LECCIONES APRENDIDAS AUDITANDO SISTEMAS AUTOMATIZADOS PARA EL CUMPLIMIENTO CON PSM

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

Lessons Learned in Auditing Automated Systems for PSM Compliance, 1st Latin America CCPS Conference, featured speaker, Buenos Aires, May 27-29, 2008.

Abstracto

Mientras la dependencia en instrumentación ha aumentado a un ritmo increíble, los recursos asignados para diseñar y administrar los equipos han disminuido en muchas compañías, generando que más carga y expectativas sean asignadas a menos y menos personas. La Calidad del desempeño del sistema instrumentado depende de un sistema de gerencia riguroso que minimiza el error humano y el potencial de falla del equipo. Este artículo se centra en sistemas instrumentados de seguridad y requisitos gerenciales aplicables a la seguridad de procesos. Se muestran observaciones de evaluaciones y auditorias, ilustrando el inadecuado desempeño de los sistemas instrumentados de seguridad, de los procedimientos de mantenimiento y operaciones, del almacenamiento y retención de prácticas y la documentación desactualizada.

Introducción

La industria de proceso ha adoptado rápidamente la automatización para mejorar la calidad del producto y niveles de producción, para reducir el potencial de error del operador y para disminuir la necesidad de mano de obra. La automatización de la industria de proceso incluye muchos sistemas, como controles y alarmas de producción, sistemas de seguridad, y sistemas de mitigación. Nuevas tecnologías a menudo ofrecen beneficios en la producción, calidad del producto y desempeño del costo. Sin embargo, nuevas tecnologías también demandan más esfuerzo y pericia a través del ciclo de vida del equipo instalado. Cuanto más electrónica programable este involucrada en la operación del equipo, más propenso será el sistema a las fallas sistemáticas, las cuales pueden ocasionar una operación impredecible. La automatización confiable conlleva a la operación más segura. La automatización mal implementada o mal mantenida, puede generar eventos peligrosos significativos, impactando a las personas, el ambiente, y los activos.

Un sistema instrumentado de seguridad es un subconjunto de "sistemas de seguridad", los cuales están cubiertos por OSHA 1910.119 (1). Los sistemas de seguridad son objeto de evaluación para satisfacer los requisitos específicos de OSHA PSM (Gerencia de Seguridad de Proceso), así como las reconocidas y generalmente aceptadas buenas prácticas de ingeniería aplicables (RAGAGEP). Los requisitos de PSM manejan cinco aspectos generales:

- Planificación.
- Análisis de Peligros y Riesgos.
- Bases de Diseño.

- Procedimientos de Mantenimiento
- Procedimientos de Operaciones

Cada punto esta presentado más adelante con referencias a párrafos específicos de OSHA PSM. Los problemas y diferencias destacados en este artículo son una recopilación de observaciones del autor sobre los últimos 12 años desde que la ANSI/ISA S84.01-1996 (2) fue publicada por ISA. Si usted reconoce los aspectos de su propia planta o unidad en mis observaciones, considere estas como una confirmación de la realidad de lo que es presentado y un desafío a ser superado por usted.

Planificación - PSM (d)(3)(ii), (d)(3)(i)(F), y (d)(3)(iii)

Muchas plantas o unidades de proceso no tienen un proceso formal de trabajo para asegurar que los equipos cumplen con RAGAGEP. Mike Marshall, (3), ha indicado recientemente en conferencias y en la reunión técnica del comité del CCPS que la visión de OSHA en la aplicabilidad del RAGAGEP es suministrada en una carta de conformidad a Lois Fresón, con fecha de ISA 29/11/2005, con respecto a ANSI/ISA S84.00.01-2004 (4,5). El Sr. Marshall indicó que el nombre de cualquier práctica de la industria podría ser sustituido en la carta donde se haga referencia al estándar 84. En esencia, OSHA espera que las plantas o unidades de proceso identifiquen buenas prácticas de ingeniería que sean aplicables, o desarrollen sus propias prácticas, y demuestren conformidad con las mismas.

> "A favor de una citación de Sección 5(a)(1), los estándares del consenso de la industria, como ANSI/ISA - S84.00.01-2004, pueden ser utilizados como evidencia que un peligro es reconocido y posiblemente puede ser disminuido".(4) Si OSHA identifica que existen prácticas aplicables al proceso que el dueño/operadora no aplicó, el dueño/operadora podría estar en una evidente violación de la cláusula “grandfather” de PSM o a la cláusula general del Acto deber de OSH.

Una cláusula “grandfather” es incluida en el ANSI/ISA S84.00.01-2004 para sistemas instrumentados de seguridad. La cláusula 1y indica que para SIS existentes diseñados y construidos de acuerdo con códigos, estándares, o prácticas antes de la emisión de este estándar (por ejemplo, ANSI/ISA-S84.01-1996), el dueño/operadora deberá demostrar que el equipo es diseñado, mantenido, inspeccionado, probado, y operado en una manera segura. En 2006, el comité de la ISA SP 84 publicó la ISA TR84.00.04 (6), un documento de guía con la ANSI/ISA S84.00.01-2004. El cual indica que hay dos pasos esenciales para determinar la aceptabilidad de los equipos existentes bajo la cláusula “grandfather”:

- Confirmar que el análisis de peligros y riesgos ha sido realizado para determinar cualitativamente o cuantitativamente el nivel de reducción del riesgo requerido para cada función instrumentada de seguridad en el sistema instrumentado de seguridad.
- Confirmar a través de una evaluación que la función instrumentada de seguridad existente ha funcionado acorde al diseño y provee el nivel de reducción de riegos necesitado.

Una evaluación de la cláusula “grandfather” requiere una revisión de la información existente de seguridad de proceso, registros de integridad mecánica, operacionales, del sistema de gerencia y medición. Si el resultado de la revisión es satisfactorio, el dueño/operadora puede elegir mantener el equipo existente tal y como se encuentra. Insuficiencias de desempeño y diferencias en la documentación deben ser corregidas a través de planes de acción para cerrar las desviaciones.

Mientras la evaluación es obviamente una expectativa de OSHA, muchas compañías no revisan activamente los equipos existente contra prácticas actuales. A veces, parece que la gerencia ve las

prácticas de la industria con desidia, como si de algún modo este grupo loco de personas con algún motivo oculto escribiera cosas poco prácticas. Hay poco apoyo para escribir las prácticas internas o el requerir cumplimiento a las prácticas de la industria. Por el contrario, el apoyo se dirige a crear una "interpretación legal" para que la falta de cumplimiento sea aceptable.

Cada vez más los comités de investigación reguladores o independientes publican conclusiones, en las que citan la falta de cumplimiento a las prácticas de la industria. Las expectativas regulatorias y obligatorias son, que el riesgo sea llevado a un nivel tan bajo como sea razonablemente práctico (ALARP). Debido a que el costo principal de los sistemas instrumentados de seguridad es pequeño en comparación con la inversión en los equipos de procesos y de los sistemas de control, los argumentos de ALARP típicamente no son aplicables al SIS. Más aun, la mayoría de las prácticas de la industria, documentan los requerimientos mínimos para la aplicación indicada. Los dueños/operadoras deben demostrar que las desviaciones al RAGAGEP cubren o exceden la intención de la práctica.

Análisis de Peligros y Riesgos - PSM (d)(2)(i)(E) y (e)(3)(iii)

El análisis de peligro y riesgo es un área donde las herramientas de software y técnicas han mejorado substancialmente desde los años 90. Reconociendo la necesidad de capturar lo último en técnicas, CCPS esta publicando una actualización de las guías “Procedimientos para Evaluación de Peligro” [HEP, 7] en 2008. HEP acentúa el análisis de eventos peligrosos y la identificación y reducción del riesgo. Los “safeguards” identificados deben estar cubiertos por información de seguridad de proceso, procedimientos operacionales y de mantenimiento, procedimientos de prueba y entrenamiento. El riesgo residual debe estar manejado con medidas de compensación y planes de acción para reducir el riesgo tanto como sea necesario.

Cada compañía tiene lotes de reportes sobre análisis de peligros y riesgos, pero la calidad de esta información es a menudo muy deficiente. Los informes de estos análisis deben ser considerados documentos oficiales de la compañía para recopilar y distribuir información con respecto a los peligros del proceso y los niveles de protección usados para responder contra ellos. Desafortunadamente, muchas plantas tratan estos análisis como una carga regulatoria y le asignan mínimo tiempo y recursos para realizarlos o soportarlos. Un análisis efectivo de peligro y riesgo identifica los acontecimientos para todos los modos de operación y desarrolla las estrategias para prevenirlos. Un análisis de peligro mediocre, puede tener como resultado la reducción inadecuada del riesgo por la insuficiente definición de la funcionalidad o el desempeño excesivo otorgado a los niveles de protección.

Componer el problema es que la información recolectada es considerada un punto de conformidad y la misma es almacenada. Es accesible, así que cada compañía parece satisfacer la carta de los requisitos del PSM. Sin embargo, la mayoría de las compañías no utilizan esta información para ningún otro propósito. Las compañías no asumen el sentido de pertenencia del análisis del peligro y riesgo. Por el contrario, muchos se quejan del contenido y del poco significado general del informe. El valor del análisis de peligros para el negocio, esta en el uso del informe para entrenar al personal, en cómo las desviaciones de la operación normal se propagan creando peligros en el proceso. El análisis de riesgo define la estrategia de reducción de riesgo seleccionada para manejar el riesgo inaceptable. La Gerencia de planta, ingeniería, operaciones, y mantenimiento deben comprender esta información si ellos son responsables de la toma de decisiones que afectan los peligros o riesgos. Los procedimientos operacionales y de mantenimiento deben incluir una descripción de los peligros del proceso, donde sus acciones potencialmente aumentan el riesgo. Los documentos del análisis de peligros deben ser discutidos por operaciones en las reuniones de seguridad.

Las revisiones del manejo del cambio y análisis de riesgo, frecuentemente fallan en detectar eventos peligrosos. En algunos casos, el análisis no identificó el evento peligroso debido a que la causa iniciadora no fue identificada, la causa no fue considerada creíble, o la severidad de la consecuencia fue subestimada. Existe una tendencia en asumir que los eventos de baja frecuencia no pueden ocurrir en una planta determinada; experiencias previas no son tomadas en consideración producto de la mala suerte ó incompetencia.

El incremento del riesgo derivados de los cambios en la operación de los equipos de proceso y diseño del equipo de seguridad no son evaluados adecuadamente. Muchas unidades de producción están operando apreciablemente por encima de la capacidad original de diseño. Los avances en la tecnología de sistema de control han sido explotados en desventaja de la seguridad permitiendo que las unidades de proceso operen significativamente por encima de la capacidad original de diseño. Algunas de ellas operan muy cercana a la máxima presión admisible de trabajo (MAWP), teniendo como resultado el inadecuado tamaño y activación de las válvulas de alivio de presión así como también la fatiga de los discos de ruptura. El tiempo total de seguridad del proceso se ha reducido a tal punto que a menudo el tiempo es inadecuado para una respuesta efectiva del operador o una respuesta automatizada del sistema. El riesgo se ha escalado o agravado debido a que los competidores incrementan la producción y construyen unidades aun más grandes, mientras los análisis de peligros y riesgos no indican ningún cambio en la escala del incidente.

Bases de Diseño - PSM (d)(3)(i)(H), (j)(6)(i), y (j)(6)(iii)

La información escrita de seguridad del proceso para los sistemas de seguridad a menudo se extravía en muchas plantas. Cuándo está disponible, a menudo no se encuentra “como-construido” y no representa la arquitectura actual del sistema. Una base del diseño “como-construido”, debe estar disponible para todos los sistemas de seguridad con la finalidad de soportar la gerencia del manejo del cambio, la validación apropiada, y el entrenamiento. Para los SIS, la base del diseño incluye la especificación de requisitos de seguridad y la verificación que ese equipo de seguridad satisface las expectativas de reducción del riesgo. La ingeniería de detalle debe asegurar que los equipos sean especificados y configurados como sea necesario para alcanzar el estado seguro y la reducción de riesgo necesaria. Las desviaciones del diseño deben ser justificadas para que sean tan seguras o aun más seguras.

En algunas plantas, las líneas entre la seguridad y el control llegaron a ser confusas en el momento en que los sistemas de control distribuidos fueron originalmente implementados. Lazos separados de control y seguridad fueron combinados dentro de un solo DCS o sistema básico de control de proceso (BPCS). En unos pocos casos, el equipo combinado fue diseñado para ser tolerante a fallas, configurado de manera segura, y gerenciado como seguridad. En la mayoría de los casos, el equipo no es ninguno de éstos. Hay generalmente poca o ninguna información de seguridad del proceso, en el diseño del sistema de control y del sistema de seguridad dentro del BPCS. El equipo compartido no es incluido en el programa de integridad mecánica. Gerencia de manejo del cambio no es aplicada al BPCS.

Los sistemas de control típicos operan en un modo intermitente o continuo, manteniendo el proceso dentro de límites prescritos. Fallas aleatorias y sistemáticas que ocurren a través del ciclo de vida son detectadas tan pronto como las mismas comienzan a afectar la producción y la calidad del producto. Por el contrario, los sistemas de seguridad operan a demanda (o inactivo). Ellos operan sólo cuando el proceso excede una condición específica. Los cambios inadvertidos o deliberados al equipo de seguridad no son fácilmente detectados durante la operación normal. Fallas del sistema de seguridad son identificadas cuando se demanda su operación, a través de pruebas funcionales o demandas reales del

proceso. Si la falla del equipo es identificada a través de las pruebas funcionales, la oportunidad para una mejora continua es evidenciada. Si por el contrario, es encontrada a través de la demanda real del proceso, podríamos estar en presencia de un incidente. Un sistema de gerencia riguroso y documentado reduce el potencial de que el funcionamiento del sistema de seguridad sea derrotado debido a un error humano.

Sin una profunda y clara estrategia de defensa, el diseño y gerencia tienden a decaer al mínimo común denominador. Todo es manejado finalmente como control antes que como seguridad, siendo que la mayor parte del sistema combinado es control. Como resultado, el potencial de causa común es más alto en todos aspectos, inclusive el hardware, software, y operadores. Cuándo el mismo hardware y software son utilizados para el control y la seguridad, fallas o errores no identificados en el equipo instalado o durante el proceso de aprobación del usuario pueden llegar a ser la causa común de falla que conlleva a un acontecimiento peligroso. De ahí, que muchas plantas elijan aplicar soluciones separadas, independientes y de diversidad en controladores, como es discutido en el Anexo F de ISA TR84.00.04.

Integridad Mecánica - PSM (j)(1)(iv), (j)(1)(v), (j)(2), (j)(3), (j)(4)(i), (j)(4)(ii), (j)(4)(iv), (j)(4)(iii), j)(5), (j)(6)(ii), (l)(1), y (m)(1) PSM

El cronograma de programa de integridad mecánica usualmente se basa en objetivos del equipo de procesos en vez de las necesidades del equipo de seguridad. Por ejemplo, el intervalo de la prueba funcional varía con el cronograma de la parada de planta programada sin la mínima consideración en cuanto al impacto que esto pueda ocasionar a la integridad del equipo. Como mínimo, el cronograma debe considerar información previa, recomendaciones del fabricante, y requerimientos de reducción de riesgo. El cronograma de integridad mecánica debe ser ajustado basado en discrepancias o fallas identificadas durante la operación de campo. El cronograma de la prueba funcional debe ser métricamente reportable "enfocado a la gerencia", asegurando probar a tiempo y asignando los recursos apropiadamente. La demora de la prueba funcional debe ser aprobada por el proceso de manejo de cambios, el cual considera el riesgo adquirido en el caso que el sistema de seguridad falle.

Muchas plantas ya no realizan la inspección rutinaria frecuente y el mantenimiento preventivo de los equipos de seguridad. Los avances en la instrumentación han sido tomados como una licencia para extender todas actividades, incluyendo las pruebas funcionales que se ejecutan en la fase de parada de planta programada “turnaround” confiando altamente en la capacidad de diagnostico del equipo para detectar fallas. Probabilisticamente, esto es una filosofía aceptable, siempre y cuando el programa de integridad mecánica mantenga el equipo en su condición inicial "como nuevo". Pero en algunas plantas, el concepto ha sido llevado demasiado lejos. Se asume que el diagnostico del equipo es suficiente, así que ninguna otra inspección, mantenimiento preventivo o pruebas son ejecutadas.

Existen varios problemas con este concepto. La falla debe haber sido identificada anteriormente para que el diagnóstico pueda cubrirla. El diagnóstico interno sufre de un alto grado de causa común y error sistemático. Los fabricantes de los equipos de seguridad generalmente no proporcionan medios para probar el diagnostico interno, así que no es posible para el usuario demostrar que cada diagnóstico funciona como es requerido. EL diagnóstico del equipo raramente cubre periféricos, conexiones del proceso, o sistemas de soporte. Un excesivo crédito al diagnóstico, extienden los intervalos calculados de la prueba funcional, aumentando la probabilidad de falla del equipo.

El mantenimiento del equipo de seguridad a menudo no se encuentra dentro de la lista de prioridades. La Gerencia no parece comprender que el tiempo fuera de servicio es un período de más alto

riesgo. Esto es especialmente cierto cuando las medidas de compensación consisten en solo listar otra tarea de seguridad de alta prioridad al ocupado operador de turno. Esta medida de compensación rara vez logra la reducción de riesgo equivalente. Después de todo, la función principal de los operadores es la producción, no la gerencia de seguridad de procesos.

Los procedimientos de prueba funcional son inadecuados o extraviados para la mayoría de los equipos del sistema de seguridad. Muchos dueños/operadoras asumen que un técnico entrenado sabe cómo probar el equipo. Sin embargo, una prueba funcional demuestra la operación del equipo según la especificación de diseño escrita para mitigar un peligro identificado del proceso. Mientras que el técnico puede comprender cómo realizar las tareas básicas, un procedimiento de prueba funcional detallado es necesario para asegurar una demostración adecuada que el equipo trabaja tal cual lo especificado en cada modo de operación previsto; por ejemplo, el criterio de prueba satisfactoria/fallada para la condición normal, de alarma y parada.

En muchas plantas, bypasses son aprobados fácilmente, sin medidas de compensación planificadas y documentadas. Bypasses permiten que el proceso continúe operando mientras el equipo de seguridad se encuentra en mantenimiento fuera de servicio. En algunos casos bypasses permanecen en el estado de bypass por un periodo de tiempo extendido sin la aprobación de la gerencia de manejo de cambios. En algunas plantas, la visión es que cualquier periodo de bypass está bien, siempre y cuando alguien lo apruebe. En la mayoría de las plantas, operaciones es notificada acerca del bypass temporal, pero a menudo no hay tiempo máximo prescrito en el que el equipo de seguridad pueda estar en una condición de fuera de servicio, sin requerir la aprobación de la gerencia de manejo de cambios. Las reparaciones o bypasses frecuentes no son reportados, registrados y no se realizan seguimientos o tendencias.

Muchas plantas utilizan recursos significativos en el mantenimiento. Sin embargo, muchos programas de integridad mecánica están fallando a causa de la mala calidad de la investigación y seguimiento de fallas recurrentes. Varias mediciones deben ser utilizadas para dar seguimiento al sistema de gerencia de calidad e integridad del sistema de seguridad. La tabla 1 proporciona ejemplos de medición que deben formar parte del sistema de reporte interno de la planta. Las pruebas funcionales deben demostrar que el equipo es mantenido en la condición "como equipo nuevo". Los procedimientos deben indicar claramente los criterios de satisfactorio/falla para que las fallas sean clasificadas apropiadamente. A los registros de mantenimiento deben practicárseles seguimiento y tendencias basados en la tecnología y el ambiente operacional. Fallas en demanda y la operación inesperada deben ser registradas y deben ser investigadas para identificar la causa raíz, y poder tomar las medidas necesarias para reducir la ocurrencia.

Revisión de seguridad en Pre-arranque - PSM (i)(2)(i)

La revisión de seguridad del pre-arranque (PSSR) es un área donde muchas plantas han mejorado desde los años 90. Muchas compañías, están usando una lista de chequeo extensa con la finalidad de abarcar los equipos mayores de procesos y control. Sin embargo, aun continúa una inadecuada evaluación en la documentación del sistema de seguridad, procedimientos y entrenamiento El PSSR evalúa:

- El equipo nuevo o modificado es instalado y demostrado para operar de acuerdo con la intención del diseño.
- Se están utilizando los procedimientos adecuados.

- 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 el libro del CCPS “Guías para ejecutar una revisión efectiva de seguridad del pre-arranque”(8). Para Sistemas Instrumentados de Seguridad, el PSSR es igual a la etapa 3 “Evaluación Funcional” del ANSI/ISA S84.00.01-2004.

Procedimientos Operacionales - PSM (f)(1)(i), (f)(1)(ii), (f)(1)(iv), y (g)(1)(i)

La mayoría de las plantas tienen excelentes procedimientos de control de calidad que cubren el proceso de producción. La influencia de estándares de calidad ISO es verdaderamente aparente. Los operadores están generalmente bien entrenados en los procedimientos operacionales existentes, aún en las plantas donde la desviación a los procedimiento es común. La diferencia es que los procedimientos no cubren todo lo que ellos deberían cubrir.

Muchas plantas no tienen los procedimientos que especifican las acciones que deben ser tomadas por el operador durante operaciones anormales y de emergencia. Los procedimientos a menudo no definen las condiciones específicas del proceso (por ejemplo, nunca exceda, nunca se desvíe) donde la parada de planta es requerida. En estas mismas plantas, al operador se le pide que pare o detenga el proceso, si lo cree necesario. Cuándo "necesario" no es definido, una incertidumbre significativa es introducida en las acciones de operador. ¿Sería la acción correcta y oportuna? El entrenamiento del operador debe incluir el reconocimiento de la seguridad del proceso específico y los peligros para la salud; manejando operaciones anormales y de emergencia, utilizando las prácticas de trabajo seguro, aplicable a las tareas de trabajo. Esto llega a ser aún más importante cuando el operador proporciona "compensación" para el equipo de seguridad fallado o en bypass.

Mientras es ampliamente reconocido que el error humano es uno de las primeras causas de incidentes de seguridad de proceso, este conocimiento no ha tenido como resultado los procedimientos detallados de operación segura. En muchas plantas, los procedimientos operacionales no cubren adecuadamente los siguientes puntos:

- Acontecimientos peligrosos potenciales.
- Descripción de los ISS (por ejemplo, cómo detectar y actuar para detener el evento) y la respuesta esperada del proceso si el sistema actúa como lo planeado.
- Acción del Operador si la función ISS falla.
- Qué acciones tomar cuándo se detectan fallas del equipo.
- Qué acciones tomar en presencia de alarmas.
- Que hacer cuando el sistema no actúa como lo esperado.
- Cuando ejecutar (por ejemplo, condición de nunca exceda, nunca se desvíe) la parada manual.
- Las condiciones requeridas para un arranque seguro.
- Expectativas de reportes para acontecimientos anormales inclusive alarmas de seguridad, enclavamiento “interlock”, y la activación del SIS.

Los procedimientos detallados son esenciales para la operación segura, pero el error humano no puede ser eliminado completamente. W. Eduards Deming, extensamente considerado como el padre de control de calidad, creyó que 85% de la eficacia de un trabajador es determinada por el sistema con que se trabaja, sólo 15% por su propia habilidad. Los procedimientos raramente pueden sustituir al diseño de

falla segura, pero en su lugar deben ser considerados como un suplemento del buen diseño. Buenos procedimientos y equipos en las manos de un operador competente y entrenado son la receta para el éxito. Un buen equipo de seguridad que es bien mantenido, permite que el operador se concentre en la producción en vez de cubrir las insuficiencias del equipo.

Conclusión

Los dueños/operadoras deben aplicar un sistema de gerencia, que incluya procesos de trabajo y mediciones que aseguren que el equipo de seguridad opere consistentemente en una manera segura y cumpla con los requerimientos jurídicos y gubernamentales. Esto requiere un programa completo para identificar e integrar las buenas prácticas de ingeniería, tales como ANSI/ISA S84.00.01-2004, en procesos de trabajo. Las prácticas y los procedimientos internos deben definir claramente las expectativas, para que la calidad de la tarea sea factible, aun cuando la tarea sea ejecutada por el mejor empleado, un empleado promedio, o un empleado algo distraído.

Los procesos de trabajo y actividades recomendados para sistemas instrumentados de protección están previstos en la publicación del CCPS “Lineamientos para Sistemas Instrumentados de Protección” (9) y para Sistemas Instrumentados de Seguridad en la ISA TR84.00.04. Los siguientes puntos deben ser reunidos y mantenidos durante la vida del equipo:

- Reportes de los análisis de peligros y riesgos.
- Documentos de Bases de Diseño.
- Procedimientos de Operaciones, pruebas y mantenimiento.
- Registro de las Inspecciones, pruebas funcionales y mantenimiento.
- Reportes de fallas (por ejemplo, informes de disparo de planta y de falla de equipo).
- Informe de investigación de incidentes y “Near miss”.
- Registro de manejo de cambios.
- Registro de Entrenamientos.
- Informe de Auditorias.

Referencias

OSHA, “Process Safety Management of Highly Hazardous Chemicals; Explosives and Blasting Agents, 29 CFR Part 1910.” Federal Register 57, 36, Washington, DC (1992).

Instrumentation, Systems and Automation Society (ISA), ANSI/ISA S84.01-1996, “Application of Safety Instrumented Systems (SIS) for the Process Industry,” Research Triangle Park, NC (1996).

Mike Marshall, OSHA Directorate of Enforcement Programs, 2007 Center for Chemical Process Safety (CCPS) technical steering committee meeting, Salt Lake City, Utah (2007).

OSHA, correspondence, Richard Fairfax, Director, Directorate of Enforcement Program, to Lois Ferson, Manager of Standards Services, Instrumentation, Systems and Automation Society, DEP/GIE/SMK, dated November 29, 2005.

ANSI/ISA S84.00.01-2004, Functional Safety: Safety Instrumented Systems for the Process Industry Sector, Instrumentation, Systems, and Automation Society, NC (2004).

ISA TR84.00.04, Guidelines for the Implementation of ANSI/ISA S84.00.01-2004 (IEC 61511), Instrumentation, Systems, and Automation Society, NC (2005).

Guidelines for Hazard Evaluation Procedures, 3rd edition, American Institute of Chemical Engineers, NY (2008).

Guidelines for Performing Effective Pre-Startup Safety Reviews, American Institute of Chemical Engineers, NY (2007).

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

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.