ASEGURAMIENTO DE LA CALIDAD Y SISTEMAS INSTRUMENTADOS DE SEGURIDAD

Angela E. Summers, PhD, PE, y Giorgio Palermo SIS-TECH Solutions, LP
12621 Featherwood Drive, Suite 120, Houston, TX 77034

Abstracto

Un proceso perfecto no tendría peligros, pero en un mundo real, la perfección es casi imposible de alcanzar. Existen condiciones latentes en los equipos, procedimientos, y en el entrenamiento del personal que al acumularse suficientemente, pueden generar desafíos en la Operación Segura en las plantas o unidades de proceso. La Operación segura, es sostenida a través de la implementación de una estrategia de reducción de riesgo, que depende de una gran variedad de prácticas de equipos de seguridad, para prevenir que sustancias químicas sumamente peligrosas sean liberadas a la atmósfera.

La calidad en el diseño y gerencia son absolutamente esenciales si realmente se pretende alcanzar una reducción de riesgo y prevención de incidentes – no solo la reducción de riesgo calculada.

Este artículo emplea el ciclo “Shewhart Cycle” el cual introduce una variedad de actividades implicadas en lograr una Operación Segura haciendo uso de Sistemas Instrumentados de Seguridad (ISS). Así mismo, el artículo utiliza el proceso planificar, generar, revisar y actuar (Plan, Do, Check and Act) para discutir el aseguramiento de la calidad y su aplicación en Sistemas Instrumentados de Seguridad (ISS).

Introduccion

Los accidentes continúan ocurriendo debido a que muchos dueños/operadoras usan los números de ocurrencia de lesionados y fatalidades como una medida predominante para así demostrar la Operación Segura. Un enfoque en el impacto directo puede llevar a la normalización de los eventos de venteo de Hidrocarburos y/o gases y a una tolerancia hacia aquellos eventos que incrementan la probabilidad de ocurrencia. Más aun, las lesiones y fatalidades deberían ocurrir con tan poca frecuencia que el impacto de los datos no sea significativo para supervisar el desempeño.

Los accidentes usualmente ocurren cuando los equipos de Seguridad no son diseñados, instalados, operados, probados y mantenidos apropiadamente. La industria ha adoptado teorías y estándares para asegurar que los equipos de procesos puedan ser operados de una manera segura. Para prevenir errores y mejorar la seguridad de los procesos, se requiere implementar sistemas que reduzcan las condiciones que contribuyen a los errores. El problema no es que se cuenta con personal que no esta calificado para ejecutar las funciones, el problema es que el sistema que gobierna los equipos no es lo suficientemente riguroso como para asegurar la confiabilidad

Un Sistema de control de calidad debe ser usado con la finalidad de proporcionar las herramientas necesarias para mantener la confiabilidad de los equipos; de lo contrario, los accidentes continuaran ocurriendo en la medida en que se acumulen o existan suficientes condiciones latentes. Una estrategia preactiva, podría ser monitorear el comportamiento, errores y fallas que generan una condición de peligro.

Identificar las oportunidades para mejoras, es un proceso esencial para contrarrestar la acumulación de las condiciones latentes minimizando así, el riesgo inicial.

Planificacion

Según Deming el 85% de la efectividad de los trabajadores esta determinada por el Sistema con que se trabaja, solo 15% por su propia habilidad [1]. La Planificación asegura que los procesos de trabajo conlleven a que los equipos operen consistentemente en una manera segura, cumpliendo con los requisitos jurisdiccionales y gubernamentales; así como también con las reconocidas buenas prácticas de Ingeniería. El producto de una planificación es un sistema de gerencia de políticas, normas y procedimientos que procuran identificar y controlar la liberación de sustancias químicas sumamente peligrosas. Algunas de las normas de trabajo y actividades recomendadas para Sistemas Instrumentados de Protección están previstas en el libro del CCPS, “Guidelines for Safe and Reliable Instrumented Protective Systems” [2] y para los Sistemas Instrumentados de Seguridad en la norma ANSI/ISA 84.00.01-2004 [3].

No hay substituto para el conocimiento. [4] Sólo una pequeña cantidad de conocimiento puede ahorrar muchas horas del trabajo o prevenir los errores que conllevan generar a condiciones de peligros en los procesos. Muchos dueños/operarios pierden el conocimiento de los procesos y la historia a medida que los operadores y personal técnico se retiran o salen simplemente para obtener mejores trabajos. Los errores se acumulan a menos que exista un análisis y mejoramiento continuo de las normas de seguridad para contrarrestar la pérdida de pericia causada por los retiros, reducción de personal y la degradación de los equipos causada por el uso a través de los años. El conocimiento del proceso es sostenido por una base escrita de información de seguridad de proceso (PSI), cubriendo los peligros del proceso, la tecnología, y el equipo.

El conocimiento crece cuándo los procedimientos de evaluación de peligros [5] son utilizados a través de la vida del equipo para identificar y evaluar los acontecimientos significativos relacionados a la operación del proceso. El riesgo del acontecimiento es analizado cuantitativamente o cualitativamente para determinar las causas y la frecuencia potencial de ocurrencia. Capas independientes de protección son utilizadas para asegurar que una falla simple o los errores no comprometan la operación segura del proceso. Cuándo el riesgo residual excede los criterios de riesgo de dueño/operario, se recomienda la aplicación de diseños de Ingeniería y mecanismos administrativos de seguridad para reducir el riesgo por debajo de los criterios deseados. Adicionalmente, el conocimiento evoluciona con el tiempo, cuando la investigación y desarrollo tecnológico alcanzan las áreas operativas. Los eventos tales como la pérdida de contención o derrames, identifican las debilidades en la estrategia de la reducción del riesgo y usualmente conllevan a la implementación de capas de protección adicionales.

El personal debe ser entrenado en las situaciones de peligros del proceso asociados con sus actividades del trabajo. El personal debe tener las habilidades y el conocimiento necesarios para realizar su trabajo con la calidad deseada, así que las habilidades mínimas y conocimiento del trabajo requeridos deben ser especificados. Cuándo el tipo de aprendizaje “instrucción en el trabajo” es requerido, el programa de capacitación debe contemplar, cómo las habilidades y el conocimiento son desarrollados en una manera oportuna y segura y cómo el progreso es medido [2].

Un documento de bases de diseño debe definir el PSI para el equipo de seguridad y debe ser revisado y confirmado a través del análisis de peligros de proceso. Para sistemas instrumentados de seguridad, las bases de diseño son las especificaciones de hardware y las especificaciones de

requerimiento de seguridad del software. La base del diseño debe estar sujeta al control de revisiones durante la vida útil del equipo y de asegurar lo siguiente:

- El equipo de la seguridad ha sido probado trabajando en un ambiente operativo con el desempeño requerido.
- El sistema ha sido diseñado para exceder la reducción del riesgo especificada en el análisis de peligros.

"Sin embargo, las cosas más importantes son desconocidas y no pueden ser encontradas". [4] Así, aún cuándo personas capacitadas aplican la teoría y los estándares adecuados, siempre existen lecciones que pueden ser aprendidas. Para contrarrestar lo desconocido, los dueños/operadoras dependen de una profunda estrategia de defensa, que utiliza múltiples capas independientes de protección para disminuir el riesgo operacional [6]. Estas capas incluyen sistemas instrumentados de seguridad (ISS) que logran o mantienen el estado seguro en presencia de condiciones inaceptables del proceso. Adicionalmente, esta defensa disminuye la causa común, el modo común y los errores sistemáticos que generan la falla de múltiples capas de protección.[7,8].

Finalmente, la planificación debe considerar la seguridad y la gerencia/manejo de cambios. El acceso físico y virtual al ISS debe ser restringido con ayuda de procedimientos administrativos y medios físicos [2]. Las evaluaciones de la independencia deben considerar las fallas de las comunicaciones e interfaces de operación. Los procedimientos escritos deben contemplar el cómo iniciar, documentar, revisar, y aprobar los cambios al ISS, no debe tomarse como un reemplazo de un equipo similar. Cualquier cambio al proceso y sus equipos debe ser evaluado bajo el proceso de "Gerencia de Cambios" con la finalidad de determinar el impacto en los requisitos de ISS.

HACER

La fase "hacer", implica la implementación de políticas, prácticas, y procedimientos. Desde una perspectiva de implementación de proyecto, la ingeniería de detalle es completada dando como resultado la instalación del ISS, el cual opera según su base de diseño excediendo el desempeño requerido. La ingeniería de detalle incluye información suficiente para asegurar que el ISS sea especificado, construido, instalado, comisionado operado, y mantenido apropiadamente. Los equipos que forman parte del ISS deben estar probados con la finalidad de asegurar el desempeño requerido en condiciones operacionales semejante.

Durante la clasificación del equipo se considera también los atributos fundamentales de las capas de protección, como son: la independencia, funcionalidad, integridad, confiabilidad, auditabilidad, gerencia de manejo de cambios, y seguridad en el acceso. La Ingeniería de detalle debe proporcionar una lista del equipo ISS, identificando al equipo a través de una designación única (por ejemplo, el número identificador); la inspección e intervalos de pruebas requeridos.

Las actividades de validación incluyen la prueba de Entrada/Salida de cada ISS nuevo o modificado con la finalidad de demostrar y documentar que el equipo es instalado según la especificación y opera correctamente en cada modo de operación. La validación debe completarse de manera satisfactoria antes del arranque de cualquier modo de operación, debido a que posibles situaciones peligrosas podrían ocurrir en donde se requiera de la operación de un sistema de seguridad nuevo o modificado.

Las pruebas funcionales son realizadas periódicamente utilizando un procedimiento escrito para demostrar la operación exitosa del ISS y para identificar y corregir las desviaciones de la base del diseño y la especificación del equipo. El personal de Mantenimiento es entrenado en los procedimientos para asegurar que luego de ejecutado los procedimientos el equipo retorna a su condición y capacidades “como si fuera un equipo nuevo”. El intervalo de la prueba es escogido basado en requerimientos de agentes de regulación o de aseguradoras, la historia de un equipo que opera en condiciones operacionales similares, recomendaciones del fabricante, y en los requerimientos para la reducción del riesgo.

Los planes de Operaciones deben considerar los requisitos de inspección y mantenimiento preventivos necesarios para mantener a los equipos en sus condiciones y capacidades “como si fuera un equipo nuevo”. Las pruebas de los equipos pertenecientes a los ISS deben demostrar que el programa de integridad mecánica mantiene el desempeño y funcionalidad requerida de los mismos. Los resultados de la revisión de registros y tendencias del programa de integridad mecánica pueden ser usados más adelante en la fase de confirmación del ciclo de calidad. Los procedimientos Operacionales deben cubrir métodos aprobados y seguros para interactuar con los equipos de seguridad, tales como los “bypasess”, acciones manuales de disparo y reestablecimiento de las funciones de seguridad. El personal de operaciones debe estar entrenado y evaluado en los procedimientos tantas veces como sea necesario, con la finalidad de asegurar que se toman las acciones correctas en su debido momento. Las acciones de los operadores en respuesta a una operación anormal de la unidad de procesos deben ser registradas y deben ser auditadas periódicamente.

CONFIRMAR

¿Por qué método? Sólo el método cuenta. [4] La fase de confirmación aplica la medición a los procesos del trabajo con la finalidad proporcionar un método uniforme para valorar el desempeño contra los requisitos. La operación sostenible se logra enfocándose en la medición, la cual proporciona la indicación del desempeño en una base de tiempo real. Ejemplos de medición para ISS pueden encontrase en la Tabla 1. Recomendaciones de Mediciones adicionales han sido publicadas por CCPS [9].

Las cosas más importantes no pueden ser medidas. [1] Escoger la medición apropiada para el seguimiento puede parecer una tarea complicada. A veces, el personal técnico quiere medir todo simplemente porque ellos pueden. La métrica debe ser escogida con cuidado, con la finalidad de que solamente la cantidad correcta de datos significativos sea tomada. Una buena métrica puede conllevar a que el personal realice sus actividades de la manera correcta. Es lamentable, pero verdadero, el personal se comportará en contra de la razón y a favor del interés de la compañía de ser necesario para que “las metas sean alcanzadas".

Por otro lado, cuanto más se conoce acerca del equipo y lo que afecta su operación, mejores los resultados en cuanto al manejo del riesgo. Para el equipo de seguridad, la calidad de la instalación es limitada por el rigor, la puntualidad y consistencia de las actividades del programa de integridad mecánica. Las investigaciones de incidentes deben evaluar cualquier falla posible o insuficiencia identificada del ISS. Los disparos en falso y las demandas reales del proceso hacia el ISS deben ser monitoreados, analizados y comparados con las expectativas obtenidas a raíz del análisis de los peligros. El proceso de “Gerencia del Manejo del Cambio” debe ser usado para cerrar las diferencias encontradas durante el proceso de investigación.

En el mundo real, muchos dueños/operadoras siguen esencialmente el viejo adagio: "Mídalo con un calibrador. Márquelo con un marcador. Córtelo con una sierra”. Los procesos de análisis de peligros

que se usan, se han convertido cada vez más cuantitativos con más factores y modificadores; la verificación de reducción de riesgo usa múltiples dígitos significativos; y el reporte de las actividades de integridad mecánica simplemente describe “Prueba Satisfactoria”.

Sin embargo, la estrategia de la reducción de riesgo es probada por los datos de integridad mecánica. La reducción de riesgo proporcionada por un equipo es el inverso de su probabilidad de falla en demanda (PFD). La PFD es calculada como el número de veces que el ISS ha fallado de manera peligrosa, dividido por el número de veces que el ISS ha sido demandado. Utilizando técnicas probabilísticas, la PFD de un equipo específico puede ser utilizada para determinar el desempeño del sistema y compararlo con lo asumido en las bases del diseño [7].

Las fallas repetitivas indican que el programa de integridad mecánica es inadecuado. El seguimiento de las fallas es esencial para cerrar el ciclo vital de seguridad. El análisis causa raíz, es usado para determinar el porqué la medición esta generando tendencias hacia la dirección equivocada, para que entonces puedan ser aplicados los planes de acción con la finalidad de mejorar el sistema de gerencia, el equipo, los procedimientos, y el entrenamiento del personal. El Mejoramiento continuo es incorporado en el “PSM” por un concepto comúnmente llamado "grandfathering", donde el dueño/operadora determina y documenta que el equipo existente es diseñado, mantenido, inspeccionado, probado, y operado de una manera segura. Esto requiere una evaluación de las prácticas de diseño y gerencia existentes contra las actuales buenas practicas de ingeniería y los requerimientos del proceso. La revisión debe determinar si el ISS existente opera de acuerdo con las bases de diseño y si el sistema actual de gerencia es suficiente para que soporte la reducción de riesgo requerida.

Actuar

¿"Qué es un sistema? Un sistema es una red de componentes interdependientes que trabajan juntos para tratar de alcanzar el objetivo. Un sistema debe tener un objetivo. Sin un objetivo, no hay sistema. El objetivo del sistema debe ser claro a todos en el sistema. El objetivo debe incluir los planes para el futuro. El objetivo es un juicio de valor [4].

La fase de actuar implica las acciones tomadas en respuesta a las tendencias en la medición y oportunidades de mejora continua. Es la oportunidad de la cultura de seguridad del dueño/operadora para brillar y para que el riesgo sea reducido tanto como sea razonablemente práctico. Los planes de acción deben definir los pasos a seguir, metas, y tiempos necesarios para cumplirlas. Los planes deben ser periódicamente revisados para determinar si existe la necesidad de acelerar las actividades o ampliar los objetivos. Por ejemplo, la actualización planificada del ISS puede acelerarse cuando el fabricante retira el soporte del equipo. Para tener éxito, los planes de acción deben ser comunicados al personal afectado con la finalidad de que ellos entiendan y comprometan con los mismos.

La mejora continua es necesaria para mantenerse por encima de condiciones latentes que representan desafíos potenciales en la seguridad y debilitan las capas de protección. Implementar actualizaciones que apunten a mejorar la eficacia operacional a largo plazo toman tiempo en completarse, dependiendo de la complejidad y el grado del cambio implicado. Cuando el ISS es cambiado, los planes y objetivos operacionales deben considerar cualquier riesgo adicional que deba ser manejado durante la transición. La operación y las bases de integridad mecánica del ISS deben ser revisadas y de ser necesario, aplicar revisiones con la finalidad de asegurar que el equipo, los procedimientos, y el entrenamiento de personal estén en sincronía con las modificaciones.

SUMARIO

Deming pensaba que la experiencia por sí sola no enseña nada y que los datos sin el contexto no tienen sentido. La información obtenida de la experiencia debe ser interpretada contra una conducta esperada, el diseño del equipo y el desempeño de las operaciones. Pero, la experiencia no es siempre el mejor maestro. Sin un entendimiento primordial de las causa raíces, los datos de campo pueden ser mal interpretados, creando una imagen errada de la realidad. Sólo los datos que sean entendidos dentro de su contexto apropiado, proporcionan una base sólida para la operación segura.

Los accidentes son prevenidos cuándo los puntos relacionados con la seguridad son manejados con una perspectiva de calidad. Las fases planificación, ejecución, confirmación e implementación son esenciales para una operación segura y confiable. Un sistema de gerencia sostenido en la medición debe ser utilizado para establecer los objetivos y evaluar el desempeño contra políticas, prácticas, y procedimientos. Análisis de las diferencias deben ejecutarse periódicamente con la finalidad de verificar que el desempeño actual excede las expectativas establecidas en el análisis del peligro y las bases del diseño. Las diferencias del desempeño deben ser solventadas a través de planes de acción que reduzcan el riesgo y prevengan los accidentes.

Referencias

Deming, W. Edwards, Out of Crisis, MIT Press, (1986).

Guidelines for Safe and Reliable Instrumented Protective Systems, American Institute of Chemical Engineers, NY, (2007).

ANSI/ISA 84.00.01-2004, Functional Safety: Safety Instrumented Systems for the Process Industry Sector, Instrumentation, Systems, and Automation Society, NC, (2004).

Deming, W. Edwards, The New Economics for Industry, Government, Education, 2nd Edition, MIT Press, (2000).

Guidelines for Hazard Evaluation Procedures, Second Edition with Worked Examples, American Institute of Chemical Engineers, NY, (1992).

Layer of Protection Analysis: A Simplified Risk Assessment Approach, American Institute of Chemical Engineers, NY, (2001).

ISA TR84.00.02, Safety Instrumented Functions (SIF) – Safety Integrity Level (SIL) Evaluation Techniques, Instrumentation, Systems, and Automation Society, NC (2002).

ISA TR84.00.04, Guidelines for the Implementation of ANSI/ISA 84.00.01-2004 (IEC 61511), Instrumentation, Systems, and Automation Society, NC (2005).

CCPS/AICHE, “Process Safety Leading and Lagging Metrics,” proposed metrics for review published on AICHE website (Jan 2008).

Tabla 1 Ejemplo: Medición Relacionada a Sistemas Instrumentados de Seguridad.

Pasos del Ciclo de Vida	Ejemplo de Medición
Análisis de Peligros	Número total de análisis de peligro y riesgo planificados durante un intervalo definido
	▪ Numero de Análisis completados
	▪ Numero de Análisis retrasados
	▪ Porcentaje de Análisis de peligro y riesgo retrasados.
	▪ De aquellos análisis retrasados, número total de días en retraso.
Bases de Diseño	Número total de equipos de Seguridad
	▪ Número de equipos con documentación final. “Como construido”
	▪ Número de equipos con documentación incompleta o modificaciones pendientes.
	▪ Porcentaje de equipos con documentación incompleta o modificaciones pendientes.
Integridad Mecánica	Número total de inspecciones planificadas durante un intervalo definido.
	▪ Número de inspecciones planificadas pero incompletas.
	▪ Número de inspecciones completadas.
	▪ Número de inspecciones retrasadas
	▪ Porcentaje de inspecciones a tiempo por ejecutar.
	▪ Porcentaje de inspecciones retrasadas
	▪ Para aquellas inspecciones completadas, numero de inspecciones satisfactorias.
	▪ Porcentaje de inspecciones satisfactorias
	Número total de pruebas a equipos planificadas durante un intervalo definido
	▪ Número de pruebas incompletas
	▪ Número de pruebas completas
	▪ Número de pruebas retrasadas
	▪ Porcentaje de pruebas planificadas
	▪ Porcentaje de pruebas retrasadas
	Para aquellas pruebas completadas:
	▪ Numero de pruebas en donde el equipo fue encontrado dentro de las especificaciones del fabricante.
	▪ Numero de pruebas en donde el equipo fue encontrado fuera de las especificaciones del fabricante (ej., fallado de manera peligrosa, fallado de manera segura o en estado degradado)
	▪ Porcentaje de pruebas con resultados dentro de las especificaciones del equipo.
	▪ Porcentaje de pruebas con resultados fuera de las especificaciones del equipo.
	Número total de equipos de seguridad
	▪ Número total de fallas encontradas vía diagnostico.
	▪ Número total de fallas encontradas vía inspección o pruebas.
	▪ Número total de fallas en donde fue necesaria la reparación o el reemplazo del equipo.
	▪ Número total de equipos fallados que fueron colocados nuevamente en servicio dentro del tiempo de reparación permitido.
	▪ Porcentaje de equipos que fueron colocados nuevamente en servicio dentro del tiempo de reparación permitido.

Pasos de Ciclo de Vida	Ejemplo de Medición
Operación Degradada	Número total de equipos de seguridad que están fuera de servicio (en bypass, deshabilitado, en override o bajo prueba/reparación) durante la operación del proceso por un intervalo definido
	▪ Número total de horas en que el equipo de seguridad esta fuera de servicio.
	▪ Número de equipos de seguridad que han sido colocados nuevamente en servicio dentro del tiempo de reparación permitido.
	▪ Número de equipos de seguridad que se encuentran fuera de servicio pero, están bajo la autorización de un MOC.
Desempeño del Proceso	Porcentaje de arranques en donde se presentaron situaciones operacionales anormales o de emergencia.
	Número total de Paradas del Proceso durante un intervalo definido de tiempo.
	▪ Numero que es debido a una operación inesperada de los equipos de seguridad.
	▪ Numero que es debido a operaciones anormales o de emergencia.
	Numero total de alarmas de seguridad durante un intervalo definido de tiempo.
	▪ Numero de alarmas que actualmente están presentes o alarmas intermitentes (se presentan de manera regular sin ninguna acción por parte del operador).
	▪ Número de alarmas de seguridad que requieren acciones o respuestas por el operador.