Comparación entre sistemas instrumentados de seguridad convencionales y sostenibles

Un sistema instrumentado de seguridad (SIS) sostenible es más abierto que uno convencional y más accesible para el personal de una planta de proceso, a la vez que brinda oportunidades para la realimentación y la mejora continua.

Por Hidehito Shiratsu
Yokogawa
www.yokogawa.com

Sobre el autor

Hidehito Shiratsu es especialista en márketing de sistemas de seguridad y control integrados (ICSS) en *Yokogawa Electric Corporation*, responsable del negocio de sistemas de control de seguridad y planificación de producto. Antes, estuvo a cargo del desarrollo y planificación de controladores lógicos programables (PLC) y de sistemas operativos en tiempo real (RTOS). Shiratsu cuenta con una licenciatura en Ingeniería Electrónica.

Nota del editor. La traducción del documento estuvo a cargo de la redacción de AADECA Revista, especialmente para este número.

Un sistema instrumentado de seguridad (SIS) convencional para una planta de proceso en general consiste en un conjunto de cajas negras de software, accesible solo para un número limitado de personal altamente especializado y técnico. Un SIS sostenible con gestión de seguridad funcional (FSM) y monitoreo de desempeño integrados es igual de capaz para ejecutar estrategias de seguridad de planta, pero es mucho más accesible para que lo opere y entienda un rango más amplio de personal, incluyendo los operadores de la sala de control.

Esto conduce a mejoramiento general de la seguridad del proceso y a mantener la integridad del SIS a través de todo el ciclo de vida de la planta. A la vez, se lleva a cabo de manera automática captando las fallas y demandas del proceso, y analizándolas en contraste con los indicadores de desempeño de la seguridad (SPI), como se muestra en la figura 1, que indica el desempeño de la seguridad de forma continua a través de todo el ciclo de vida de la planta.

Quienes comercializan componentes de seguridad e instrumentación, que reconocen las limitaciones de un SIS convencional, utilizan varios métodos para automatizar la recopilación de datos y las funciones de análisis para crear un SIS sostenible.

Elementos SIS sostenibles

Un SIS sostenible provee un acercamiento holístico y permite que los usuarios recuperen la posesión del entorno de seguridad del proceso, puesto que se hace comprensible, manejable, compatible

y seguro, lo que permite que la planta de procesos se focalice en su negocio principal.

Un SIS sostenible ayuda a alcanzar un nivel óptimo de seguridad de planta y provee paz mental durante la realización del proyecto y las fases operacionales. Un SIS sostenible consiste en gran cantidad de elementos diseñados para mejorar la seguridad en el piso de planta, incluyendo una solución que asegura la aplicación de la seguridad, una solución de monitoreo del desempeño de la seguridad y un solucionador lógico de seguridad (figura 2).

- Solución que asegura la aplicación de la seguridad. Permite que la aplicación de seguridad se pueda mantener fácilmente en el nivel requerido a través de todo el ciclo de vida de la planta de acuerdo a los estándares de seguridad funcional IEC 61508 "Seguridad funcional" e IEC 61522 "Sistemas instrumentados de seguridad para el sector de la industria de procesos".
- Solución de monitoreo del desempeño de la seguridad. Provee los SPI para un SIS y otras capas de protección independientes conectadas al sistema de control distribuido (DCS). Además, satisface los estándares actuales de seguridad, que periódicamente requieren evaluar el desempeño de seguridad real de un proceso respecto del objetivo de desempeño diseñado, y verificar la seguridad de planta cuando se saltea la función de seguridad.
- Solucionador lógico de seguridad. Detecta los peligros en el equipamiento de seguridad. Por ejemplo, *TÜV Rheinland* puede certificar algunos solucionadores lógicos de seguridad hasta funciones de seguridad con un nivel 3 de integridad (SIL 3), de acuerdo a IEC 61508, o Exida, para el nivel de ciberseguridad 1 de EDSA ISASecure.

Figura 1.

Cuestiones de SIS convencional para el personal de planta

Un SIS convencional requiere que el personal de planta realice trabajo laborioso para mantener la integridad de la seguridad a través de todo el ciclo de vida de la planta. Otros desafíos y cuestiones del SIS convencional incluyen:

- El personal de mantenimiento de planta encuentra barreras para entender el SIS debido a la baja visibilidad de implementación
- Quizá haya brechas entre la especificación del requisito de seguridad y la lógica implementada, lo que genera desafíos cuando se analiza el desempeño de los sistemas de seguridad durante la fase operacional de la planta.
- Se requiere entrenamiento extensivo para comprender cómo opera un SIS convencional.

- La falta de transparencia dificulta que una gran cantidad del personal comprenda los objetivos de diseño del SIS y se recupere de forma eficiente de los incidentes. Generar y analizar manualmente los reportes de estado es una tarea que consume tiempo puesto que la interpretación de los datos crudos es una labor intensiva.
- Los reportes de estado de un SIS convencional registran los eventos pasados y las alarmas en un formato que no es amigable con el usuario o que se pueda elaborar de forma sencilla para su interpretación.
- La cantidad de datos para analizar aumenta con el tiempo, y en casos en los que la data se debe almacenar a través de todo el ciclo de vida de la planta por cuestiones de auditorías, la gestión y almacenamiento de esos datos se convierte en un desafío mayor.

Gestionar un SIS convencional es engorroso. El personal de mantenimiento de planta a veces considera que SIS convencional no refleja el estado real de SIS de forma precisa debido a cambios inapropiados en la documentación y/o procedimientos de devolución incompletos. Documentar los cambios y satisfacer FSM en general es un proceso manual, lo que dificulta hacer el seguimiento cronológico y compilar las modificaciones. Estos procesos manuales para tratar con las modificaciones y gestionar FSM con un SIS convencional no son sostenibles en entornos complejos.

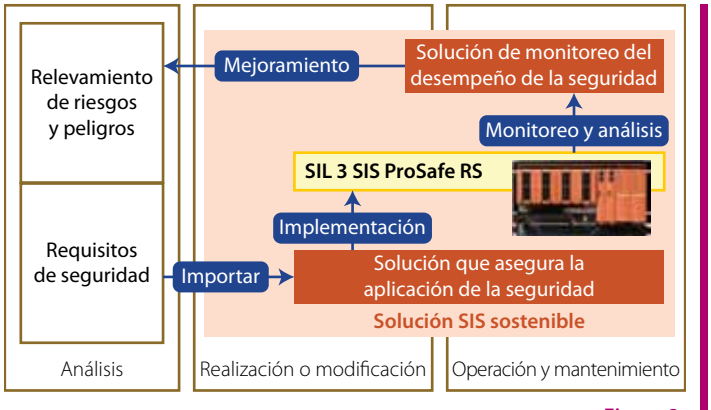

Figura 2.

Ventajas de un SIS sostenible para el personal de planta

Un SIS sostenible implica un mejor proceso ya que atiende todos los problemas que se encontraban utilizando SIS convencional. Un SIS sostenible implica automatización para gestionar aplicaciones de seguridad y datos de proceso.

Un SIS sostenible cuenta con interfaces más accesibles y amigables con el usuario que puede comprender, configurar y gestionar un amplio rango del personal —por lo tanto, reduce la dependencia de un reducido grupo de ingenieros entrenados—. Las características clave son la visualización mejorada del comportamiento del proceso en caso de falla (figura 3), análisis automatizado y acciones de mitigación del riesgo. La posibilidad de simulaciones fuera de línea de SIS sostenible permite verificar las funciones de seguridad antes de activarlo, permitiendo que los operadores (o diseñadores) de SIS verifiquen el diseño, y comprendan las consecuencias que surjan de la mayoría de las funciones instrumentadas de seguridad (SIF).

Un SIS sostenible recolecta automáticamente las estadísticas de seguridad para facilitar el mejoramiento de SIF, también captura y graba automáticamente la evidencia requerida del desempeño de seguridad y la disponibilidad SIF, para la auditoría de parte de las autoridades de regulación. El SIS sostenible, dado que permite la mejora continua de las características de seguridad de la planta a través de una optimización dinámica de SIF, analiza las diferencias entre los SPI medidos y los esperados.

Un sistema de gestión de base de datos digitalizada asegura actualizaciones consistentes documentadas y sincronizadas. Esta forma de gestión

automatizada del cambio ayuda a lograr la consistencia general de la información del sistema de seguridad y permite la ejecución tranquila de proyecto. El acceso sencillo al historial del registro de seguridad simplifica los procesos de auditoría. Poder rastrear, identificar y restringir los cambios no-autorizados en el SIS es crítico para mitigar las amenazas de ciberseguridad.

Mejorar la seguridad de planta con SIS sostenible

Un SIS sostenible representa funciones de seguridad de proceso con la forma de documentos de diseño, matrices de causa y efecto y diagramas de estado/transición. Hace que la funcionalidad sea más fácil de entender para todos los departamentos de modo que los ingenieros de proceso, mantenimiento, operadores, pueden asistir a los ingenieros de aplicación, dando soporte y solucionando problemas de forma interactiva.

Los documentos de diseño se pueden simular de forma dinámica, lo que permite que los diseños y las modificaciones se puedan testear a fondo con una simulación fuera de línea antes de su activación. Además, un SIS sostenible ayuda a conocer el impacto de aplicar excepciones en la función de seguridad antes de que sean implementadas, incluyendo cualquier impacto que pudiera haber sufrido en otro equipamiento. Un SIS sostenible mejora la visibilidad de situaciones de peligro potenciales e incrementa la seguridad gracias a que refuerza la norma y la trazabilidad.

Un SIS sostenible recolecta automáticamente las estadísticas de seguridad para las mejoras de SIF, y graba la evidencia del desempeño de seguridad y la disponibilidad de SIF para la auditoría de parte de autoridades regulatorias. El desempeño de la seguridad del diseño se compara con el su desempeño real para resaltar los problemas, validar el diseño, optimizar la agenda de pruebas, y

Figure 3. Visualización mejorada del comportamiento del proceso en caso de falla

ayudar a los usuarios a mejorar la disponibilidad y seguridad de la planta.

Toda la información de SIS se graba en la base de datos de SIS sostenible, lo que hace posible que sea sencillo recuperar el historial de actividades relacionadas con la ingeniería y los cambios que se hayan implementado. Los últimos documentos de diseño se pueden generar automáticamente en cualquier momento para asegurar que no haya inconsistencias en la aplicación que se está implementando. Las modificaciones se pueden idear sobre la base de un documento de diseño sin ningún recelo.

Un SIS sostenible simplifica el diseño, operación y mantenimiento de los sistemas de seguridad de planta. Este concepto y sus elementos de software asociados se pueden aplicar a los diseños nuevos y a los ya existentes.

Algunas plantas de proceso existentes quizá cuenten con un equipo disponible para implementar un SIS sostenible, mientras que otras quizá requieran asistencia desde el diseño inicial hasta su implementación, incluyendo soporte durante toda la vida del SIS sostenible. ❖