Un transmisor 3144P SIS de Rosemount puede indicar cuando detecta una sonda de temperatura defectuosa. Además, un medidor de flujo inteligente tipo Coriolis de Micro Motion puede detectar condiciones del proceso tales como slug flow, o cambios en la densidad de los reactivos que podría indicar que un catalizador se está contaminando.

Alertas y alarmas inteligentes

Las pruebas de carrera parcial, los diagnósticos y otras tecnologías para identificar (o incluso predecir) problemas en lazos de seguridad pueden ayudar a mantener la PFD_{prom} requerida – pero sólo si la gente adecuada averigua sobre los problemas a tiempo para tomar la acción correctiva.

La detección comienza en el proceso, usando dispositivos inteligentes capaces de monitorizar continuamente la condición operativa de los dispositivos y del lazo. Esto incluye la detección de condiciones tales como una válvula que se pega, baja presión de suministro de aire del actuador o un sensor de temperatura defectuoso.

A quién se debe informar – y cómo – depende de la naturaleza de un problema detectado. Para deterioro gradual que pudiera conducir a un problema en el futuro, un correo electrónico automático al personal de mantenimiento podría permitirles programar las reparaciones adecuadamente. Por el contrario, las situaciones que representan una amenaza en un futuro cercano al proceso o la fiabilidad SIS podrían generar una alarma inmediata para alertar a los operadores para que tomen la acción correctiva.

En todos los casos, es posible que se requiera la creación de un registro del problema en papel para satisfacer los requisitos normativos de informes.

La ventaja PlantWeb

PlantWeb Alerts notifica a la gente adecuada sobre problemas potenciales – sin abrumar a los operadores con alarmas molestas. Esta capacidad es posible gracias a los diagnósticos de los dispositivos de campo inteligentes de Emerson, al software AMS™ Suite: Intelligent Device Manager y al sistema DeltaV™, permite analizar inmediatamente la información entrante, clasificarla de acuerdo a quién se debe avisar, darle prioridad de acuerdo a la gravedad y criticidad en el tiempo, y luego no sólo decir a los destinatarios qué está mal sino aconsejarles sobre qué hacer al respecto – en un lenguaje cotidiano claro.

Con el complemento opcional SIS Reporting Messenger, los resultados detallados de las pruebas de diagnóstico SIS del actuador de carrera parcial, sensor y condición operativa del lazo SIS se transmiten y se imprimen automáticamente.

Sumario

En este curso usted ha aprendido que:

- Los componentes físicos principales de un sistema instrumentado de seguridad son sensores, solucionadores lógicos y elementos finales de control.
- Los componentes y subsistemas esenciales son aquéllos necesarios para llevar a cabo la función instrumentada de seguridad. Éstos deben cumplir con los requisitos de nivel de integridad de seguridad (SIL).
- Los componentes y subsistemas no esenciales proporcionan soporte para diseñar o dar mantenimiento al sistema instrumentado de seguridad, pero no interfieren con su funcionamiento. Éstos *no* tienen que cumplir con los requisitos SIL.
- Los componentes esenciales del sistema instrumentado de seguridad deben ser certificados o comprobados en uso. El mejor enfoque generalmente depende de la complejidad del dispositivo y de si usted tiene suficientes datos de uso anterior.
- La probabilidad de falla en demanda (PFD) de un componente o sistema afecta a su habilidad de proporcionar la reducción de riesgo necesaria y el nivel de integridad de seguridad (SIL).
- Las pruebas de aceptación más frecuentes pueden reducir la PFD, y las pruebas de carrera parcial pueden extender los intervalos entre las pruebas de aceptación completas.
- Las alarmas inteligentes ayudan a informar a la gente correcta cuando hay un problema potencial con el proceso o sistema.