SIS 303

Decomisionamiento

15 minutos

Generalidades

Se puede pensar que el decomisionamiento de un sistema instrumentado de seguridad es un tipo especial de modificación, lo que significa que se deben considerar todos los requisitos que describimos en el curso SIS 302.

Sin embargo, las modificaciones típicas descritas en ese curso tienden a ser pequeñas, y a mantener o incluso incrementar la seguridad. Por otro lado, cuando decomisionamos un sistema instrumentado de seguridad **quitamos capas de protección** – desde una función de seguridad hasta todo el sistema de seguridad. Por lo tanto, necesitamos garantizar que lo que quede sea

- Adecuado para proteger contra los peligros restantes
- No alterado (degradado) por el hardware y software que hemos quitado
- Todavía configurado eficazmente, sin capas confusas de código “muerto”

Este curso proporciona consejos sobre cómo hacer eso. Al final usted encontrará un breve examen para ayudarle a evaluar lo que ha aprendido.

Sugerencia

Mientras estudia los temas de este curso, preste especial atención a lo siguiente…

- Las diferencias entre el comisionamiento total y el parcial
- Qué debe incluir el plan de decomisionamiento
- Buenas y malas prácticas para decomisionar el software
- Los roles de las pruebas, validación y documentación.

¿Listo(a) para comenzar? Haga clic en el icono ">" a continuación para ir al primer tema.

¿Total o parcial?

El decomisionamiento de un sistema instrumentado de seguridad puede ser **total** o **parcial**.

El **decomisionamiento total** ocurre cuando ya no se necesita la protección proporcionada por el sistema instrumentado de seguridad – generalmente porque ya no se usa el proceso para el que fue diseñado este sistema.

En este caso, el decomisionamiento es relativamente directo: Se para la planta y se quita el sistema instrumentado de seguridad. Todavía puede haber peligros para el personal, tales como los de químicos desagradables, pero los peligros del proceso ya no están porque no hay proceso.

El **decomisionamiento parcial** puede ocurrir cuando las modificaciones del proceso – por ejemplo, el cambio a un aditivo menos peligroso o la eliminación de una reacción exotérmica – reducen el número de funciones de seguridad que debe proporcionar el sistema instrumentado de seguridad.

Para esta situación, el decomisionamiento involucra quitar los sensores SIS, los elementos finales de control, los solucionadores lógicos y el software que ya no se necesitan ***sin*** afectar los componentes que todavía se requieren para proteger contra los peligros restantes.

Para asegurarse de que usted quite las piezas correctas – y ***sólo*** las piezas correctas – se requiere una planificación cuidadosa.

Plan de decomisionamiento

Antes de que comience el decomisionamiento, la norma IEC 61511 requiere que individuos calificados trabajen juntos para desarrollar, evaluar y aprobar un plan completo de decomisionamiento. El plan debe incluir:

- Quién identificará, supervisará, conducirá y aprobará las actividades e hitos del decomisionamiento, y cómo lo harán

- Cómo se evaluará la seguridad funcional restante del sistema instrumentado de seguridad, incluyendo una revisión actualizada de las evaluaciones de peligros y riesgos asociados

- Cómo se mantendrá la seguridad funcional si las actividades de decomisionamiento deben ocurrir mientras el proceso permanece en funcionamiento

- Cómo el decomisionamiento de una unidad física afecta a las unidades adyacentes que están en operación y a los servicios del establecimiento y públicos.

El plan también debe incluir una detallada referencia cruzada a la documentación de la especificación de requisitos de seguridad (SRS), identificando cuáles párrafos y otra documentación son afectados por el decomisionamiento.

En breve, la planificación del decomisionamiento debe incluir la misma atención a los detalles que el diseño original del sistema instrumentado de seguridad y que cualquier modificación.

Problemas de software

Los criterios y procedimientos para retener o quitar sensores y elementos finales de control son muy directos. El decomisionamiento de software es más complejo debido a que las interrelaciones entre las diferentes partes de código pueden ser menos aparentes.

Sin código muerto. Un error común que se comete con el software que no se necesita es ponerlo como comentario o ramificarlo dentro del código bajo el disfraz de que "podríamos necesitarlo en el futuro". En lugar de eso, se debe quitar el código que no se necesita y/o se debe reconstruir.

A los auditores de software no les gusta – y cuando se trata de software de sistemas instrumentados de seguridad, no tolerarán – lo que generalmente se conoce como "código muerto" que resida en el solucionador lógico. Además de complicar las auditorías de la funcionalidad de seguridad, el código muerto proporciona más oportunidades para fallas sistemáticas. Si el software no está ahí, no puede fallar ni interferir con la función de seguridad. Tampoco se necesitará tiempo del procesador para explorarlo y ejecutarlo, ni memoria para almacenarlo.

De manera similar, el uso de entradas falsas o virtuales se considera una mala práctica de software. Por ejemplo, si un elemento **AND** incluye una entrada que ahora está decomisionada, resista la tentación de reemplazar la entrada con un valor de registro. En lugar de eso, reconstruya el elemento **AND** con el número adecuado de entradas requeridas para satisfacer la lógica restante del sistema instrumentado de seguridad.

"¿Qué hace esto?" Aunque usted no debe dejar código viejo en el sistema, también debe asegurarse de no quitar funcionalidad que todavía se necesite en el sistema instrumentado de seguridad. Frecuentemente se preguntará, "¿Qué tal si lo que estoy a punto de hacer impide que el sistema instrumentado de seguridad funcione como debe?"

Esta pregunta es mucho más sencilla de responder cuando usted tiene la documentación de que hemos estado hablando en todos los cursos – desde las especificaciones iniciales de requisitos y de diseño hasta los registros detallados de cualquier modificación. Sin ella, usted tendrá que separar el código y analizarlo para averiguar su funcionamiento o, lo que es peor, adivinar el propósito de cada línea.

La documentación clara, concisa y completa facilita el trabajo, y lo hace más rápido y más seguro. Todas esas horas que invierta en el diseño, implementación y documentación del software le pagarán grandes dividendos al poder decomisionar con confianza una parte del software.

La ventaja PlantWeb

El sistema instrumentado de seguridad de DeltaV almacena y ejecuta cada función instrumentada de seguridad (SIF) en un módulo de software separado y autocontenido. Para decomisionar una función instrumentada de seguridad (SIF), usted simplemente quita ese módulo individual – sin que haya impacto en las otras funciones instrumentadas de seguridad.

La característica Version Control and Audit Tracking (control de versión y seguimiento de auditoría) de DeltaV registra automáticamente el cambio, y así la documentación también es fácil.

Pruebas

Las pruebas son tan importantes para el decomisionamiento como lo fueron para las etapas anteriores del ciclo de vida del sistema instrumentado de seguridad.

Las personas que desarrollan el plan de decomisionamiento deben revisar los planes de pruebas usados para comisionar originalmente el sistema instrumentado de seguridad, modificarlos según sea necesario y crear nuevos cuando sea necesario – todo con la intención de garantizar que no se comprometa la seguridad funcional proporcionada por el sistema instrumentado de seguridad restante.

Si se realiza el decomisionamiento del sistema instrumentado de seguridad mientras el proceso permanece en operación, también puede necesitar planes de pruebas intermedias. Por ejemplo, si las actividades de decomisionamiento ocurren sólo durante el turno de día y el sistema instrumentado de seguridad proporcionará seguridad funcional durante el segundo y tercer turnos, se requerirán pruebas intermedias para garantizar que se vuelva a comisionar el sistema instrumentado de seguridad para cubrir los turnos segundo y tercero.

Revalidación

Como aprendimos en el curso SIS 203, la validación es una actividad que demuestra que el sistema instrumentado de seguridad funciona como fue diseñado. Involucra una completa prueba de entradas/salidas diseñada para brindar una solución SIS que cumpla con la norma IEC 61511.

Una vez que estén completas las actividades de decomisionamiento parcial, se debe volver a validar cualquier función de seguridad que permanezca que pudiera haber sido afectada por el trabajo. Con algunos sistemas se tendría que repetir la validación de seguridad funcional completa.

Documentación

No debe ser sorpresa que todas las actividades de decomisionamiento necesitan ser documentadas de acuerdo a los mismos altos estándares que el otro trabajo que se hizo en el sistema instrumentado de seguridad.

También hemos visto qué tan importante puede ser la documentación previa para el trabajo de decomisionamiento. Cuando la documentación actual refleja realmente el

estado del sistema instrumentado de seguridad actual, la confianza en el plan de decomisionamiento se eleva.

Por el contrario, si la documentación del sistema instrumentado de seguridad no es actual, entonces se debe posponer el desarrollo del plan de decomisionamiento hasta que se pueda realizar una completa auditoría del sistema instrumentado de seguridad y que toda la documentación refleje el estado “como se construyó”.

Sumario

El comisionamiento del sistema instrumentado de seguridad requiere el mismo nivel de planificación cuidadosa y atención a los detalles que cualquier otras etapa del ciclo de vida de seguridad, por la misma razón: los errores pueden costar vidas. En este curso hemos aprendido que:

- La meta más importante del decomisionamiento de un sistema instrumentado de seguridad – especialmente el decomisionamiento parcial – es garantizar la protección adecuada contra cualquier peligro que permanezca en el proceso.

- La norma IEC 61511 requiere un completo plan de decomisionamiento aprobado antes de que empiece el trabajo.

- Al decomisionar software de un sistema instrumentado de seguridad, se necesita cuidado especial para quitar exactamente el código adecuado – dejando ni demasiado ni muy poco para que el sistema instrumentado de seguridad funcione como debe.

- Las pruebas y la validación son tan importantes para el decomisionamiento de un sistema instrumentado de seguridad como lo fueron para poner el sistema en servicio.

- La buena documentación no sólo se requiere; sino que también facilita el decomisionamiento.