Gestionando Sistemas Instrumentados de Seguridad con Legado

No sería maravilloso trabajar sobre una hoja de papel en blanco? Diseñar una solución desde los primeros bocetos? No sabría, todo el trabajo que he realizado ha sido sobre instalaciones que ya existen. Lo más cerca que estuve a "greenfield" fue expansion.

Para cada proyecto siempre he debido tener en cuenta decisiones tomadas por aquellos que estaban antes que yo. No es diferente al considerar la seguridad funcional – pero aquí uno también debe tener en consideración el cumplimiento de la instalación histórica. El Primer trabajo pudo haberse realizado antes de que la seguridad funcional se hubiese inventado o (como suele suceder) se hubiese comprendido correctamente. Este artículo revisa asuntos y temáticas relacionados con el "legado" de los sistemas de seguridad y sus modificaciones.

Revisando los básicos

No hay manera de escapar de algunos fundamentos. Si estamos operando procesos peligrosos, necesitamos entender cuáles son los peligros potenciales, confirmar que las medidas de reducción del riesgo en sitio hagan de este un riesgo tolerable y poner en sitio sistemas para gestionar y monitorear los mismos sistemas (confirmando que el panorama de riesgos no cambie). No hay manera de evitar esto. No importa si la planta ha estado operando por cuatro o cuarenta años. Estos son bloques de construcción necesarios para la fundación de todo lo siguiente.

Estamos muy acostumbrados a la revalidación de nuestros estudios de riesgo. Es posible que cada cinco años desempolvemos nuestros estudios Hazop y revisemos si existe algo en los P&ID's que podamos haber pasado por alto. Si hemos llevado a cabo nuestras evaluaciones de Seguridad Funcional de etapa 4 (más adelante),

pueden ser un input clave en la revalidación de nuestros estudios de riesgo. Si encontramos algo nuevo, tendremos que actualizar nuestros estudios de determinación SIL, como por ejemplo nuestros LOPA´s. Aquí es donde se hace más complicado – ¿Cuánto crédito puedes tomar por la reducción del riesgo mediante sistemas que fueron instalados hace años (a veces hasta hace décadas) que sabes no cumplen con IEC 61511?

Revisión rápida sobre el cumplimiento de los componentes

IEC 61511 define tres maneras diferentes en las que se puede confirmar que los componentes cumplen con las normativas (y por lo tanto son adecuados para ser utilizados en funciones instrumentadas de seguridad).

- Los fabricantes de productos pueden desarrollar nuevos productos para estar seguros, siguiendo las reglas de gestión y diseño de la seguridad funcional encontrados en IEC 61508 (conocidas como “Route 1” aunque se puede identificar como “seguro por diseño”).
- Los fabricantes de productos pueden recoger datos de retorno sobre productos existentes (retrospectivamente) y confirmar que son lo suficientemente confiables para estar seguros (conocidos como “Route 2” y “Probados en Uso”). Esta demostración debe estar basada en un número suficiente de dispositivos utilizados durante cierta cantidad de años de servicio.
- Los responsables (usuarios finales) pueden recoger datos sobre ensayos de prueba, inspecciones, etc y confirmar que los dispositivos utilizados son lo suficientemente confiables para ser seguros (conocido como” Uso anterior”). De nuevo la demostración debe estar basada sobre dispositivos con los años de servicio suficientes.

Estos son las ÚNICAS formas en las que se puede mostrar que un componente es adecuado para uso en una función de seguridad instrumentada.

Si solo hubiéramos conocido cumplimiento en base a Uso Anterior

Para nuestros sistemas/alarmas de seguridad instalados, si hubiéramos conocido Uso Anterior, habríamos registrado datos en ensayos de prueba, inspecciones, demandas y alarmas falsas. De esta manera habríamos estado construyendo una base de datos que hoy podríamos utilizar para confirmar el desempeño del legado de nuestras alarmas. Si tuviéramos muchos de los mismos dispositivos instalados (de pronto a lo largo de múltiples instalaciones) habríamos podido construir esta data para contar con la suficiente experiencia operativa y cumplir con los niveles estadísticos de confiabilidad definidos en el estándar. Pero típicamente no sabíamos sobre Uso Anterior y no registramos los datos. Incluso si en algún momento existieron, se pudieron haber perdido – especialmente si el negocio fue vendido/comprado a lo largo del tiempo.

Estamos donde estamos

¿Pensando en que probablemente no hemos registrado la data necesaria para demostrar Uso Anterior, que podemos hacer? Hay preguntas fundamentales que debemos contestar si vamos a tomar el crédito por la reducción de riesgo por nuestras alarmas con legado.

Que hace? Una revisión clave para tomar crédito por la reducción de riesgo de cualquier capa de protección es confirmar que en efecto te protege. Resulta que solo puedes confirmar que un sistema te protege si puedes describir lo que hace y luego verificar que lo hace de la manera correcta.

Algunas preguntas para tener en consideración:

- ¿Que está midiendo?
- ¿Cuál es el punto de activación?
- ¿Qué acciones se toman en el punto de activación?
- ¿Qué es actuado para llegar al estado de seguridad?
- ¿Cuál es precisamente el estado de seguridad?
- ¿Qué tan rápido debe actuar?
- ¿Qué acciones secundarias debe ejecutar (activar alarmas, enviar señales al sistema de control)?
- ¿Qué tanto nivel de reducción de riesgo representa? En otras palabras, ¿qué tan confiable es respecto a fallas peligrosas no detectadas?

La primera de estas preguntas "Que hace?" debe quedar registrada en las Especificación de Requisitos de Seguridad (SRS). Es posible/probable que para sistemas de seguridad con legado no exista un documento SRS. Sin importar esto, es útil y valioso escribir un SRS básico que describa las funciones del sistema de seguridad. Esto no quiere decir que será fácil escribirlo – puede no serlo, pero el ejercicio es importante y comúnmente satisfactorio. Trabaje desde los principios – inspeccione el equipo, revise los planos. No se confié en los rumores – lo que el sistema realmente hace puede ser muy diferente a lo que dicen que hace.

Podemos no contar con datos históricos sobre los ensayos de prueba e inspecciones, pero debemos comenzar en algún lugar, utilice cualquier tipo de información que encuentre para llegar a un primer estimado de la confiabilidad del sistema de seguridad. Recuerde que estamos interesados en la tasa de fallas peligrosas no detectadas (una tasa de falla que incluimos en los cálculos). No estamos revisando la confiabilidad general, solo lo que causaría que el sistema fallara sin que lo supiéramos – si nos encontráramos en una demanda solo sabríamos que el sistema era defectuoso porque no nos protegía. Puede existir data de confiabilidad del proveedor Y existen varias bases de datos "genéricas" que pueden ser útiles. Recuerde que este solo es un estimado inicial. No es suficiente, debemos trabajar para que sea suficiente incluyendo recolección de datos nuevos y su monitoreo.

Comience a recolectar datos ya

Es común para nosotros contar con tan pocos dispositivos que nunca construiremos una confianza estadística significativa sobre la confiabilidad de nuestra data. Sin importar esto, es importante realizar el viaje, aunque no se llegue al destino. Registre y analice la data relacionada con el desempeño de los sistemas.

- Ensayos de Prueba: Esto nos suministra información sobre fallas peligrosas no detectadas. El área clave de enfoque cuando hablamos de confiabilidad en los sistemas.
- Inspecciones: normalmente detectaremos fallas sistemáticas, como el remplazo de dispositivos fallidos por alternativas no aprobadas (no podemos establecer confiabilidad sobre un componente si no lo remplazamos por el mismo)
- Demandas: Nos indican si nuestro sistema funciona "en el mundo real". El número de demandas es un KPI importante. Si contamos con más demandas de las esperadas, algo no está bien. De pronto la frecuencia del evento iniciador esta disparada, de pronto tenemos eventos iniciadores que no identificamos en el Hazop, es posible que nuestras otras medidas de reducción del riesgo no estén trabajando como deberían. Debemos evaluar todos estos aspectos.
- Alarmas engañosas, a cierto nivel no nos importa que la alarma de seguridad sea más entusiasta de lo que debería. Sin embargo, si nuestro sistema de seguridad continuamente distrae a los operadores de producción y encuentra formas de evadir los bypass, a un alto nivel esto se puede convertir en comportamiento inseguro.

Si vamos a tomar crédito por las alarmas de seguridad como una función de seguridad instrumentada, entonces debemos implementar un régimen de ensayos de prueba. Ahora que contamos con un SRS básico que describe lo que el SIF debe hacer, podemos diseñar un ensayo de prueba adecuado. Si la alarma no incluye canales redundantes, una prueba de extremo a extremo (tratando el SIF como una caja negra) puede ser suficiente. Si existen canales redundantes, las cosas serán más complejas.

No olvide que, así como debe probar las operaciones de la alarma, también debe realizar pruebas sobre acciones secundarias (configuración de alarmas).

Si necesita una reducción de riesgo mayor

Uno de los resultados de este trabajo puede ser que descubra que sus sistemas de seguridad no cierran la brecha de reducción del riesgo. En 61508 existe una clausula que puede serle útil. En vez de remplazar el sistema existente (que puede venir trabajando durante muchos años), considere añadir funciones instrumentadas de seguridad adicionales. La cláusula 7.4.3 “Síntesis de elementos para lograr la capacidad sistemática requerida” en IEC 61508-2 es un worth read – esencialmente describe como SIL 1+ SIL 1 = SIL2 mientras usted tenga diversidad (que casi siempre será el caso cuando agregue nueva instrumentación a un sistema con legado).

Gestión y Evaluación de Seguridad Funcional

Ya que estamos realizando trabajo cubierto por todo el ciclo de vida de la seguridad funcional, hemos seguido los principios de gestión de la seguridad funcional. A cierto nivel esto puede ser considerado simplemente como una buena práctica de ingeniería: Tener un plan, contar con personas competentes, realizar revisiones cuidadosas, guardar un buen registro de documentación – no debe ser oneroso. Adicionalmente deberíamos realizar evaluaciones de seguridad funcional (FSA), el alcance de la etapa 4 de FSA son operaciones y mantenimiento – así que esto cubre la gestión de los sistemas instrumentados de seguridad, con legado o recientes. La etapa 4 de FSA examinará todos los aspectos de la gestión SIF que ha mencionado este documento, junto a la implementación de una Gestión de Seguridad Funcional. Resaltará todas las áreas de no cumplimiento, que junto al monitoreo del desempeño de SIF proporcionaran un panorama más claro de donde no está cumpliendo.

Hoy es el primer día del resto de nuestras vidas.

Normalmente podemos tener el pensamiento de “Yo no habría comenzado por ahí”, pero la historia no puede cambiarse sino solo el futuro. Para todas nuestras funciones instrumentadas de seguridad, con legado, recientemente instaladas, debemos poner los básicos en sitio. Conozca los peligros, conozca la reducción del riesgo necesaria, describa el SIF, revise que el SIF lo proteja y sea lo suficientemente confiable y registre datos para analizar el desempeño. Siga los pasos de la Gestión de Seguridad Funcional y lleve a cabo de manera regular evaluaciones de seguridad funcional. El futuro puede ser mejor que el pasado.

[Puede consultar información sobre referencias y el autor en el documento original en ingles en la revista hazardex de marzo.]