Jornadas de Calidad

Análisis de confiabilidad de una batería estandarizada

Por ***Franco Luis Palmieri, Angel Adrián Moreno y Pablo Alonso*** (Repsol YPF)

El objetivo del trabajo es calcular la probabilidad de falla de la operación de una batería estandarizada, a fin de asegurar la salida de producción sin accidentes, sin fallas peligrosas, y respetando la política de medioambiente establecida por la compañía.

Se consideró la operación exitosa de la batería a la capacidad de la misma para cumplir las siguientes funciones: separar, calentar, almacenar, evacuar y medir los fluidos que se procesan en ella.

Una vez obtenida la tasa de falla, se consigue la confiabilidad de la batería de producción estandarizada de un yacimiento de petróleo y gas. La cuantificación del éxito o fracaso se realiza mediante la técnica de árboles de falla.

La tasa de falla obtenida del sistema de seguridad da un valor de aproximadamente 8,8 E 6 fallas/hora, lo cual nos da una confiabilidad del 93% aproximadamente.

Según valores internacionales estamos en el orden 10 E 6, lo que resulta en un sistema operativo continuo - alta demanda - SIL 1.IEC 61508. En las consideraciones realizadas se ha priorizado la seguridad de las operaciones, resignando en cierto grado la operatividad.

Teniendo en cuenta que existe la posibilidad de intervención del operador (falla humana), el nuevo estándar IEC 61511 permite adicionar a los cálculos realizados un FRR (Factor de Reducción de Riesgo) de 0,1, obteniendo un resultado final de 8,8 E 7, que corresponde a un SIL 2.

La tasa de falla del sistema de operación, da un valor de 2 E 4, lo cual resulta en una confiabilidad del 18%, aproximadamente. Una segunda revisión de este sistema, con la implementación de redundancia en los sistemas de medición y control, nos lleva a una tasa de falla de 1,02 E 4, lo que otorga una confiabilidad del 40,97%.

Se han analizado por separado los sistemas de seguridad y de operatividad, teniendo en cuenta que cada uno de ellos debe ser considerado independientemente.

Si bien el valor de confiabilidad de la operación es bajo, tenemos que tener en cuenta que se han incluido absolutamente todos los sistemas de control y medición, que es lo que genera la mayor cantidad de fallas.

Concluyendo podemos decir que la confiabilidad obtenida para la batería estandarizada es altamente satisfactoria, por lo tanto se podrán seguir construyendo sin modificaciones en sus planos actuales.

Introducción

En una batería de producción se junta todo el fluido producido (agua, petróleo y gas) por un grupo de pozos, a fin de realizar una serie de operaciones y mediciones antes de que estos fluidos sean bombeados hacia las plantas de tratamiento. Las operaciones que se realizan en una batería son:

- Separar el gas de los líquidos (agua más petróleo) a fin de captar, medir y enviar el gas separado a la red de consumo (gasoducto).
- Calentar los líquidos (agua más petróleo) separados a fin de facilitar su movimiento dentro de la batería.
- Disponer de capacidad suficiente para cubrir necesidades de almacenaje temporal.
- Medir la producción de líquidos (agua más petróleo) bombeados y determinar el porcentaje de agua total.

Diagrama de flujo típico

El fluido que producen los pozos llega a la batería por una línea de conducción individual para cada pozo, e ingresa a una instalación denominada "colector", el que se compone de un conjunto de válvulas y conexiones cuyo objetivo será el manejo y control del flujo para enviarlo a diferentes lugares dentro de la batería y por diferentes circuitos. A partir del colector, el flujo puede ser dirigido a un separador gas - líquido y de éste a los tanques, o puede previamente pasar por un calentador a fin de ser precalentado a su ingreso a la batería, luego a los separadores, tanques y bombas.

Definiciones y conceptos generales

Se define como "tasa de falla" a la cantidad de fallas que un ítem tendrá durante un cierto tiempo de vida del mismo.

Se define como "confiabilidad" a la habilidad de un sistema para ejecutar las funciones requeridas, bajo determinadas condiciones, durante un periodo de tiempo establecido. Se mide como la probabilidad de que un sistema esté operativo sin falla durante el tiempo de la misión.

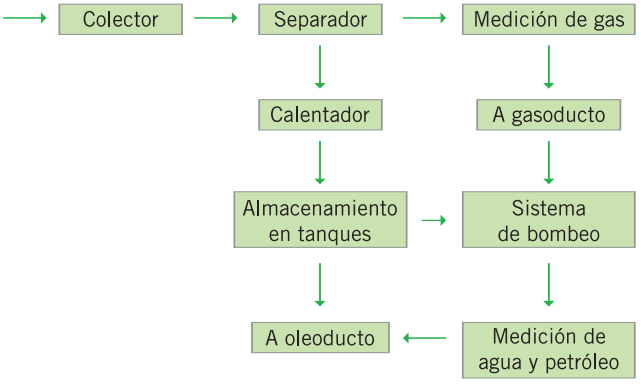
Se define como "disponibilidad" a la habilidad de un sistema para estar disponible y operativo en todo tiempo, ejecutando sus funciones requeridas.

Se define como "falla peligrosa" a la falla a la función asignada, falla no detectable, sólo detectable por inspección. La falla peligrosa impide actuar al sistema de seguridad en caso de ser demandada su acción, o sea, el sistema está indisponible.

La "falla segura" se entiende como aquella falla que provoca la acción segura del sistema.

Los arreglos redundantes determinan la característica en el sentido de dar prioridad a la continuidad del proceso o a la seguridad del mismo.

Se define como "probabilidad de



falla sobre demanda" a la que ocurre encontrándose el sistema de protección indisponible. Ocurre el accidente.

"Eventos iniciantes" son aquellos eventos que pueden afectar la normal operación de un sistema. Existen listados exhaustivos y se agregan aquellos provenientes del buen juicio ingenieril.

Seguridad versus control

Las seguridades toman acción cuando las variables de los equipos y del proceso alcanzan valores fuera del rango de seguridad de los mismos.

Esta situación puede deberse a múltiples motivos, falla de un equipo (rotura de caños, válvulas trabadas), condiciones anormales del proceso (caudal de gas anormal, bajas temperaturas) y falla del propio equipo de control, errores del operador al conducir en manual el proceso, etc.

Una situación a considerar es la puesta en marcha normal o de emergencia de un equipo, ya que las variables críticas pueden moverse a valores fuera del rango de seguridad.

Las normas internacionales indican en forma mandatoria que los sistemas de seguridad deben ser independientes de los sistemas de control de proceso para evitar las causas comunes de falla, pero aún respetando esta práctica, puede ser que cuando el proceso se encuentre inestable alguna seguridad sea puenteada a la espera de la normalización del mismo, lo que constituye una mala práctica que aumenta el riesgo del proceso.

La probabilidad de accidente es igual al producto de la probabilidad del evento peligroso y la probabilidad de indisponibilidad del sistema de seguridad, y esto se cumple solamente si ambos eventos son independientes.

La norma internacional IEC 61508 se ocupa de la confiabilidad de los sistemas relacionados con la seguridad, vinculados a los riesgos del proceso. Y se utiliza únicamente el modo de falla peligroso. Se da satisfacción simultánea a la seguridad y continuidad del proceso. Se debe tener en cuenta que las interrupciones inesperadas del proceso son en sí mismas peligrosas, independientemente de las pérdidas económicas que se producen.

Cumplir con la confiabilidad que la norma exige es condición necesaria pero no suficiente, por cuanto debe verificarse que el sistema de seguridad seleccionado garantice un valor de confiabilidad a la no interrupción del proceso suficientemente razonable.

Técnica del árbol de fallas

El árbol de fallas es un método sistemático para adquirir información de un sistema, que puede ser utilizada para la toma de decisiones y abarca un proceso complejo.

Se ha decidido qué información es la relevante antes de comenzar a realizar el estudio y la recolección de los datos necesarios (tasas de falla, sistemas, etc.).

El límite de cada subsistema y del sistema en general responde básicamente al punto de vista empleado en relación con el área de trabajo.

El límite es definido antes del análisis, no obstante, éste puede ser cambiado sobre la base del análisis realizado.

Un sistema es entonces una entidad determinística que posee una interrelación entre diversos elementos. La definición de sistema, subsistema y sus componentes es relativa y depende del contexto del análisis. Un sistema es una estructura integral compuesta por otras estructuras denominadas subsistemas, a su vez compuesta de bloques básicos llamados componentes. El análisis por el método del árbol de fallas es un proceso deductivo, en el cual se realizan los siguientes pasos:

- Postulación del estado específico "estado de falla".
- Encadenamiento sistemático de las fallas básicas que contribuyen a que se produzca ese evento no deseado.

El árbol de fallas en sí mismo es un modelo gráfico de las diversas combinaciones paralelas y secuenciales de fallas que darán como resultado la ocurrencia del evento no deseado predefinido.

Es un modelo esencialmente cualitativo, aunque puede ser evaluado cuantitativamente.

Un evento indeseable constituye el punto superior en un diagrama de árbol de fallas, el cual provee el método para determinar las causas que hacen llegar a ese punto.

Desarrollo

Una batería de producción debe realizar todas las funciones en forma segura (separar, calentar, almacenar y medir los fluidos que ingresan en ella), sin fallas peligrosas, sin accidentes. Para esto debemos tener en cuenta:

- La seguridad del proceso en todo momento, resignando la operatividad. El estudio de confiabilidad del sistema de seguridad implica el cálculo del *Safety Integrity Level* (SIL) para distintos escenarios de riesgo.
- La operatividad de todo el proceso, incluyendo los dispositivos de medición y control, los cuales en sí mismos no generan fallas peligrosas, sino fallas seguras.

Confiabilidad del sistema de seguridad de una batería estandarizada

Estudio del "*Safety Integrity Level* (SIL) para batería".

Objetivo: análisis del nivel de integridad requerido para el sistema de protección instrumentado de seguridad correspondiente a una batería estandarizada.

Esquema de escenario aplicando estándar IEC 61508 como marco del estándar IEC 61511-3. Verificación de la integridad funcional actual del sistema instrumentado de seguridad y propuesta de mejora en la integridad funcional del sistema si los resultados así lo indican, incluyendo estudio y cálculo del nuevo sistema de seguridad.

Escenario de riesgo n° 1

Generación de una onda de presión de gas, motivada en causas naturales de la fuente de ingreso (pozo), fallas de equipos o sistemas, fallas humanas, fallas operativas y/o de mantenimiento.

El valor de presión de gas supera la presión de calibración de los sistemas

incluidos.

Esta elevación de la presión afectará a los siguientes equipos o sistemas:

- Línea Principal: *piping, fitting* y válvulas.

Consideraciones. Separador gas - líquidos

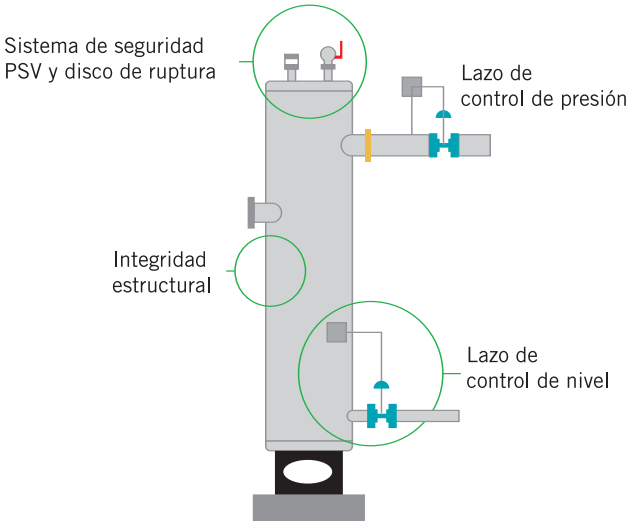
El fluido ingresa al recipiente, el gas se separa saliendo por la parte superior y el líquido sale por la válvula de control mediante la acción de la misma por un flotante y un controlador neumático de nivel. El separador posee instrumentación de control local (manómetro, termómetro y nivel visor). La seguridad del equipo está dada por la presencia de la PSV (*Pressure Safety Valve*) y el DSE (Disco de Ruptura) ubicados en la parte superior y calibrados a la presión de seguridad establecida; además de un sistema instrumentado de seguridad compuesto de una válvula de control de alivio por sobrepresión en el sistema. Para el mantenimiento de los sistemas de seguridad el separador se desvincula del proceso.

Se consideran los siguientes subsistemas:

- *Vessel*.
- Instrumentación.
- Válvula (incluye la válvula, el controlador y el flotante).
- Cañerías y válvulas manuales de entrada y salida.
- PSV (*Pressure Safety Valve*).
- DSE (disco de ruptura).
- Sistema instrumentado de seguridad de alivio por alta presión.

La falla peligrosa en este sistema ocurre cuando la PSV queda bloqueada por alguna causa del tipo de fluido (hidratos por ej.) y ante una demanda no actúa ésta ni el disco de ruptura. Tenemos entonces un sistema 2 fuera de 3 cuando se opera en forma normal, lo cual implica:

- actúa primero la válvula de alivio de sobrepresión;
- si continúa el aumento de presión actúa la válvula de seguridad;
- si sigue aumentando se rompe el disco de ruptura y el sistema queda inoperante (el separador deja de separar los fluidos).



Metodología a aplicar

Método cualitativo *risk graph*

- Consecuencia del evento indeseable.
- Frecuencia y exposición en zona peligrosa.
- Posibilidad de evitar el evento peligroso.
- Probabilidad de la ocurrencia del evento no deseado.

Componentes de riesgo del sistema en estudio

C2: heridas serias permanentes a una o más personas, muerte de una persona.

F1: rara frecuencia de exposición en zona de peligro.

P1: posibilidad de evitar el evento peligroso bajo ciertas condiciones.

W2: baja probabilidad de ocurrencia del evento indeseable.

El resultado obtenido es: SIL 1.

Método cualitativo *severity matrix*

- Número de sistemas independientes relacionados a la seguridad.
- Número de facilidades externas, para reducción de riesgo.
- Severidad del evento indeseable.
- Probabilidad del evento indeseable.

Componentes de riesgo del sistema en estudio

Número de sistemas independientes relacionados con la seguridad: UNO (instrumentado).

Número de facilidades externas: DOS (válvula de seguridad y disco de ruptura).

Severidad del evento indeseable: serio.

Probabilidad del evento: media.

El resultado obtenido es: probablemente no se requiere de un sistema relacionado con la seguridad. Se decide que sea mínimamente un SIL 1.

Método cuantitativo

- Técnica de árbol de fallas.
- Frecuencia tolerable para el acontecimiento del evento indeseable.
- Frecuencia NO protegida (demanda sobre el sistema de seguridad instrumentado).

Lista de eventos iniciantes

- Falla mecánica del disco de ruptura.
- Falla al abrir la válvula de seguridad ante un aumento de presión.
- La válvula de control del sistema de alivio de presión falla al abrir.

La tasa de falla obtenida del sistema de seguridad da un valor de 2,79 E 6 fallas/hora.

Según valores internacionales estamos en el orden 10 E 6, lo que resulta en un sistema operativo continuo - alta demanda - SIL 1.IEC 61508. Teniendo en cuenta que existe la posibilidad de intervención del operador (falla humana), el estándar IEC 61511 permite adicionar a los cálculos realizados un FRR (Factor de Reducción de Riesgo) de 0,1, obteniendo un resultado final de 2,79 E 7, que corresponde a un SIL 2.

PFD: Ft / Fnp.

PFD: probabilidad de falla sobre demanda.

Ft: frecuencia aceptable del accidente.

Fnp: frecuencia del accidente sin protección (demanda).

PFD: tasa de falla peligrosa x tiempo entre inspecciones.

Ft = PFD x Fnp.

Ft = tasa de falla sobre demanda x tiempo entre inspecciones x demanda.

Ft = valor resultante del SIL x periodo entre test x demanda.

Ft = (fallas/año) x (años/test) x (demanda/año).

Ft = 2,79 E 7 x 0,5 años /test x 1.

Ft = 1,395 E 7 accidentes/año.

Antecedentes

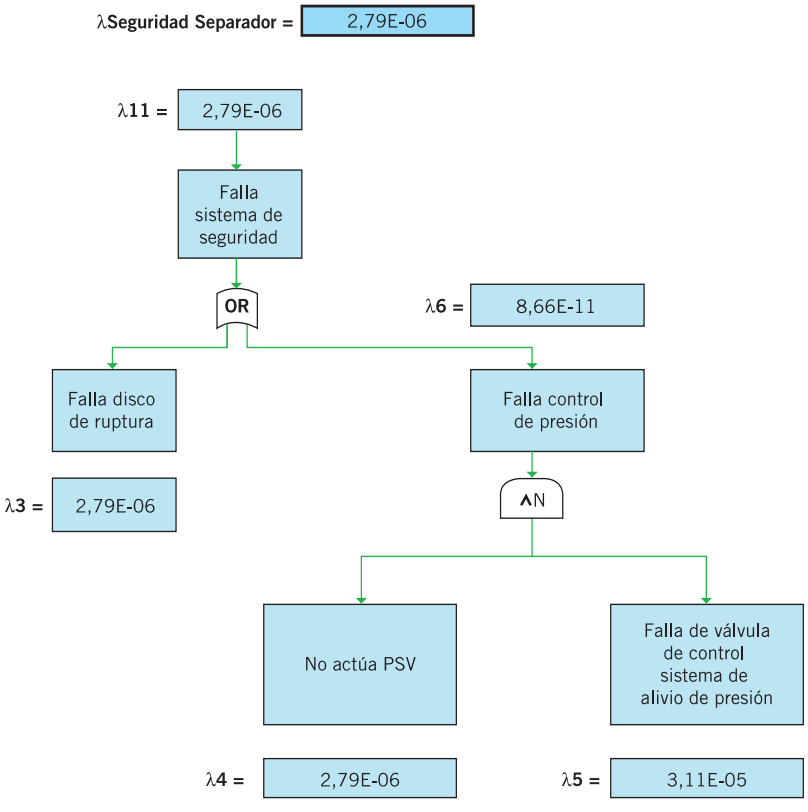
- Especificaciones de la compañía. Procedimientos aplicados.
- Diagramas P&ID.
- Diagrama de causa - efecto.
- *Piping classes* según diseño de presión en el *vessel*.
- Reportes históricos de incidentes y accidentes en la instalación.
- Instrumentación, control y monitoreo remoto. Datos de cada componente.

Base de datos

- Tasa de fallas según "OREDA Data Bank".

Se utilizará tasa de falla correspon-

Sistema de seguridad en separador gas-líquido



diente a tiempo calendario.

Se utilizará valor medio de la tasa de falla.

- Documentación de proveedores de instrumentos instalados.
- Valores universales considerados para el cálculo.
- Experiencia en instalaciones.
- Base de datos propia de sistema SAP.

Escenario de riesgo n° 2

Generación de una onda de presión de gas, con aumento de presión y temperatura en el *vessel* y seguida de fuego en equipos y/o sistemas. El valor de presión de gas supera la presión de regulación de los sistemas incluidos. Esta elevación de la presión afectará a los siguientes equipos o sistemas: línea principal: *vessel*, *piping*, *fitting* y válvulas.

Consideraciones. Calentador indirecto de petróleo

El calentador es de tipo indirecto. El tubo de fuego calienta agua y el vapor generado en la cámara a su vez calienta el serpentín por donde circula el fluido (petróleo).

Se consideran los siguientes subsistemas:

- *Vessel* (incluye recipiente, quemador, piloto, y serpentín).
- Instrumentación (manómetros, termómetros).
- Válvula (incluye la válvula propiamente dicha, el controlador de nivel de agua, el control por temperatura de salida y por presión de cámara). La acción del control es apagar el quemador ante bajo nivel de agua, alta temperatura de salida y alta presión de cámara.
- Cañerías y válvulas manuales de entrada y salida.
- PSV y termocupla o sensor UV para detectar falla de llama.

La falla peligrosa en este sistema ocurre cuando el sistema de control deja de asegurar el control de las variables (presión de cámara, temperatura de salida y nivel de agua) y el sistema de seguridad no actúa ante una demanda de alguna de las variables anteriores, lo cual ocurre cuando se bloquea la PSV o falla el sensor de llama. Tenemos entonces un sistema 2 fuera de 2, lo cual entrega una aceptable seguridad, con una buena operatividad.

Metodología a aplicar

Método cualitativo *risk graph*

- Consecuencia del evento indeseable.
- Frecuencia y exposición en zona peligrosa.
- Posibilidad de evitar el evento peligroso.
- Probabilidad de la ocurrencia del evento no deseado.

Componentes de riesgo del sistema en estudio

C2: heridas serias permanentes a una o más personas, muerte de una persona.

F1: rara frecuencia de exposición en zona de peligro.

P1: imposibilidad de evitar el evento

peligroso bajo ciertas condiciones.
W2: baja probabilidad de ocurrencia del evento indeseable.
El resultado obtenido es: SIL 1.

Método cualitativo *severity matrix*

- Número de sistemas independientes relacionados a la seguridad.
- Número de facilidades externas, para reducción de riesgo.
- Severidad del evento indeseable.
- Probabilidad del evento indeseable.

Componentes de riesgo del sistema en estudio

Número de sistemas independientes relacionados con la seguridad: UNO (instrumentado).

Número de facilidades externas: DOS (válvula de seguridad y seguro de llama).

Severidad del evento indeseable: serio.

Probabilidad del evento: media.

El resultado obtenido es: SIL 1.

Método cuantitativo

- Técnica de árbol de fallas.
- Frecuencia tolerable para el acontecimiento del evento indeseable.
- Frecuencia NO protegida (demanda sobre el sistema de seguridad instrumentado).

Lista de eventos iniciantes

- Falla sensor de seguro de llama.
- Falla al abrir la válvula de seguridad ante un aumento de presión.

Según valores internacionales estamos en el orden 10 E 6 lo que resulta en un sistema operativo continuo - alta demanda - SIL 1.IEC 61508. Teniendo en cuenta que existe la posibilidad de intervención del operador (falla humana), el estándar IEC 61511 permite adicionar a los cálculos realizados un FRR (Factor de Reducción de Riesgo) de 0,1, obteniendo un resultado final de 3,19 E 7, que corresponde a un SIL 2.

PFD: Ft / Fnp.

PFD: probabilidad de falla sobre demanda.

Ft: frecuencia aceptable del accidente.

Fnp: frecuencia del accidente sin protección (demanda).

PFD: tasa de falla peligrosa x tiempo entre inspecciones.

Ft = PFD x Fnp.

Ft = tasa de falla sobre demanda x tiempo entre inspecciones x demanda.

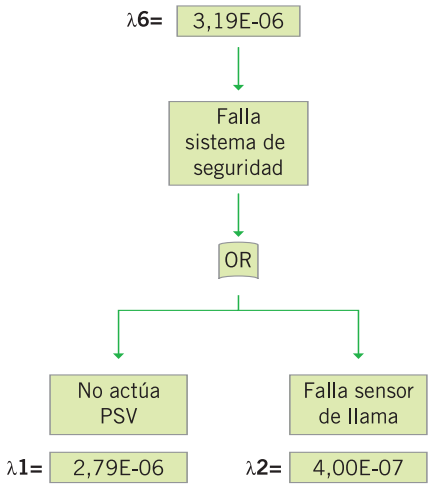
Ft = valor resultante del SIL x periodo entre test x demanda.

Ft = (fallas/año) x (años/test) x (demanda/año).

Ft = 3,19 E 7 x 0,5 años/test x 1.

Ft = 1,595 E 7 accidentes/año.

Sistema de seguridad de un calentador de petróleo



La tasa de falla obtenida del sistema de seguridad da un valor de 3,19 E-6 fallas/hora.

Antecedentes

- Especificaciones de la compañía. Procedimientos aplicados.
- Diagramas P&ID.
- Diagrama de causa - efecto.
- *Piping classes* según diseño de presión en el *vessel*.
- Reportes históricos de incidentes y accidentes en la instalación.
- Instrumentación, control y monitoreo remoto. Datos de cada componente.

Base de datos

- Tasa de fallas según "OREDA Data Bank".

Se utilizará tasa de falla correspondiente a tiempo calendario.

Se utilizará valor medio de la tasa de falla.

- Documentación de proveedores de instrumentos instalados.
- Valores universales considerados para el cálculo.
- Experiencia en instalaciones.
- Base de datos propia de sistema SAP.

Escenario de riesgo n° 3

Generación de un aumento o disminución de presión interna en el *vessel*.

Esto afectará a los siguientes equipos o sistemas:

- Línea principal: *vessel*.

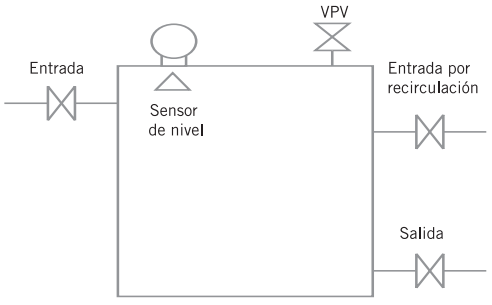
Se consideran los siguientes subsistemas:

- *Vessel*.
- Evacuación del fluido (Salida).
- Válvula de presión y vacío (VPV).
- Cañerías y válvulas manuales de entrada y salida.

La falla peligrosa en este sistema ocurre cuando el tanque colapsa o cuando falla la válvula de presión y vacío ante una demanda de presión en el recipiente.

Tenemos un sistema 1 de 2.

Consideraciones: tanque de almacenamiento de petróleo



Metodología a aplicar

Método cualitativo *risk graph*

- Consecuencia del evento indeseable.
- Frecuencia y exposición en zona peligrosa.
- Posibilidad de evitar el evento peligroso.
- Probabilidad de la ocurrencia del evento no deseado.

Componentes de riesgo del sistema en estudio

C2: heridas menores.
F1: rara frecuencia de exposición en zona de peligro.
P2: posibilidad de evitar el evento peligroso bajo ciertas condiciones.
W1: muy baja probabilidad de ocurrencia del evento indeseable.
Resultado: no hay requerimientos especiales.

Método cualitativo *severity matrix*

- Número de sistemas independientes relacionados a la seguridad.
- Número de facilidades externas, para reducción de riesgo.
- Severidad del evento indeseable.
- Probabilidad del evento indeseable.

Componentes de riesgo del sistema en estudio

Número de sistemas independientes relacionados con la seguridad: UNO (instrumentado).

Número de facilidades externas: UNA (muro de contención).

Severidad del evento indeseable: serio.

Probabilidad del evento: media.

Resultado obtenido: SIL 1.

Método cuantitativo

- Técnica de árbol de fallas.
- Frecuencia tolerable para el acontecimiento del evento indeseable.
- Frecuencia NO protegida (demanda sobre el sistema de seguridad instrumentado).

Lista de eventos iniciantes

- La válvula de presión y vacío no actúa ante una demanda.

La tasa de falla obtenida del sistema de seguridad da un valor de 2,81 E 6 fallas/hora.

Según valores internacionales estamos en el orden 10 E 6 lo que resulta en un sistema operativo continuo - alta demanda - SIL 1.IEC 61508. Teniendo en cuenta que existe la posibilidad de intervención del operador (falla humana), el estándar IEC 61511 permite adicionar a los cálculos realizados un FRR (Factor de Reducción de Riesgo) de 0,1, obteniendo un resultado final de 2,81 E 7, que corresponde a un SIL 2.

PFD: Ft / Fnp.
PFD: probabilidad de falla sobre demanda.
Ft: frecuencia aceptable del accidente.
Fnp: frecuencia del accidente sin protección.
PFD: tasa de falla peligrosa x tiempo entre inspecciones.
Ft = tasa de falla sobre demanda x tiempo entre inspecciones x demanda.
Ft = valor resultante del SIL x periodo entre test x demanda.
Ft = (fallas/año) x (años/test) x (demanda/año).
Ft = 2,81 E 7 x 1 años/test x 0,1.
Ft = 2,81 E 8 accidentes/año.

Antecedentes

- Especificaciones de la compañía. Procedimientos aplicados.
- Diagramas P&ID.
- Diagrama de causa - efecto.
- Diseño de presión en el *vessel*.
- Reportes históricos de incidentes y accidentes en la instalación.
- Instrumentación, control y monitoreo remoto. Datos de cada componente.

Base de datos

- Tasa de fallas según "OREDA Data Bank".

Se utilizará tasa de falla correspondiente a tiempo calendario.

Se utilizará valor medio de la tasa de falla.

- Documentación de proveedores de instrumentos instalados.
- Valores universales considerados para el cálculo.
- Experiencia en instalaciones.
- Base de datos propia de sistema SAP.

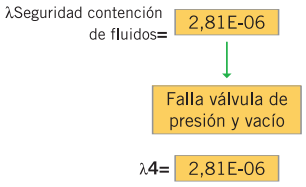
Arbol de fallas. Sistema de seguridad

La tasa de falla obtenida del sistema de seguridad da un valor de aproximadamente 8,8 E 6 fallas/hora, lo cual nos da una confiabilidad del 93% aproximadamente.

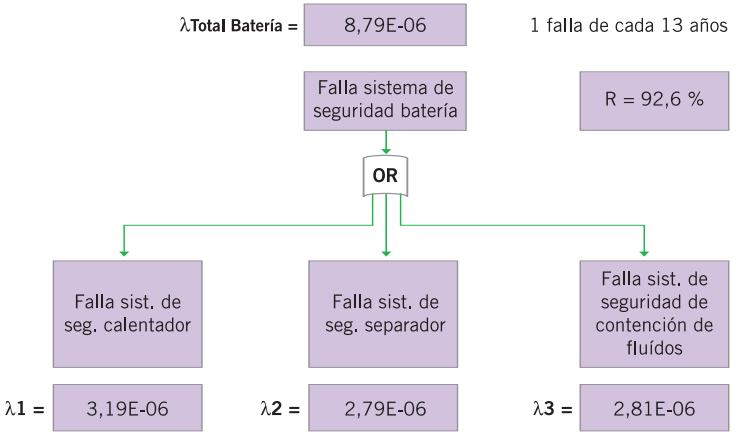
Según las tablas de valores internacionales estamos en el orden 10 E 6, lo que nos da un sistema operativo continuo - alta demanda - SIL 1.IEC 61508. Es necesario considerar aquí que hemos priorizado la seguridad de las operaciones, resignando la operatividad.

Teniendo en cuenta que existe la posibilidad de intervención del operador (falla humana), el nuevo estándar IEC 61511 permite adicionar a los cálculos realizados un FRR (Factor de Reducción de Riesgo) de 0,1, llevando el resultado final a 8,8 E 7, es decir, SIL 2.

Sistema de seguridad de tanques de almacenamiento



Tasa de falla seguridad de batería



Confiabilidad en la operatividad de una batería estandarizada

Se consideró la operación exitosa de la batería a la capacidad de la misma de cumplir todas las funciones de separación, calentamiento, almacenamiento, medición y evacuación de los fluidos ingresados.

Lista de eventos iniciantes

Calentador de líquidos

- Rotura del serpentín.
- Rotura del recipiente.
- Rotura de las cañerías de entrada o salida de fluido.
- No existe alimentación de gas combustible.
- El sensor de temperatura de salida no emite señal.
- El sensor de control de nivel no emite señal.
- Falla al abrir la válvula de control integral SARCO.

Separador de gas - líquidos

- Rotura del recipiente.
- Rotura de las cañerías de entrada o salida de fluido.
- El sensor de control de nivel no emite señal.
- Los instrumentos de monitoreo local no funcionan.
- El operador realiza una maniobra equivocada ante la falla en el instrumental.

Contención de fluidos

- Colapso del recipiente.
- Rotura de las cañerías de entrada o salida de fluido.
- Bloqueo de la pierna de rebalse.
- El sistema de evacuación de fluidos no funciona.

Evacuación de fluidos

- El motor eléctrico no arranca.
- El equipo de arranque no funciona.
- Falta de energía relacionada con el sistema exterior de distribución de la misma.
- Falta de energía relacionada con el sistema exterior de generación de la misma.
- Rotura de los rodamientos.
- Rotura del acople.
- Rotura de cuerpo mecánico de la bomba.
- Rotura de cuerpo hidráulico de la bomba.
- Falla eléctrica en bomba de reserva.
- Falla mecánica en bomba de reserva.
- La válvula de recirculación de fluidos al recipiente del sistema de control falla al cerrar.
- El sensor de nivel del recipiente de contención no emite señal.
- El sistema de control automático no actúa ante falla del sensor de nivel.
- El operador del sistema de control SCADA realiza una acción incorrecta ante la falla del sensor de nivel y del control automático local con PLC.

Sistema de medición de fluidos

- Rotura de cañerías de entrada y salida al sensor de medición de caudal.
- El filtro antes del sensor está bloqueado.
- El sistema de control de medición de caudal se resetea innecesariamente.
- Rotura del sensor de medición de caudal.
- Falla de la electrónica del computador de flujo neto de fluido medido.
- No hay suministro de energía de red en el sistema de medición.
- El sistema de energía alternativa no funciona.

Sistema de medición de gas de salida

- Rotura de cañerías de entrada y salida al sensor de medición de caudal.
- Falla de la electrónica o programa del computador de flujo de gas medido.
- El sensor de medición de presión diferencial no emite señal.
- El sensor de medición de presión estática no emite señal.
- La válvula del sistema de control de aporte a gasoducto falla al abrir.
- No hay suministro de energía de red en el sistema de medición.
- El sistema de energía alternativa no funciona.

Arbol de fallas. Operatividad batería

(ver figura de página 31)

Conclusiones

La tasa de falla obtenida del sistema de seguridad da un valor de 1,02 E 4 fallas/hora, lo cual nos da una confiabilidad del 41% aproximadamente.

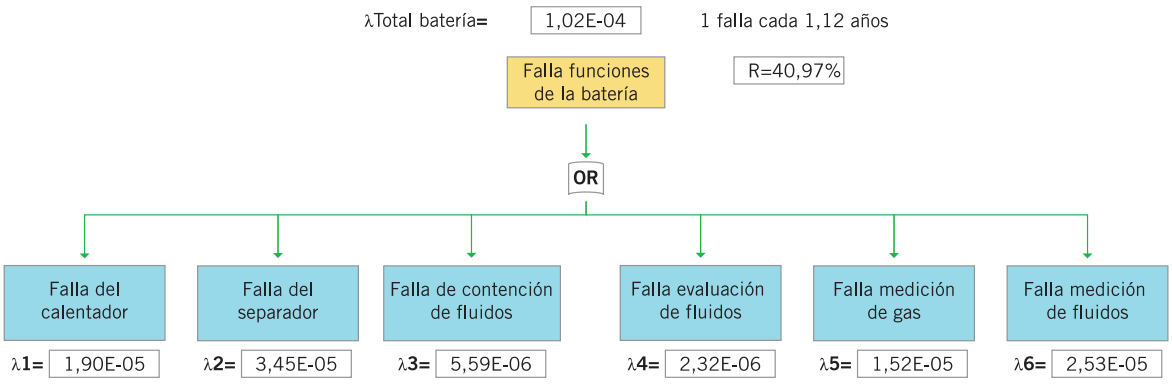
El valor de confiabilidad de la operación obtenido es relativamente bajo, se han tenido en cuenta dentro de este sistema todos los sistemas de control y medición, siendo éstos últimos los que generan la mayor cantidad de fallas.

Acciones a corto plazo

- Comparar el valor de confiabilidad con los datos obtenidos desde el sistema de gestión.

Implementar la gestión sobre los activos faltantes.

Tasa de falla total de la batería estándar operaciones



- Trabajar en nuevos diseños o arreglos de redundancia que permitan aumentar la confiabilidad en los subsistemas o componentes con tasa de falla alta.
- Ajustar los periodos entre test y los procedimientos de mantenimiento a fin de alcanzar el nivel de confiabilidad establecido.

Acciones a mediano plazo

- Intervención temprana de Ingeniería de Mantenimiento en los diseños del sector de Ingeniería de Proyectos introduciendo diseño con base riesgo incorporando la técnica del árbol de falla y normas internacionales IEC 61508 y IEC 61511-3, a los efectos de determinar la confiabilidad, seguridad y operatividad del proyecto.
- Definir procedimientos de tareas de *commission* y *precommission* de instalaciones, equipos e instrumental de medición y sistemas de seguridad, asegurando la mantenibilidad.

Acciones a largo plazo

- Calcular el costo de llegar a un valor de confiabilidad mayor.

Bibliografía

- *Manual de árbol de falla (Fault tree handbook - U.S. Nuclear Regulatory Commission).*
- *Manual de producción,* Repsol YPF.
- "OREDA Data Bank", catálogo *Offshore Reliability Data,* 4ª edición, 2002.
- *Procedimientos de mantenimiento,* Repsol YPF.
- Otros bancos de datos de origen internacional y datos propios extraídos del sistema de gestión.