LA VISION DE INGENIERIA DE PROCESO SOBRE AUTOMATIZACION SEGURA

Angela E. Summers, SIS-TECH Solutions, LP

Publicado en Chemical Engineering Progress, December 2008.

Este procedimiento paso a paso aplica Sistemas Instrumentados de Seguridad (SIS) para reducir los riesgos del proceso continuamente.

Balancear las inversiones en producción y seguridad puede ser retador. Cuando los proyectos de mejoramiento de la producción son ejecutados, el retorno de la inversión puede ser verificado numéricamente en tiempo real con relativa certeza.

En contraste, proyectos de seguridad buscan prevenir un evento, como una lesión, y no producen nada que pueda ser medido en tiempo real. En una planta bien operada y manejada, eventos de peligro significativos ocurren tan infrecuentemente que virtualmente el impacto en la data de la tendencia de la operación del proceso es insignificante. Peor aun, la tendencia impactada no proporciona oportunidad de corrección antes del evento. Cuando las tendencias pueden ser detectadas, los problemas sistemáticos son, por lo general, extensos y se ramifican profundamente dentro de la organización.

Algunos beneficios de seguridad pueden ser medidos, pero muchos solo informan el impacto en principales indicadores de rendimiento con poco reconocimiento en elementos de prevención de perdidas. Ahorros en prevención de pérdidas necesitan ser rastreados para demostrar el retorno de la inversión.

Suficiente teoría y estándares existen para asegurar que los equipos de proceso pueden ser operados con seguridad. El riesgo puede ser manejado exitosamente a lo largo de la existencia del proceso usando sistemas de seguridad que demuestran satisfacer los requerimientos de documentación. Un sistema gerencial de calidad se requiere para sostener la integridad del sistema de seguridad; de otro modo, incidentes pueden ocurrir cuando se acumulan suficientes condiciones latentes. Una propuesta proactiva utiliza mediciones para rastrear los comportamientos, errores y fallas que son precursores a eventos peligros (1).

Los Sistemas Instrumentados de Seguridad (SIS) son comúnmente usados para lograr o mantener el estado seguro de los procesos cuando ocurren condiciones anormales de operación. A través de los años, muchos términos se han usado para describir los tipos o clases de SISs para facilitar un entendimiento más rápido del propósito del sistema (Figura 1). En algunos casos, las prácticas industriales dictan los requerimientos para clases o aplicaciones específicas.

ANSI/ISA Standard 84.00.01-2004, “Seguridad Funcional: Sistemas Instrumentados de Seguridad para el Sector Industrial de Procesos (o simplemente ISA 84.01) (2) utiliza el término Sistemas Instrumentados de Seguridad (SIS) para un ISS diseñado para ser independiente y separado del sistema de control del proceso básico (BPCS) para proporcionar protección contra anomalías generadas en los

sistemas de control. La reducción de riesgo requerida del SIS determina su objetivo del Nivel de Integridad Seguro (SIL), el cual es un punto de referencia basado en la probabilidad de falla en demanda (PFD):

- SIL 1: 0.01 < PFD < 0.1
- SIL 2: 0.001 < PFD < 0.01
- SIL 3: 0.0001 < PFD < 0.001

Para ser clasificado como un sistema que cumple con un SIL especifico, el SIS debe ser diseñado y manejado bajo un sistema gerencial de calidad que perdure durante el tiempo de la vida útil del equipo. Este artículo describe como ISSs y SISs son implementados como parte de una estrategia exitosa de reducción de riesgo.

1. Definir de una estrategia de reducción de riego.

El Ingeniero de Proceso tiene una responsabilidad absoluta por la operación de seguridad de las plantas. Entre más pronto se defina la estrategia de reducción de riesgo, mejor funcionará y menos costará. Identifique los peligros del procesos en la fase inicial del diseño del proceso, para que las medidas puedan ser implementadas con el fin de reducir o eliminar peligros a través de diseños inherentemente más seguros (3).

Una vez que el diseño del proceso sea completado, el riesgo restante necesitara ser manejado por el tiempo de vida del equipo del proceso. Aunque diseños inherentemente más seguros podrían incrementar el costo de capital inicial, los mismos reducen substancialmente los riegos a largo plazo. Sistemas de seguridad deben ser implementados únicamente cuando los diseños inherentemente más seguros llegan a ser poco prácticos, debido a que equipos de seguridad requieren inversión a largo plazo en actividades administrativas, operativas e integridad mecánica.

Para desarrollar la estrategia de reducción de riesgo, comience con un Análisis de Peligros del Proceso (PHA) y revise el diseño del proceso y su control, operación y prácticas de mantenimiento. Seleccione un grupo multidisciplinario de personas con experiencia en estas áreas, y use un procedimiento aceptado de evaluación de peligros (4), tal y como operabilidad y peligro (HAZOP), “what-if”, ó un análisis de lista de chequeo, para determinar cómo las desviaciones en la operación deseada del proceso conllevan a los peligros del proceso.

Identifique las causas o condiciones que conllevan a estas desviaciones. Por ejemplo, un bajo flujo puede ser causado por falla del lazo de control de flujo. Eventos pueden ser causados por una falla sencilla o por múltiples fallas. Asegúrese que las causas identificadas son las mínimas que conllevaran a la desviación del proceso. Las causas iniciadoras más comunes están relacionadas con las fallas de:

1. Lazos de control que forman parte del BPCS
2. Acciones que requieren intervención humana
3. Equipos mecánicos

Estos eventos pueden ocurrir de manera múltiple durante la vida del proceso, así que si la consecuencia es significativa, sistemas de seguridad son generalmente requeridos para cubrir el riesgo identificado.

Estime la severidad de las consecuencias, tomando en cuenta las condiciones posibles del evento. El factor de ocupación durante un evento anormal típicamente no es el mismo que el factor de ocupación durante operación normal. Si una condición anormal de operación ocurre, cuales son las responsabilidades de los operadores o el grupo de mantenimiento? Si la alarma de seguridad se activa, se espera que el operador responda localmente? Entre más lento sea el evento, más probable es una respuesta de campo y un factor de ocupación más alto, posiblemente incluyendo supervisores, personal de mantenimiento y operaciones.

El riesgo del proceso de un evento particular está relacionado a la probabilidad de que el evento ocurra y la severidad de las consecuencias si las mismas se presentan. Compare el riesgo del proceso con los criterios de riesgo de la compañía (5) para determinar que acción se requiere para reducir el riesgo por debajo del criterio (Figura 2). El riesgo residual representa una probabilidad de que una consecuencia inaceptable podría ocurrir, de modo que manténgalo tan bajo como sea razonablemente posible.

Para bajar el riesgo, implemente una estrategia “de defensa profunda” en la cual una o más capas de protección independiente (IPLs) actúan para interrumpir la secuencia del evento, tal como se ilustra en la Figura 3. Independencia se logra cuando la operación del IPL no es afectada por el acontecimiento de la causa iniciadora o por la falla de otro IPL. Si más de una función esta asignada al mismo IPL para prevenir un evento de peligro identificado, el IPL debe cumplir los requisitos generales de funcionalidad e integridad de todas sus funciones. Verifique durante el PHA que los IPLs identificados están apropiadamente clasificados y que la documentación disponible claramente describa los requerimientos funcionales y de integridad del IPL. Siete atributos principales de un IPL deben ser manejados rigurosamente durante la vida del proceso (6):

- Independencia
- Funcionalidad
- Integridad
- Confiabilidad
- Auditable
- Seguridad de acceso
- y Gerencia del Manejo de cambios.

En el pasado, era común (y aun es común en aplicaciones pequeñas) que las alarmas de seguridad y controles estuvieran separados del BPCS. En años recientes, algunas Operadoras han implementado alarmas de seguridad y controles en el BPCS cuando el mismo está diseñado y manejado para lograr la integridad y confiabilidad pretendida. Alcanzar la integridad segura desde el BPCS no es un asunto trivial – esto requiere de redundancia, diagnósticos, y controles administrativos que van mas allá de lo que típicamente es necesario para un sistema de control.

Además de encargarse del riesgo del proceso originado de los eventos iniciadores identificados (o desviaciones de procesos), la estrategia de reducción de riesgo debería también cubrir las consecuencias secundarias asociadas con la operación de los IPLs, tales como la reducción en la producción, paradas de planta, y el envió de gases al cabezal de venteo (Figura 4). Consecuencias secundarias pueden ser asumidas como los efectos que origina la estrategia de reducción de riesgo – cada vez que un IPL se activa, hay un efecto en el proceso. Determine el costo de las operaciones inesperadas de los IPLs para

establecer el índice máximo de activación inesperado aceptable. La estrategia final de reducción de riesgo debería asegurar que los efectos secundarios sean aceptables o manejados apropiadamente.

2. Implementando la Estrategia.

ISSs operan mejor cuando están basados en una lógica muy sencilla. Por ejemplo: “Cuando la alarma de alta presión inicia la apertura del venteo de control de presión”, o “cuando ocurre la alta temperatura, cierre de la válvula de alimentación” Esta lógica es suficientemente sencilla que puede ser implementada en sistemas cableados usando mecanismos amplificadores de disparo, módulos de alarmas o relees.

Sistemas cableados son económicamente atractivos para aquellos sistemas que tienen menos de 10 funciones. Si estamos en presencia de un sistema de más de 10 funciones, los PLCs generalmente llegan a ser económicamente más atractivos. ISSs no son sistemas inherentemente complejos, pero ellos pueden llegar a ser complejos por diseño. Continúe enfocándose en lógica sencilla inclusive en un PLC, donde la facilidad de programación de software invita a la lógica compleja, incrementando la posibilidad de errores en el programa.

PLCs son sistemas complejos con el potencial de un elevado número de fallas sin identificar, incluyendo muchas de ellas sistemáticas. Debido a las fallas desconocidas e impredecibles asociadas con los PLCs, ISA 84.01 (Cláusula 11.5) requiere que el PLC sea configurado de manera segura para las aplicaciones SIS. La configuración segura aborda los bien conocidos modos de fallas de las entradas, salidas, procesadores principales y comunicaciones. Esto requiere de diagnósticos adicionales y capacidades de tolerancia a fallas que generalmente no se encuentran disponibles en arquitecturas comunes de sistemas de control, pero que están disponibles en sistemas comercializados como los que cumplen con el estándar IEC 61508.

ISA 84.01 (Cláusula 11.5) requiere la implementación de un proceso de aprobación por parte del usuario para asegurar que el equipo de campo tiene suficiente historia previa de uso en un ambiente de operación similar y que los modos de falla son entendidos y tomados en consideración en el diseño, operación y prácticas de integridad mecánica.

Plantas dependen de los equipos ISS para alcanzar o mantener la operación segura. Un ISS debe ser lo suficientemente robusto para soportar el estrés ambiental y proveer la integridad y confiabilidad requerida. Para cada instalación, defina las condiciones ambientales que impactan la selección de equipos de ISS, tales como:

- Composición de los procesos, Ej.: sólidos, sales o corrosivos.
- Condiciones operacionales de los procesos, Ej.: temperaturas extremas, presión o vibración
- Condiciones externas, Ej.: necesidades de protección contra el invierno ó clasificación de áreas peligrosas.
- Requerimientos del tiempo de respuesta relacionado con el tiempo seguro disponible de los procesos.
- Criticidad, Ej.: desviacion, exactitud, resistencia al fuego y cierre hermético

La respuesta oportuna del ISS es crítica para la reducción exitosa del riesgo. El tiempo seguro del proceso comienza cuando el proceso alcanza el límite definido de operación segura y finaliza cuando se origina la fuga. El ISS debería ser capaz de tomar una acción hacia el proceso en menos de la mitad del tiempo seguro del proceso asignado. La especificación de los equipos finales requiere de un entendimiento de la respuesta dinámica del proceso, la exactitud de los instrumentos, y el tiempo de respuesta de los instrumentos que forman parte del lazo.

El retraso en la detección y error en la medición son generalmente bastante bajos cuando los instrumentos son adecuadamente instalados y comisionados. Una parada de planta causa el intervalo de tiempo mas significativo, incluyendo el tiempo requerido para la parada (o arranque) y la masa y energía retenida en el sistema después que la función de seguridad es completada (Figura 5). El tiempo seguro del proceso puede ser largo (de segundos a minutos) o corto (milisegundos), dependiendo de la dinámica del proceso y el diseño del equipo. La asignación del tiempo seguro del proceso se ve afectado indistintamente si un IPL puede efectivamente operar antes de que otro IPL se activado o antes que los eventos peligrosos ocurran.

Evaluar las causas comunes potenciales en los sistemas de servicio del proceso, tales como la electricidad, comunicaciones, aire de instrumentos, agua de enfriamiento y potencia hidráulica. Asegúrese que los sistemas de servicio del ISS están diseñados para llevar a los equipos afectados a un estado seguro específico con la finalidad de lograr la integridad requerida. La aprobación de diseños “no en falla segura”, deberían tomar en cuenta el impacto en la estrategia de reducción de riesgo, el tipo de ISS, la integridad de los sistemas de servicio y medios alternos para alcanzar un estado seguro. El acceso humano y cibernético a cualquier ISS debería ser lo suficientemente restringido utilizando procedimientos administrativos y medios físicos para asegurar que este acceso no impacta la integridad del ISS.

Documentar la base del diseño del ISS y mantenerlo bajo un control de revisiones como información de seguridad del proceso por la vida del sistema. Todos los ISSs son únicos en que cada uno esta diseñado para cubrir un evento de riesgo especifico asociado con el proceso. Dos ISSs podrían ser similares, pero ninguno es exactamente igual. La base del diseño del ISS debería cubrir lo siguiente:

- Requerimientos para la detección y respuesta ante potenciales eventos peligrosos.
- Requerimientos para la detección de fallas, tal como diagnósticos y pruebas funcionales.
- Requerimientos para la tolerancia a fallas contra fallas peligrosas.
- Provisiones para bypasses seguros para mantenimiento y prueba, incluyendo el máximo periodo de tiempo que el ISS pueden estar en bypass antes de que la acción del manejo de cambio (MOC) sea requerida.
- Provisiones para la operación segura cuando el equipo de proceso es operado con una falla en el ISS.
- Provisiones para una parada segura si el SIS falla en tomar acción cuando le es requerido
- Requerimientos para el arranque y parada.

Las bases de diseño de los SIS esta contemplada por la ISA 84.01 (Cláusulas 10 a la 12). El Reporte Técnico TR84.00.04 (7) proporciona una guía extensa en los requerimientos de diseño para el hardware y software usados para implementar los SISs. Considere desarrollar prácticas uniformes para aplicaciones similares que promuevan consistencia en la implementación del ISS, para así reducir costo de entrenamiento y el potencial de errores humanos (8).

ISA 84.01 (Cláusula 11.4) requiere tolerancia a fallas contra fallas peligrosas para funciones SIL3, de modo que equipos de seguridad redundantes deberían ser proporcionados para los SISs de SIL3. La tolerancia a fallas no es requerida para SIL1 o SIL2 cuando el equipo SIS es seleccionado basado en el uso previo, es independiente de la causa iniciadora, e implementado de tal manera que los modos de falla dominante llevan el equipo SIS a un estado seguro especifico.

ISA 84.01 (Cláusula 11.9) también requiere que la integridad del SIS sea verificada cuantitativamente. Asegurarse que los equipos seleccionados son adecuados para el uso en el ambiente de operación, que los subsistemas tienen los mínimos requerimientos de tolerancia a fallas y que los sistemas logran la funcionalidad e integridad requerida. El Reporte Técnico ISA TR84.00.02 (9) provee una guía en la verificación del SIL de los SISs.

El equipo ISS debería ser incluido en un programa de integridad mecánica (10) que busque mantener el ISS en la condición “tan bueno como nuevo”. La integridad mecánica incluye una variedad de actividades, tales como inspección, mantenimiento preventivo, reparación/reemplazo, y pruebas funcionales. Incluye la instrumentación y controles usados por el operador para detectar y tomar una acción manual. Mantenga una lista de equipos que identifique los equipos ISS por nombre específico e incluya la inspección requerida y el intervalo necesario de prueba funcional necesario para asegurar que el equipo mantiene su condición adecuada para el servicio.

El intervalo inicial de prueba funcional esta determinado basado en las oportunidades de pruebas fuera de servicio “offline”, regulaciones relevantes, historia del equipo en ambientes similares de operación, recomendaciones del fabricante, y requerimientos de integridad. Cuando la prueba funcional es requerida más frecuentemente que en período de paradas programadas, sería necesaria capacidades de la prueba funcional y reparación en servicio “online”.

Si la actividad “online” requiere la acción de bypass, documente las medidas de compensación que proporcionen una protección equivalente a la funcionalidad deshabilitada del ISS. Evalúe las actividades de bypass y los peligros potenciales para definir las medidas de compensación y el tiempo máximo de reparación permitido. Implemente alarmas de bypass cuando sea práctico, y reinicie las alarmas de bypass y alarmas de seguridad para cada turno de operación. Asegúrese que los operadores conocen el estado de los equipos ISS y que hacer si una desviación del proceso ocurre.

3. Valide, inicie, opere y mantenga la estrategia.

La validación ha sido tradicionalmente referida como una prueba de aceptación en sitio (SAT) porque esto representa la aceptación formal del ISS instalado y comisionado por el personal de operación de la planta. El equipo es probado para trabajar como lo es requerido, y de este punto en adelante, cambios serán revisados y aprobados de acuerdo con las practicas MOC de la planta. La validación es ejecutada después de la calibración del instrumento y el chequeo de los lazos ha sido completado. Un plan de validación es desarrollado para asegurar la ejecución del SAT, revisión minuciosa de la documentación y resolución de cualquier hallazgo en forma ordenada. ISA 84.01 (Cláusula 15) aborda la validación de SISs.

La validación demuestra que el ISS opera de acuerdo con la base del diseño tal cual como instalado y comisionado. Esta es una prueba de Entrada-hacia-Salida del ISS que también prueba que el

equipo de ISS interactúa como esta previsto con otros sistemas, tales como el BPCS y la interfase del operador. El SAT también proporciona una oportunidad para el primer pase de validación de los procedimientos operacionales y de mantenimiento. La validación debe ser completada antes del inicio de cualquier modo de operación donde un evento peligroso pudiera ocurrir que requiera la operación de un ISS nuevo ó modificado. Algunos usuarios requieren que la validación sea hecha después de cualquier parada mayor programada del proceso o parada de planta.

Complete la revisión segura del arranque (PSSR) para verificar que:

- El ISS nuevo o modificado es instalado y demostrado para operar de acuerdo con la intención del diseño.
- Se están utilizando los procedimientos adecuados para asegurar la funcionalidad y reducción de riesgo requerida.
- Los análisis de peligro apropiados ó revisión del manejo de cambios han sido realizados y sus recomendaciones tomadas en consideración.
- El entrenamiento del personal involucrado ha sido completado.

Información adicional sobre el PSSR puede ser encontrada en Referencia #12

Defina claramente los límites seguros de operación en los procedimientos operacionales, y la acción apropiada a tomar cuando estos límites sean excedidos. La respuesta del Operador a una indicación, alarma o incidente es dictada primero por los procedimientos y entrenamiento y después por la experiencia. Audite la respuesta del Operador hacia las alarmas de diagnostico del ISS y alarmas de seguridad. ISA 84.01 (Cláusula 16 y 17) cubre los requisitos de procedimientos operacionales y de mantenimiento para los SISs. Estos procedimientos deberían incluir:

- Una descripción de los eventos peligrosos a los cuales se intenta prevenir.
- Una descripción del ISS
- La respuesta apropiada del operador para detectar fallas del equipo ISS y provisiones para la operación con fallas detectadas (Ej.: medidas de compensación).
- Condiciones bajo las cuales es seguro restablecer un ISS
- Uso de bypasses para el arranque y las condiciones del procesos a ser monitoreadas durante el arranque.
- La respuesta esperada por el Operador cuando las alarmas de seguridad son recibidas.
- Puntos de ajuste de disparo, el estado seguro esperado cuando un disparo se completa, y la forma de notificación del disparo (si se encuentra incluida)
- Acciones esperadas del operador si el estado seguro no es alcanzado.
- Las condiciones del proceso de “nuca se exceda, nunca se desvíe”, la cual requiere una parada manual.

Los equipos de seguridad instalados están sujetos a los mismos factores de estrés operacional que el equipo de control, y pueden fallar en cualquier momento. Por lo general, los equipos de seguridad, operan en modo de demanda, Ej.: no se supone que actúe hasta que una condición anormal ocurra. Cuando el ISS falla, pueda que no sean completamente aparente, como lo seria una falla en una aplicación de control. Frecuentemente, equipos demuestra un índice de falla a través del tiempo que sigue una curva comúnmente llamada como curva de bañera (bathtub) (Figura 6).

Las primeras fallas son causadas por errores en las fases de fabricación, ensamble, pruebas, instalación y comisionamiento. Mucha de estas fallas son el resultado del manejo rudo, almacenamiento inapropiado en la pre-instalación, malas prácticas de instalación, ó practicas descuidadas de construcción. Una Inspección rigurosa, comisión y validación son necesarias para identificar y corregir estas fallas.

El periodo de deterioro es caracterizado por un incremento en el índice de falla con respecto al tiempo. Una pobre integridad mecánica ha sido citada como la primera causa de falla de un equipo. Un mantenimiento de prevención puede extender la vida útil del equipo y mejorar su confiabilidad. Los registros de integridad mecánica proporcionan datos que el equipo es mantenido en la condición "tan bueno como nuevo" y justifican su uso continuo. Consecuentemente, el personal de mantenimiento debe ser capacitado en las actividades necesarias para asegurar la integridad del equipo.

Pruebas funcionales periódicas deberían ser realizadas con una frecuencia suficiente para detectar la transición desde el periodo de vida útil al periodo de deterioro, y así poder identificar y planificar la necesidad de reemplazar ó actualizar un equipo. La falla del equipo debería ser investigada usando un análisis de causa raíz para reducir o eliminar las causas de la falla. El intervalo de la prueba funcional debería ser evaluado periódicamente basado en experiencia de planta, degradación del hardware, la confiabilidad demostrada del software, etc., y en un evento en el cual la falla se repite, el intervalo debería ser acortado según sea necesario para asegurar la detección pertinente de fallas.

Ejecute las pruebas funcionales usando los procedimientos de operación y mantenimiento que aseguren que la prueba sea finalizada correctamente, consistentemente y de una manera segura. Las pruebas funcionales deberían determinar la condición inicial/final del equipo para todos los modos de operación definidos. La documentación debería identificar el procedimiento, equipo y persona que ejecutaron la prueba. Identifique y evalúe las desviaciones que podrían ocurrir desde la base del diseño y especificaciones del equipo, Ej., MOC incompleto o degradación acelerada. Después, use las pruebas funcionales para entrenar al personal en la funcionalidad del ISS esperada y para verificar la claridad y que tan completos se encuentran los procedimientos.

La reducción de riesgo en un mundo real es demostrado por los datos de integridad mecánica. Los registros asociados con cualquier ISS deben mostrar que el equipo puede operar como fue especificado durante todos los modos de operación contemplados. Esto es verdadero especialmente para los SIS, los cuales usualmente proveen la última oportunidad para llevar al proceso a un estado seguro.

El análisis y el seguimiento de fallas es esencial para cerrar el ciclo de vida de seguridad. Fallas repetidas probablemente indican que el equipo instalado no es capaz de cumplir los requisitos de funcionamiento. Use un análisis de causa raíz para determinar porque las matrices están en una tendencia hacia la dirección incorrecta, para así implementar planes de acción que mejoren la gerencia del sistema, equipo, procedimientos y entrenamiento del personal. Identifique fallas especiales y previamente desconocidas, y comuníquelas al personal, asegurándose que las lecciones son aprendidas y no ocultadas en el historial de integridad mecánica.

4. Maneje cambios de acuerdo con la estrategia.

Deming, considerado el padre del control de calidad, creyó que 85% de la eficacia de un trabajador es determinada por el sistema con que trabaja, y sólo 15% por su propia habilidad (11). Una

estrategia exitosa de reducción de riesgo acepta que las personas están envueltas en cada aspecto del ciclo de vida de un ISS. Por lo tanto, la integridad reportada por cada ISS esta limitada por el sistema de control de calidad que identifica y busca eliminar defectos en el sistema. Errores Humanos deben ser reducidos a tal punto que los mismos no impacten significantemente la integridad del sistema (12). Aseguramiento de las cualidades que tiene el personal es la clave.

El conocimiento evoluciona con el tiempo a medida que la investigación y el desarrollo cede paso a las mejoras operacionales en plantas de proceso. Eventos que envuelven operaciones anormales identifican debilidades en la estrategia de reducción de riesgo, que conlleva a la necesidad de más protecciones y matrices de funcionamiento mejoradas. Nuevas ideas identifican maneras para disminuir los riesgos aun más.

Periódicamente evalúe los ISS existentes contra criterios actuales y prácticas industriales para determinar si el equipo esta diseñado, mantenido, inspeccionado, probado y operado de una manera que pueda pasar una inspección publica. Utilice un procedimiento MOC para iniciar, documentar, revisar y aprobar los cambios a los ISSs, otros que no sean un reemplazo de partes en los ISSs, con partes de las mismas características, modelo y función. Evalúe los cambios en el proceso y sus equipos para determinar su impacto potencial en las bases de diseño aprobadas del ISS antes de implementar el cambio. El personal necesita entender que inicia una revisión o proceso de MOC y por que darle un seguimiento a los cambios es importante.

Actualice los documentos a una revisión de “cómo construido”, incorporando cambios realizados desde la última revisión formal de dibujos/documentos. Mantenga la documentación bajo el control de revisión por la vida del equipo. A la documentación se le debe poder realizar un seguimiento hacia el análisis de riesgos del proceso y debería ser auditable.

Ideas Finales

Un sistema de gerencia efectivo usa una propuesta sistemática para manejar el riesgo a través de la vida del equipo de proceso. Con una continua participación de ingeniería de procesos, la estrategia de reducción de riesgo puede ser adaptada para alcanzar las metas de operación, mantenimiento y confiabilidad. Una estrategia fuerte y sostenible asegura que el diseño del proceso, el diseño de ISS, y los procedimientos de operación y mantenimiento sean rigurosamente manejados para lograr una alta integridad y confiabilidad con la menor posibilidad para falla de causa común. A lo largo de la vida del equipo, esta propuesta tendrá un efecto positivo en la operación del proceso y ofrece beneficios significativos para los usuarios.

Artículos Citados

1. Overton, T., and S. Berger, “ Process Safety: How Are You Doing?” *Chem. Eng. Progress*, 104 (5), pp. 40–43 (May 2008); the full metrics report is available on the CCPS website, www.aiche.org/ccps/knowledgebase/measurement.aspx.
2. International Society of Automation, “Functional Safety: Safety Instrumented Systems for the Process Industry Sector,” ANSI/ISA 84.00.01-2004, ISA, Research Triangle Park, NC (2004).

3. Center for Chemical Process Safety (CCPS), "Inherently Safer Processes," Second Edition, American Institute of Chemical Engineers, New York, NY (Dec. 2008).

4. Center for Chemical Process Safety (CCPS), "Guidelines for Hazard Evaluation Procedures," Third Edition with Worked Examples, American Institute of Chemical Engineers, New York, NY (2008).

5. Center for Chemical Process Safety (CCPS), "Guidelines for Developing Quantitative Safety Risk Criteria," American Institute of Chemical Engineers, New York, NY (expected 2009).

6. Center for Chemical Process Safety (CCPS), "Guidelines for Safe and Reliable Instrumented Protective Systems," American Institute of Chemical Engineers, New York, NY (2007).

7. International Society of Automation, "Guidelines for the Implementation of ANSI/ISA 84.00.01-2004 (IEC 61511)," ISA TR84.00.04, ISA, Research Triangle Park, NC (2005).

8. Gentile, M. and A. Summers, "Cookbook Versus Performance SIS Practices," *Process Safety Progress,* 27 (3), pp. 260-264 (2008).

9. International Society of Automation, "Safety Instrumented Functions (SIF) – Safety Integrity Level (SIL) Evaluation Techniques," ISA TR84.00.02, ISA, Research Triangle Park, NC (2002).

10. Center for Chemical Process Safety (CCPS), "Guidelines for Mechanical Integrity Systems," American Institute of Chemical Engineers, New York, NY (2006).

11. Deming, W. E., "Out of Crisis," MIT Press, Cambridge, MA (1986).

12. Gentile, M. and A. Summers, "Random, Systematic, and Common Cause Failure: How Do You Manage Them?" *Process Safety Progress*, 25 (4), pp. 331–338 (2006).

13. Summers, A. E. and W. H. Hearn, "Quality Assurance in Safe Automation," *Process Safety Progress,* 27 (4), pp. 323-327 (2008).

14. Center for Chemical Process Safety (CCPS), "Guidelines for Performing Effective Pre-Startup Safety Reviews," American Institute of Chemical Engineers, New York, NY (2007).

ANGELA E. SUMMERS, PhD, es presidente de SIS-TECH (12621 Featherwood Dr., Suite 120, Houston, TX 77034; Phone: (281) 922-8324; E-mail: asummers@sis-tech.com; Website: www.sis-tech.com) y tiene 20 años de experiencia en sistemas instrumentados de seguridad (SIS), ingeniería de procesos e ingeniería ambiental. Ella es ingeniero profesional con licencia en Texas, y es miembro de AIChE, ISA, IEC y ANSI, y es una participante activa en comités de estándares industriales. Ella ha publicado más de 50 artículos, contribuido en capítulos de manuales de ingeniería, y editado reportes técnicos y libros en temas relacionados con seguridad de los procesos y diseño de sistemas instrumentados. Summers recibió en el año 2005 el reconocimiento "ISA Albert F. Sperry" y fue admitida en el año 2007 al "Process Automation Hall of Fame" por sus contribuciones a la automatización segura en la industria de proceso. Ella recibió su PhD en ingeniería química de la Universidad de Alabama, MS en ingeniería ambiental de la Universidad de Clemson y BS en ingeniería química de la Universidad del estado de Mississipi.

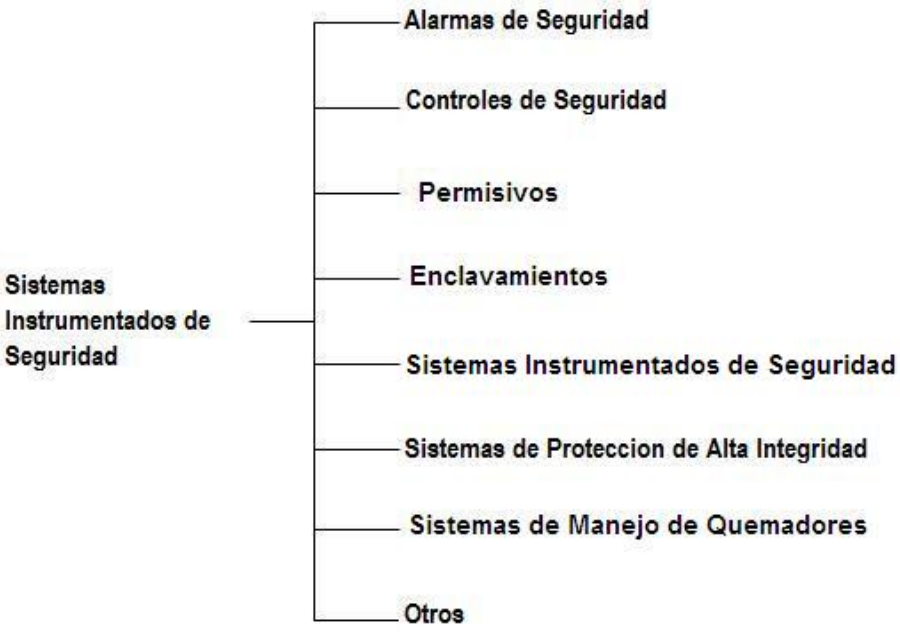

Figura 1. Variedad de términos usados para clasificar los sistemas instrumentados de seguridad.

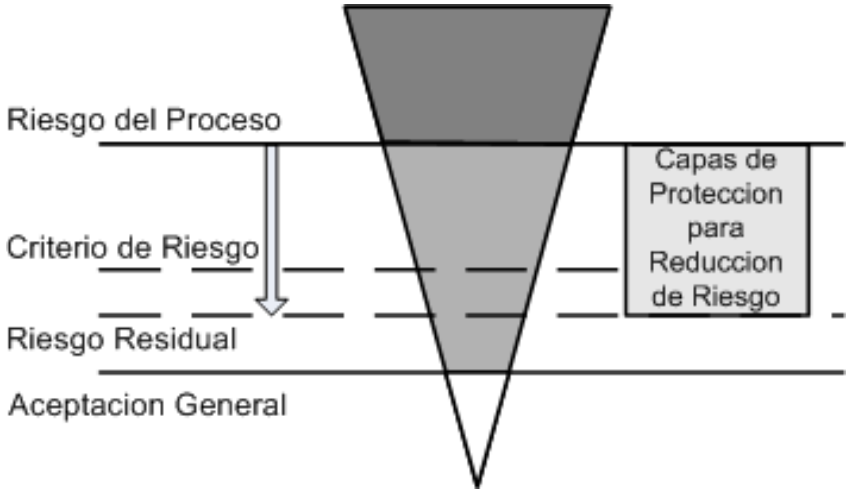

Figura 2. Comparando el riesgo del proceso con el criterio de riesgo de la compañía ayuda a determinar que se requiere para reducir el riesgo tanto como sea razonablemente práctico.

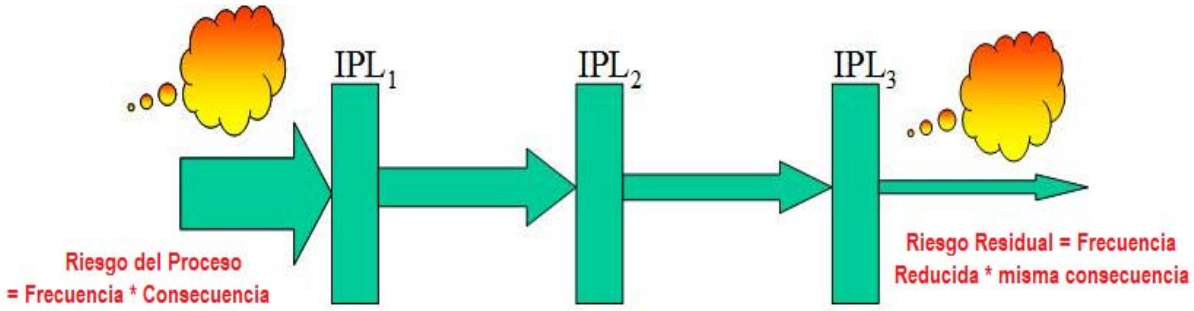

Figura 3. Riesgo del Proceso es reducido por tres capas de protección independiente.

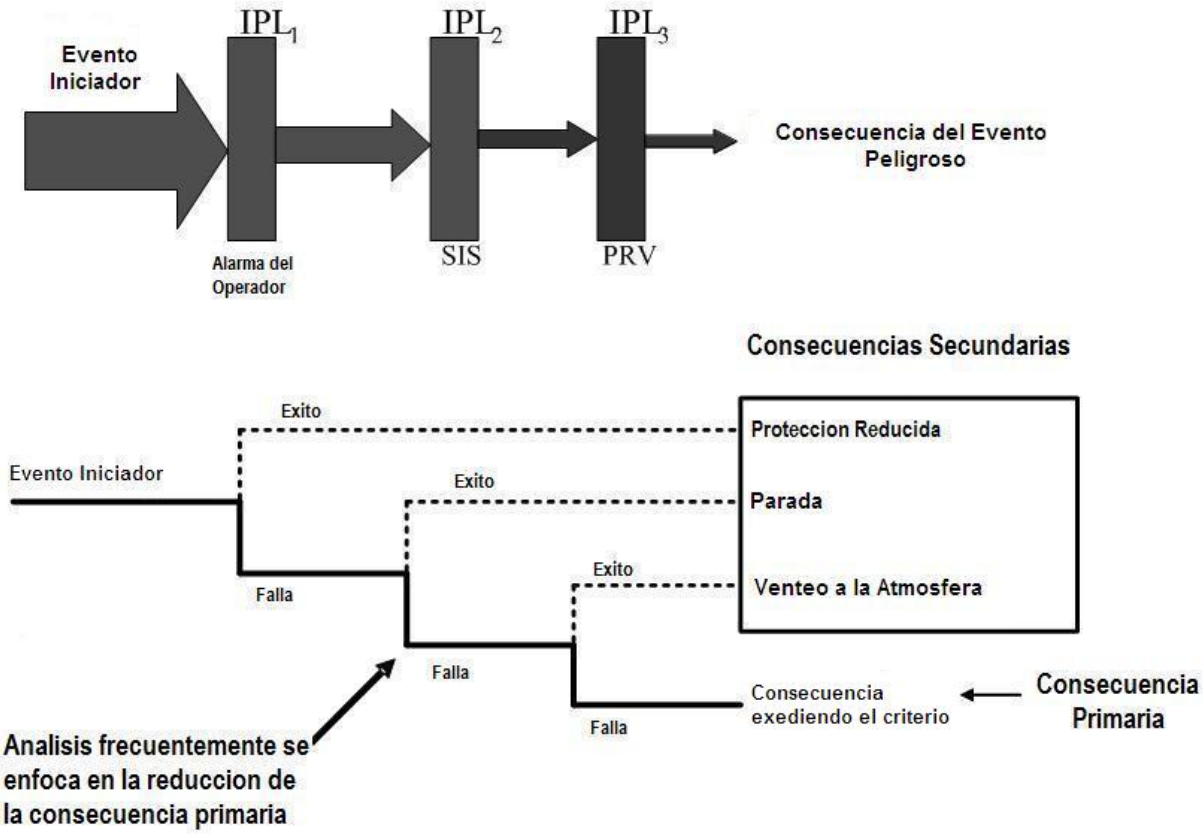

Figura 4. Un árbol de eventos ilustra consecuencias primarias y secundarias de un evento iniciador.

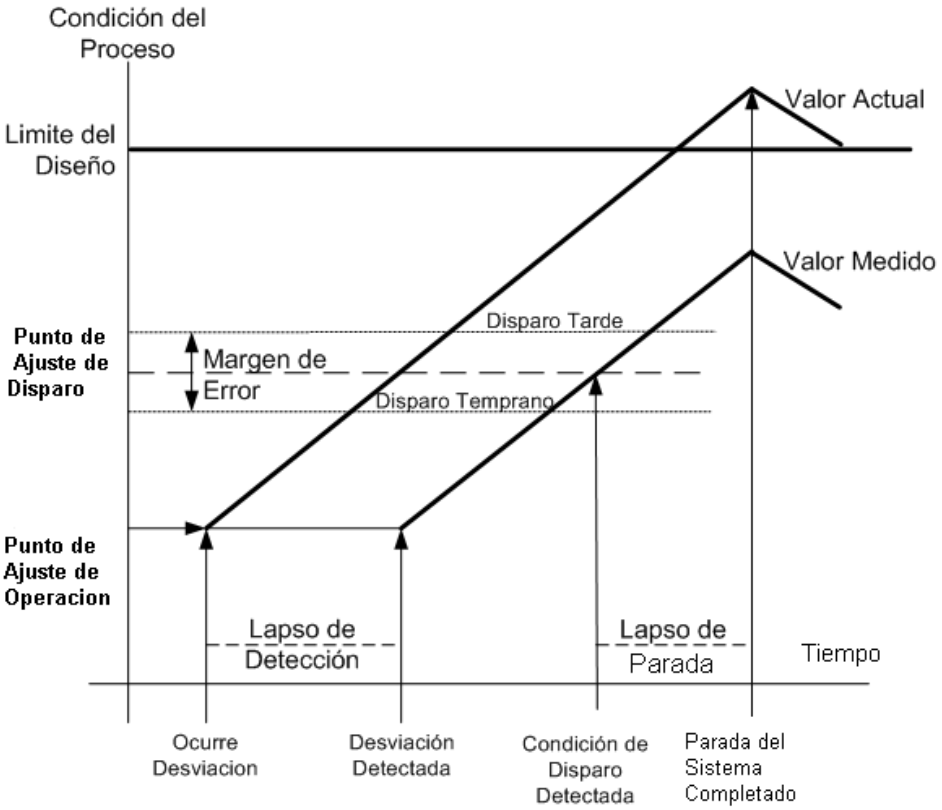

Figura 5. Efectividad del ISS esta relacionado con el lapso de la detección, error en la medición, y el lapso de parada (8).

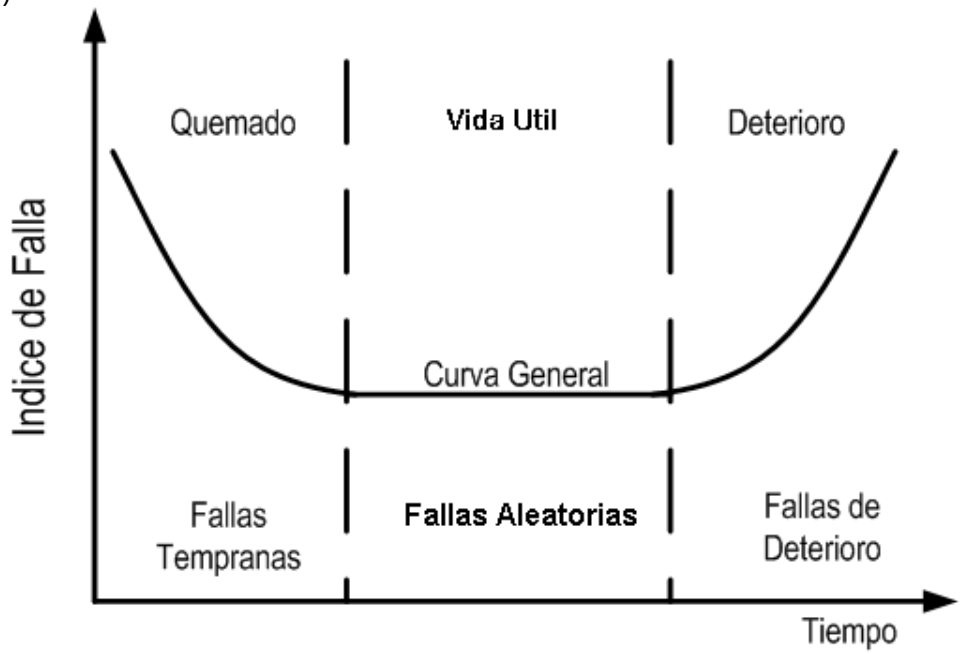

Figura 6. El índice de falla con respecto al tiempo de la mayoría de los equipos de seguridad pueden ser representado por la llamada curva de bañera (bathtub curve)