El rol y estado de la tecnología en la prevención del accidente.

(Notas tomadas del libro Accidentes y Riesgos Sociales, H.E. Ecay – HEE Consultores)

En la integración de un determinado sistema de seguridad o de toma de decisiones, donde el hombre y ciertos mecanismos en forma combinada son responsables de un dado parámetro o variable de proceso, el hombre será considerado un simple block con una tasa de falla asignada al igual que los restantes componentes no biológicos.

Si bien el hombre puede controlar más de un lazo de seguridad o control, los sistemas inanimados también pueden hacerlo, y en cada caso particular se evaluará el riesgo del sistema aplicando las tecnologías de árboles de falla, árboles de eventos y teoría del riesgo. La tecnología actual sobre la medición del riesgo con el apoyo del entrenamiento (bancos de simulación), verificación, calificación, auditoria y validación permite este logro.

Los factores humanos que influyen al momento de tomar una decisión dependen de un gran número de condicionamientos. Estos factores son de diferente índole y de gran importancia. Lo curioso de esto es que el hombre en si mismo, afectable por cansancio, aburrimiento, tedio, miedo a la decisión, entre otras cosas, logra, combinado con sistemas automáticos, optimizar la ingeniería del riesgo. Todo el análisis permite disminuir el riesgo para las personas y maquinarias del ámbito en cuestión.

La ingeniería de proyecto debe saber prevenir situaciones de riesgo inmediatamente o casi inmediatamente al darse la alarma y finalmente contar con la actuación de un sistema de seguridad. En esta etapa la conducción del evento se confía al operador del sistema en cuestión que con conocimiento y decisión transfiere el automatismo a control manual y opera el sistema de la mejor manera.

Un ejemplo significativo donde la capacidad humana se muestra con toda claridad, es en procesos complicados continuos, donde los sistemas automáticos son mayormente en serie, y las variables individuales de los diferentes equipos que componen el proceso tienen efectos mutuos. La capacidad de un operador para relacionar el comportamiento contagioso de varias variables del proceso y poder averiguar donde está la causa de inicio es una función extremadamente difícil para ser automatizada, a lo que se agrega la rapidez para salvar el problema y defender la planta de la mejor manera posible. Así el operador capacitado y entrenado, puede descubrir fallas evitando consecuencias que podrían llegar a ser terribles.

Cualquier problema que pueda resultar en daños considerables o hasta tal vez irreversibles, como puede ser la pérdida de una vida, requiere de la toma de decisiones rápidas y acertadas. Para esto la capacidad humana que depende de una capacitación y entrenamiento adecuados en las tareas de control y seguridad es primordial a la hora de evitar graves consecuencias.

En estos contextos tecnológicos podemos dar por sentado que además de los trabajadores hay un sistema auxiliar muy complejo que diagnóstica fallas y da consejos. Algunas veces la

cantidad de información y variables a considerar es muy grande por lo que la inteligencia de esta programación sirve de ayuda en ciertas ocasiones para enfrentar situaciones en que resulta difícil la toma de decisiones.

Se puede concluir que es necesaria la variable humana para todos los procesos, por eso cada uno es interpretado (proceso industrial, sistema de transporte, generación de energía, etcétera) y se corresponde con un sistema de seguridad en que participa lo humano y lo robótico o sistema programado para complementar las necesidades.

Se puede resumir que asesorar el riesgo significa evaluar los factores que deben ser mejorados, teniendo siempre en cuenta el sistema en el cual se insertará al hombre y los valores resultantes de incorporar el automatismo. Debemos saber que el hombre es un componente más, sin ser subestimado, dentro de un sistema de seguridad que debe hacerse responsable por la parte a mejorar del riesgo que corresponda.

Los últimos modelos de gestión no se han separado del análisis de riesgo. Esto ha derivado en la creación de estándares y códigos que reglamentan el tema y en el que se basan todas las actividades correspondientes a su asesoramiento.

En algunos países desarrollados tecnológicamente estas normas son reconocidas como sistemas regulatorios con fuerza de ley. Estos códigos y normas fundamentan el riesgo como base del mantenimiento industrial moderno.

Un grupo de normas, códigos y regulaciones extranjeros son:

- OSHA-29 CFR 1910.119 “Gestión de la seguridad de proceso” (1992).
- API- 580 y API – 581 “Inspección basada en riesgo” (Mayo 2002).

- API-579 “Servicio adecuado” Fatiga y Fractomecánica
- ASME “Criterio de aceptación del riesgo” (Febrero 2000).
- ASME “Prueba de riesgo en marcha” General Doc. (2000).
- IEC 61508 Estándar internacional “Seguridad funcional de los sistemas relacionados con la seguridad” (1998 al 2000). Conformado por siete partes y direccionada a la industria en general. Queda actualmente como marco general de otras normas específicas (marco de trabajo).
- IEC 61511 “Sistema instrumentado de seguridad para el sector industrial de proceso” (2002 al 2003). Conformada por tres partes y destinada a las industrias del tipo petroquímicas, químicas, fertilizantes, metanol, refinerías de petróleo, extracción y separación de gas y petróleo, etc.
- IEC 62061 Mach. Seguridad – “Seguridad funcional relacionada con los sistemas de control programables electrónicos, electrónicos y eléctricos”
- ISO 14121 Mach. Seguridad – “Principios del asesoramiento del riesgo”.
- ISO 12100 Mach. Seguridad – “Conceptos básicos, principios para diseño”.
- ISO 13849 Mach. Seguridad – “Seguridad relacionada con partes de los sistemas de control”.
- ANSI/ISA – S 84.01-1996 “Para usar en aplicaciones de seguridad”. Sistemas instrumentados de seguridad para la industria de proceso. EPA-Agencia de Protección ambiental – Plan de gestión de riesgo. Regulación – 40 CFR 68.220-(1998)-58 FR 54190.

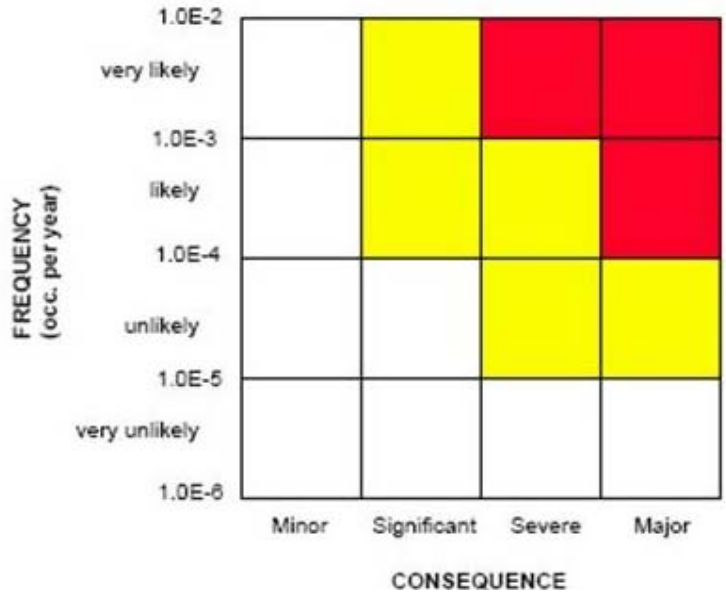
La aplicación de estos estándares, códigos y regulaciones generan una mezcla de disciplinas conjuntamente con una “visión y misión empresarial” que marca el rumbo común para todos los integrantes.

Las etapas claves de aplicación:

- Verificación: (interpretación de IEC 61511/ISA S84). El diseño conceptual es verificado contra las especificaciones requeridas de seguridad – verificación del nivel de integridad y seguridad ¿Lo entregado se ajusta a lo especificado?
- Validación: (interpretación de IEC 61511/ISA S84). Es la actividad que prueba que el sistema de integridad y seguridad trabaja. Incluye una prueba completa de entrada y salida.
- Control por auditorías: Enfatiza la importancia de asegurar el desempeño a largo plazo. El sistema de integridad y seguridad deberá ser auditado para determinar la tasa real de demanda. En el sistema de integridad y seguridad deberán ser registradas las tasas de falla.

El riesgo se define como el producto matemático de la frecuencia del evento por la consecuencia del mismo. Se expresa de manera cuantitativa con unidades específicas para cuatro conceptos diferenciados:

1) Interrupción del negocio ($ / año).
2) Daños a equipos (pies cuadrados / año).
3) Efectos a la salud (pies cuadrados / año).
4) Impacto ambiental ($ / año).



El trabajo del especialista consiste en relacionar el riesgo con la integridad requerida según los códigos y verificar si el equipo o sistema cumple con esta integridad intrínseca (física) o funcional. Los códigos referenciados son mandatorios solamente en cuestiones muy básicas, dejando al buen criterio del especialista la interpretación de los mismos y cumplimiento de las reglas.

La falla de la integridad física es el “deterioro físico ocasionado por mecanismos de falla, que producen el colapso mecánico del equipo o sistema”. Corrosión química, daño metalúrgico, fatiga, fragilidad, fracto-mecánica, avance de fisuras, etcétera.

Las dos instituciones mecánicas principales API y ASME no tienen diferencias ideológicas, pero sus técnicas y metodologías siguen distintos caminos de análisis y aplicación.

Criterio API: Partiendo de la frecuencia de falla universal de un equipo para un determinado mecanismo de daño, ajusta la misma a las características del proceso y de la empresa específica, aplicando gran cantidad de variables (componentes de riesgo) y calcula la severidad del accidente por un método cualitativo o cuantitativo que establece el propio código.

Criterio ASME:

- FMEA (Modos de falla y análisis de efectos)
- FMECA (Modos de falla y análisis crítico de efectos)
- HAZOP (Estudio del peligro y la operabilidad)
- FTA (Análisis de árboles de falla)
- ETA (Análisis de árboles de evento)
- MLD (Diagrama lógico maestro)
- What – If (Set de preguntas)
- Construcción de la lista de chequeo
- Mantenimiento de la lista de chequeo
- ¿Que pasa si? o What-If / Lista de chequeo

- Diagramas de causa y efecto

Este listado de herramientas que aplicadas correctamente en forma individual o en conjunto según la necesidad permiten evaluar, modificar, aminorar o validar el nivel de riesgo de un equipo o sistema para alcanzar el valor tolerable en un todo de acuerdo a lo establecido por los códigos o regulaciones.

Las dos instituciones líderes en la evaluación cuantitativa y cualitativa de la integridad funcional de los sistemas instrumentados de seguridad son:

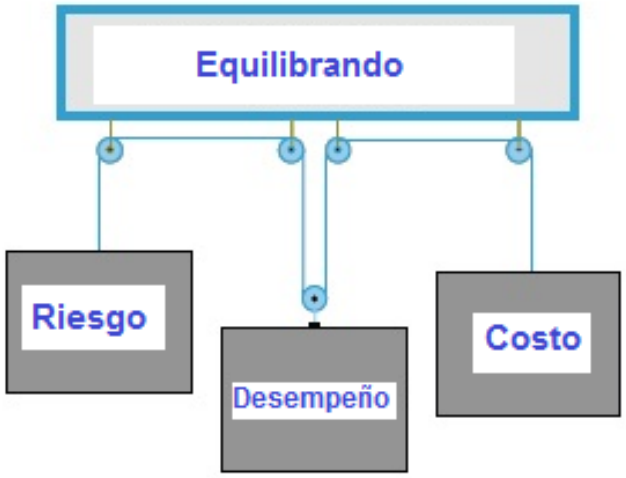
- IEC - Comisión internacional electrotécnica 61508/61511.
- ISA - Sociedad de instrumentos de América - ANSI/ISA-S 84.01-1996.

Ambas instituciones son autosuficientes, cada una de ellas en su objetivo de alcance. IEC establece los métodos para obtener el nivel de integridad de seguridad de un sistema de protección (eléctrico, electrónico y programable electrónico) e ISA se ocupa de la aplicación de los sistemas instrumentados de seguridad.

El manejo del concepto de aleatoriedad en los fenómenos naturales que están involucrados en las fallas intrínsecas y funcionales de los equipos y sistemas de los procesos industriales es de gran importancia para poder desarrollar un programa de mantenimiento general basado en el riesgo logrado a través de la confiabilidad, disponibilidad y mantenibilidad. El objetivo consiste en identificar los equipos y sistemas con riesgo crítico, concentrar recursos humanos y tecnológicos en ellos aumentando frecuencias de inspección y mejoras en la efectividad de los procedimientos, diseñando arquitecturas redundantes de mayor confiabilidad para controlar los mecanismos de deterioro principales de los componentes y disminuir la tasa de falla y reduciendo el valor del riesgo al aceptable acorde a códigos y regulaciones siempre alcanzando la mayor efectividad económica y técnica posible.

Haciendo un poco de historia vemos que durante el siglo veinte se consiguieron mejoras significativas en las áreas de gestión de tecnología, procesos y personas. Esta evolución se concretó por medio del uso y desarrollo de herramientas que fueron útiles para aumentar la productividad de bienes y servicios, bajar la tasa de accidentes mayores y de seguridad personal, mejorar la calidad de lo producido así como también aumentar la confiabilidad de la tecnología y por ende su disponibilidad. En resumen productividad con calidad, seguridad y predictibilidad de abastecimiento fueron los objetivos que se persiguieron en la generación de bienes y servicios.

Durante los últimos años estas mejoras en los resultados han entrado en una meseta y para poder salir de este estancamiento las nuevas herramientas propuestas por las instituciones normativas globales y empresas líderes son la Confiabilidad tecnológica y humana cuantitativa, la Gestión del riesgo cuantitativo y la Integridad operacional.



Vemos también como la gestión tradicional de equipos y personas migra hacia una gestión en base a procedimientos, riesgo y confiabilidad de equipos y humanos. Los antiguos enfoques del API 51, 653, 570, 510 e IEC 61508 actualmente se complementan con los API 770, 581, 579 e IEC 615011 introduciendo conceptos de riesgos y confiabilidad física, funcional y humana. (1; 2; 6; 8; 9; 12; 14; 15; 18)

Las técnicas preventivas y predictivas complementan también las herramientas de confiabilidad tecnológica para la disminución de riesgos. Las preventivas son técnicas que se mejoran sustancialmente cuando se trabaja en base a confiabilidad, dado que permite en forma cuantitativa y probabilística identificar la frecuencia óptima de mantenimiento para una determinada tecnología.

El análisis cuantitativo del riesgo industrial se deriva de la confiabilidad tecnológica que nos permite agregar un elemento que pondera no solo la frecuencia con que se desencadena una falla si no también su consecuencia.

La primera herramienta que se analizará es la llamada tasa de falla que es aplicable en forma indistinta a humanos y tecnología. También es necesaria para el cálculo de la confiabilidad. Se la representa por la letra griega λ y su traducción al inglés es “Failure Rate”. La definición que utilizaremos en este libro es “la expresión del numero de fallas de un equipo, persona o conjunto de equipos o personas por unidad de tiempo y en un determinado contexto o escenario”. Por ejemplo: La tasa de falla de siete reductores de velocidad iguales que funcionaron durante un año produciendo una sola falla en uno de ellos en ambientes protegidos es de: λ=1/7 fallas-año. Existen dos formas básicas de obtener las tasas de fallas, la primera es por obtención de datos propios de mecanismos y modos de fallas junto con los períodos a la rotura o indisponibilidad definiendo también el contexto o escenario de cálculo. La segunda manera de obtener las tasas de falla que es principalmente útil cuando no se tienen datos o antecedentes es por medio de los provistos por el mercado. Durante el diseño de un plan de confiabilidad y prevención de riesgos de una nueva tecnología se pueden usar las tasas de falla descriptas en publicaciones específicas.

Las tasas de fallas decrecientes típicamente representan los períodos de arranque o garantía de una instalación, y los crecientes en el tiempo representan la obsolescencia de la facilidad o algún modo de falla exponencial.

Una tasa de falla constante en el tiempo nos indica que la rotura se puede dar aleatoriamente en cualquier instante de tiempo, por lo tanto las estrategias de mantenimiento de este tipo de situación se relacionarán principalmente por establecer redundancias, monitoreos de condición y trabajar a la rotura, las técnicas de mantenimiento preventivo serán poco efectivas.

Enfocando ahora hacia la confiabilidad, la definición que se cree conveniente para el propósito de este libro es: "la función matemática cuyo resultado se expresa en porcentajes y su significado es la probabilidad de que un equipo, persona o conjunto de equipos y personas tenga cero falla en su misión asignada en un período de tiempo y en un contexto operativo definidos". Este parámetro es el principal indicador de calidad y desempeño de equipos, tecnología y humanos involucrados. Si se habla de tecnología por un lado, como se dijo, es un indicador de la calidad de diseño y construcción de un equipo, y por el otro, de la calidad de ejecución del plan de inspección y mantenimiento.

Otras variables necesarias para trabajar sobre integridad tecnológica son las del tipo de probabilidades puras, probabilidad de un evento, probabilidad de éxito y probabilidad de fracaso. Por ejemplo: la probabilidad de sacar un seis en un dado es de p=1/6. La probabilidad de no sacarlo es de q=5/6. Estas variables son utilizadas principalmente cuando usamos la herramienta de árbol de eventos para el cálculo de las frecuencias de riesgo de escenarios conocidos.

Cabe destacarse que cuando hablemos de consecuencias cuantitativas nos referiremos a las formas más usuales de expresarlas: en dinero, número de accidentados humanos, cantidad de equipos indisponibles y áreas contaminadas o desbastadas. La consecuencia es uno de los dos parámetros más importantes del riesgo industrial que cuenta con la probabilidad como el parámetro principal.

La severidad de un determinado evento puede ser expresada en: dinero, área impactada y en fatalidades. Estas últimas son las que más interesa remarcar en este libro, a pesar de la tecnicidad de este capítulo.

Los distintos tipos de riesgos que más importan en el ámbito industrial son: riesgo físico (sobre equipos y personas), riesgo funcional (control y seguridad de proceso), riesgo humano y riesgo de seguridad, salud y medio-ambiente.

Al mismo tiempo y como ya se nombró, el riesgo se puede dividir en riesgo cuantitativo y cualitativo.

La principal y más utilizada definición del riesgo es la que deviene de un modelo de dos variables "el producto de la probabilidad de un determinado escenario o evento multiplicado por su consecuencia de concreción". Las unidades más comunes del riesgo son dinero/tiempo, heridos/tiempo y área impactada/tiempo.

Para poder clarificar este parámetro debemos entender previamente que una industria en su área industrial o de proceso tiene dividida su tecnología en los siguientes niveles:

- Nivel de equipos, máquinas o tecnologías susceptibles de ser analizadas bajo conceptos de riesgo y confiabilidad, por ejemplo un tanque de producto
- Nivel de control del proceso, por ejemplo, el control de la temperatura del producto contenido en el tanque del ejemplo anterior
- Nivel de seguridad del proceso, en el caso de la seguridad de un tanque se usan alarmas de alto nivel y temperatura que evitan explosiones o rebalses de productos tóxicos
- Nivel humano con acciones de operación y mantenimiento