EXPERIENCIA DE YPF S.A. CON SISTEMAS INSTRUMENTADOS DE SEGURDAD

Fabián Verdun
fverdunm@ypf.com
YPF S.A.

1.- Introducción

Hoy en día la seguridad de los procesos de refinación es un aspecto crítico para la preservación de los activos, del medioambiente y de las personas. La seguridad funcional contribuye directamente en la seguridad de éstos, generando las acciones correctivas sobre dispositivos automáticos en respuesta a actuales o potenciales condiciones de peligro y evitando así que eventos se desarrollen por completo y activen mecanismos de mitigación de sus posibles consecuencias.

Las funciones instrumentadas de protección que usan tecnologías eléctricas-electrónicas se han valido de sensores, logic solvers y elementos finales para llevar al proceso a un estado seguro. Estos Sistemas Instrumentados de Seguridad fueron usados genéricamente por la industria durante muchos años proveyendo protección contra las desviaciones de proceso. La correcta gestión de estos aspectos de seguridad funcional es globalmente aceptada como una de las mejores formas de reducir el riesgo inherente en procesos industriales peligrosos.

Los estándares internacionales están conduciendo a los usuarios finales a adoptar las normas IEC61508/61511. El objetivo de estas normas es hacer de la seguridad una prioridad durante todo el ciclo de vida de cualquier planta o proceso potencialmente peligroso. YPF no es ajena a este tema y ha confeccionado sus propios estándares internos en función de las mencionadas normas. Con la vigencia de esta nueva normativa dentro del ámbito de la Compañía se decidió realizar un proyecto piloto para aplicar lo resuelto y con el objetivo de sacar conclusiones sobre el impacto de la implementación de la normativa en relación con la gestión de los sistemas SIS, concretamente en aspectos de tiempo, costes, personas e instalaciones.

Este trabajo busca mostrar lo aprendido en Sistemas Integrado de Seguridad que hasta el momento se han explorado a través del proyecto piloto. Cabe mencionar que actualmente se ha concluido con las dos primeras etapas del ciclo de vida, análisis de riesgo y asignación de SIL, y se está trabajando en las especificaciones de requisitos de seguridad. Contamos con una experiencia anterior en una unidad de Hidrocracking (Isomax).

2.- Desarrollo

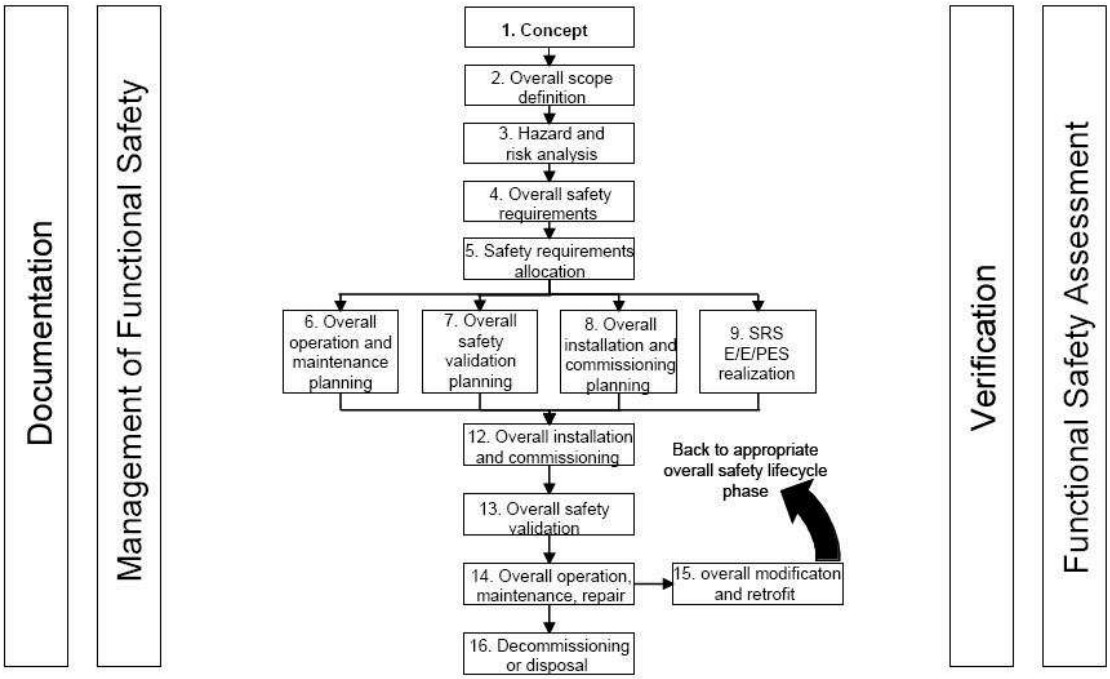
2-1.- Ciclo de Vida

La industria de proceso ha adoptado la automatización para mejorar la calidad de sus productos y las tasas de producción, reduciendo el error potencial de operación. La automatización incluyó diferentes sistemas instrumentados tales como el control de proceso, gestión de alarmas, sistemas instrumentados de protección y sistemas de parada de emergencia.

Mientras que las últimas tecnologías en instrumentación y control requieren menos soporte, una vez implementadas, la complejidad aparejada con éstas puede requerir un mayor grado de atención durante las etapas de evaluación, diseño, inspección, testeo, y mantenimiento. Las fallas no deseadas pueden ocurrir durante periodos largos de operación dejando al sistema incapaz de realizar las acciones especificadas. Esto es fundamentalmente cierto en los sistemas electrónicos programables debido a la gran combinación de posibles fallas entre sus elementos de hardware y software que comprometerían al sistema.

Grandes fueron los esfuerzos realizados con el fin de preservar y mantener al margen de la operación los peligros, mediante su identificación y posterior control. Sin embargo las catástrofes se repiten alrededor del mundo. En todos aquellos casos hay una amenaza en común que nos dice que existe un problema cultural dentro de las organizaciones, que permite tomar decisiones en contra de la seguridad.

El desarrollo de una cultura de la seguridad requiere de valores y políticas que puedan ser convertidas en prácticas y comportamientos. La política de “Operación segura es nuestra misión” debe ser respaldada por autoridades, con recursos y herramientas necesarias para ponerla en práctica. Desde los operadores de campo hasta la Dirección de la empresa deben entender y convencerse que la operación segura es el corazón de los principios de operación. Se recomienda realizar auditorias periódicas de las prácticas vigentes para verificar que se cumple con los procedimientos internos; comunicando además, que la operación segura es la recompensa al esfuerzo y que por el contrario una operación no segura no será tolerada.

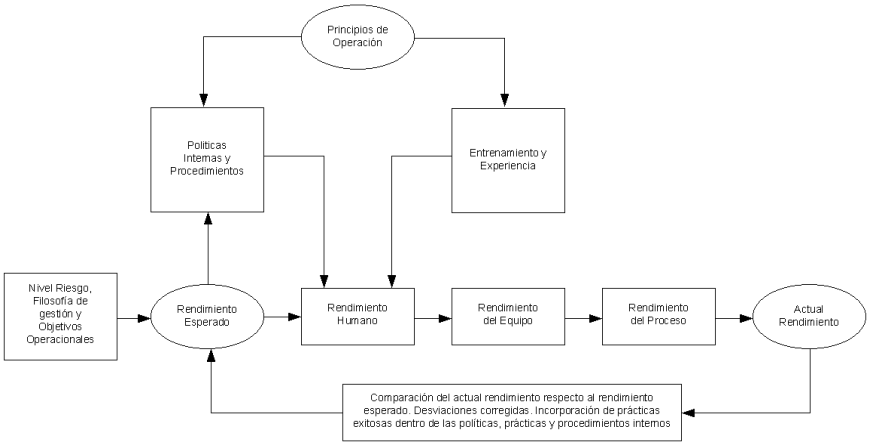


CICLO DE VIDA

Uno de los mayores avances introducido por la norma IEC 61508 es que su espectro no solo abarca los requerimientos técnicos del sistema de protección, sino que tiene en cuenta el trabajo de selección, desarrollo, uso y administración de dicho sistema. Esto se ve plasmado en el concepto de "Ciclo de Vida", que ordena todas las actividades relacionadas con el sistema de protección de manera sistemática.

Es fundamental hacer hincapié en la administración de los sistemas como elemento clave en el ciclo de vida. La administración recomendada es la que establece un grupo de características

fundamentales que mantendrán la calidad de las funciones instrumentadas. La administración sugerida combina prácticas internas, conocimiento, habilidades y experiencia para alcanzar y mantener el principio fundamental de la operación. A continuación se presenta un modelo planteado:



El nivel de exigencia usado en los controles y monitoreo del corazón de nuestro principio de operación puede afectar el actual rendimiento de nuestras funciones instrumentadas. Las funciones instrumentadas ya implementadas pueden ser monitoreadas por indicadores que involucren al personal, el equipo y el proceso, por ejemplo algunos de ellos pueden ser: fallas detectadas, tanto peligrosas como seguras, demanda del proceso, y nivel del personal que interviene. Estos indicadores y otros que se pueden incorporar deben permitir a la administración detectar rápidamente que la integridad mecánica y operacional de los equipos es insuficiente para mantener segura y fiable la operación.

El primer paso en el camino de una buena administración de los riesgos operacionales es el entendimiento de los mismos a través del análisis de peligros y riesgos. Es aquí donde nuestra refinería ha realizado los primeros pasos relacionados con esta norma. A continuación comentaremos nuestra experiencia en el tema.

2-2.- Evaluación del peligro y riesgos.

En el marco del proyecto piloto para la refinería Luján de Cuyo se ha determinado que la planta involucrada dentro de esta primera experiencia integral sea la unidad de FCC II, dicha unidad consiste básicamente en un Reactor-Regenerador, torre fraccionadora con múltiples cortes y una sección de gases. Procesa corrientes de Gas Oil Pesado proveniente de los Toppings como así también de las unidades de Vacío, Coque; y además, carga fría de tanque (intermedio oscuro), nafta de Coque o intermedio liviano (ambos como quench al riser); para obtener productos mas livianos, que se fraccionan en fuel gas, propano, butano, nafta, diesel oil, gas oil pesado y gas oil decantado

Este estudio realizado por YPF es parte de sus buenas prácticas del Negocio, a los efectos de reducir los riesgos asociados a la operación y se encuentra enmarcado dentro de su norma corporativa (SCOR N°12). El alcance del estudio comprendió los sistemas descritos por los planos de instrumentos y cañerías (P&IDs) como así también toda la información disponible de los equipos involucrados en el proceso. El método HAZOP (Hazard and Operability) es una técnica formal para la identificación de peligros potenciales y problemas de operación de procesos que involucran altos riesgos. Esta técnica, nacida a mediados de la década del 60, se ha convertido en un estándar de la industria química, petroquímica y petrolera en la actualidad. Su principal basamento es que los peligros no se manifestarán como daños si la planta se opera dentro de las intenciones del diseño.

Por lo tanto, el método plantea las posibles desviaciones, respecto de las intenciones del diseño, que pudieran ocurrir y trata de encontrar causas razonables que puedan provocar esas desviaciones. Si existen causas razonables para las desviaciones, se evalúan las consecuencias del peligro y su frecuencia probable de ocurrencia y se determina si es necesario realizar una actividad determinada para eliminar, minimizar o mitigar las consecuencias.

Si bien esta técnica es muy conocida pueden existir diferencias significativas en cuanto a la calidad de los análisis debido a la ausencia de procedimientos que establezcan la base para el análisis. Nada puede causar más frustraciones al momento del diseño que ver diferencias en los requerimientos para peligros similares, evaluados por equipos diferentes o incluso por el mismo equipo. Sin procedimientos claramente detallados por parte de la Compañía es posible encontrar variaciones de riesgos significativas que pueden ir desde no requerir reducciones de riego a reducciones de riesgo extremas.

En nuestro caso, y para el análisis realizado se han tomado las aclaraciones indicadas en la norma mencionada estableciendo el criterio uniforme durante el estudio. A continuación se muestra una de las tablas de la norma que se usaron para estandarizar el análisis realizado sobre la unidad de FCC II.

Capa de protección independiente	Comentarios	Probabilidad de fallo típica	Crédito IPL típico
Válvula antiretorno única en servicio de líquido limpio	Previene el flujo inverso (líquidos).	10^{-1} - 10^{-2}	**1**
Válvula antiretorno única en servicio de gas	Previene el flujo inverso (gases).		**0**
Dos válvulas antiretorno en serie	Dos válvulas antiretorno en serie. Previene el flujo inverso (líquidos o gases).		**1**
Disco de ruptura	En serie antes de una PSV. Servicio limpio.		**2**
Disco de ruptura	En serie antes de una PSV. Servicio sucio.		**1**
Válvula de alivio de presión (PSV o PRV)	Si se diseña, instala y mantiene adecuadamente previene una sobrepresión (salvó en caso de runaway). La PDF se refiere a no abrirse en demanda (100 % de la sección). Servicio limpio.	10^{-2} – 10^{-3}	**2**
Válvula de alivio de presión (PSV o PRV)	Si se diseña, instala y mantiene adecuadamente previene una sobrepresión (salvó en caso de runaway). La PDF se refiere a no abrirse en demanda (100 % de la sección). Servicio sucio.	10^{-2}	**1**
Múltiples PSV	Si se diseña, instala y mantiene adecuadamente previene una sobrepresión (salvó en caso de runaway). (2 × 50%) (4 × 25%)	$2*10^{-2}$ – $4*10^{-2}$	**1**
Lazo de control/BPCS[3]	Un lazo de control puede ser IPL si es independiente del suceso iniciador y de la SIF objeto de estudio	10-1	**1**
Sistema de control específico de ciertos equipos	Compresores, hornos, calderas, etc.	10^{-1} - 10^{-2}	**1**

Consecuentemente, los procedimientos deben ser sistemáticos, para reproducir siempre el mismo resultado con diferentes personas, tomando en cuenta la información del proceso y siendo posible realizar auditorías, revisiones de control, y ser consistente con las buenas prácticas de ingeniería. Lo que se espera de estos procedimientos o guías es:

- Definición del alcance.
- Aplicabilidad del método.
- Identificación de los recursos y responsabilidades.
- Definición del criterio de riesgo.
- Guía de como evaluar las consecuencias.
- Guía para determinar las frecuencias de los eventos evaluados.
- Requerimientos de documentación.

Estos procedimientos en el caso de YPF se encuentran en guías de realización del trabajo que se desprenden o se enmarcan dentro de las normas corporativas.

2-3.- Asignación de SIL

El alcance del estudio comprendió los eventos más importantes identificados en el análisis de riesgo (HAZOP). Los eventos identificados fueron desarrollados y comprobados bajo el criterio de riesgo establecido a fin de verificar la estrategia de reducción de riesgo. Para poder cumplir con esto, el grupo de trabajo debe incluir a personal con experiencia en la operación de la unidad y de sus capas de protección. Incluso se ha determinado un nivel superior de riesgo que dispara o habilita la realización de un estudio cuantitativo de las probabilidades de falla a fin de establecer la existencia o no de una capa de protección de gran reducción de riesgo.

Una causa iniciadora de un evento peligroso desencadena una sucesión de eventos que se propagan hasta alcanzar un evento peligroso, si no hay acciones que lo detengan. Por ejemplo, un lazo de control básico que falla abriendo su válvula permitirá que la presión en el recipiente donde descarga se incremente. La falla del lazo puede atribuirse a la falla de un sensor, al controlador, posicionador, válvula o algún otro equipo relevante. La frecuencia de ocurrencia de estas fallas determina la frecuencia del evento. La consecuencia de un evento, evaluadas en el peor caso creíble, determinara la severidad del mismo, que junto a la frecuencia definirán el riesgo asociado para dicho evento. El grupo debió determinar si el nivel de riesgo determinado en este análisis no viola los niveles admitidos por la Compañía, en cuyo caso no se requiere realizar acción alguna. Por el contrario si dicho nivel se encuentra por encima, el grupo debe identificar capas de protección que reduzca el nivel de riesgo a valores tolerable, si las capas de protección estándares no logran cumplir el objetivo de bajar el nivel de riesgo, se deberá pensar en capas de protección instrumentadas o en mejorar las existentes.

Cuando el riesgo del proceso excede el nivel de riesgo establecido para la compañía, se debe identificar la capa de protección instrumentada a la cual se le asignaría la diferencia (gap) entre el nivel de riesgo que existe y el admitido por la Compañía. La apropiada identificación es sumamente importante, porque la ejecución de las fases restantes del ciclo de vida depende de ello. Potenciales fallas comunes entre las distintas causas y las funciones de protección deben ser consideradas para cada evento peligroso.

Particularmente en esta etapa se utilizó un software desarrollado por la empresa IHF Consultora, en donde se volcaron las gráficas de riesgo definidas por la Compañía. Calculando en base a la información del análisis de peligro realizado previamente, los distintos gaps requeridos para cada una de las funciones instrumentadas identificadas.

Como resultado de esta etapa se puede decir que dentro de las funciones instrumentadas analizadas se ha encontrado con la siguiente distribución:

- 36 funciones de nivel de integridad 1
- 26 funciones de nivel de integridad 2
- n/e funciones de nivel de integridad 3

Actualmente nos encontramos en la etapa de realización de los requisitos de seguridad de cada una de las funciones de seguridad. Básicamente lo que se intenta realizar es generar un diseño básico de la función indicando sus sensores, PLCs de seguridad y actuadores sobre los que actuará. Respaldando cada una de las decisiones con los cálculos correspondientes de reducción de riesgo que dicha función debe alcanzar como restricción del diseño, para ello se ha utilizado un software de cálculo. Estas tareas en experiencias anteriores no fueron realizadas y creemos que fue una de las causas que impidieron alcanzar el nivel de reducción de riesgo requerido para algunas funciones instrumentadas de seguridad.

3.- Conclusiones

Dentro de esta experiencia nos parece importante resaltar como puntos más destacados lo siguiente:

1) La gestión de las funciones instrumentadas de seguridad debe ser responsable de que la calidad de las mismas se mantenga durante la vida de cada una de ellas. En caso de detectar deterioros disparar las acciones correspondientes tendientes a corregir estos desvíos.

2) Es importante determinar cuales son los procedimientos que nos da la Compañía para realizar un análisis sistemático. De manera que los resultados puedan ser reproducidos en situaciones similares o por otros grupos de trabajo.

3) Se debe generar la cultura de la seguridad con políticas y valores. Estableciéndola como corazón de los principios de la operación.

4) La demanda de trabajo que se ha requerido para cumplir con estas etapas nos sugiere que es necesario incrementar los recursos humanos involucrados como así también su nivel técnico y de gestión para este tipo de sistemas.

La experiencia resultó muy positiva para el Complejo permitiéndose capacitar, actuar y diseñar en base a este nuevo estándar. Quedan grandes desafíos por delante pero que implicarán mantener al margen de nuestras operaciones el desarrollo de eventos peligrosos.

4.- Bibliografía

a) Safety Integrity Level Selection, Ed Marszal y Eric Scharpf (ISA)
b) IEC 61508, An Introduction To The Safety Standard For End Users, Dr. Michel J.M. Houtermans.
c) Reporte Validación SIL, James Halle.
d) Control Systems, Safety Evaluation & Reliability, William Globe, (ISA)
e) Guidelines for Safe and Reliable Instrumented Protective Systems, (CCPS)