UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE QUIMICA

DIVISION DE ESTUDIOS DE POSGRADO

"DESARROLLO DE UNA METODOLOGIA DE ANALISIS CUANTITATIVO SIMPLIFICADO, BASADA EN EL ANALISIS DE CAPAS DE PROTECCION (LOPA), PARA LA DETERMINACION DEL NIVEL DE INTEGRIDAD DE LA SEGURIDAD (SIL), EN LOS SISTEMAS INSTRUMENTADOS DE SEGURIDAD (SIS), EN UNA PLANTA REFORMADORA DE NAFTA PESADA".

T E S I S

PARA OBTENER EL GRADO DE

MAESTRO EN INGENIERIA QUIMICA
(PROCESOS)

P R E S E N T A :

JULIO CESAR RODRIGUEZ JIMENEZ

MÉXICO, D.F.

2004

JURADO ASIGNADO

Presidente.	Dr.	Carlos Escobar Toledo
Vocal.	Dr.	Ricardo Aceves García
Secretario.	Dr.	Julio Ricardo Landgrave Romero
1er. Suplente.	Dr.	Alfonso Durán Moreno
2o. Suplente.	Dr.	Reynaldo Sandoval Gonzáles

SITIO DONDE SE REALIZÓ EL TEMA:

Laboratorio E-212, Conjunto E, Facultad de Química, UNAM.

Refinería "Gral. Lázaro Cárdenas", Minatitlán, Veracruz.

Asesor: Dr. Modesto Javier Cruz Gómez.

AGRADECIMIENTOS

A la Universidad Nacional Autónoma de México, por darme la oportunidad de aprender de lo mejor de la ciencia y la cultura de este país.

A el convenio UNAM-INSTITUTO MEXICANO DEL PETROLEO-PETROLEOS MEXICANOS por haberme dado la oportunidad de estudiar la maestría en ingeniería química.

Al consejo nacional de ciencia y tecnología (CONACYT) por su apoyo económico que me permitió terminar mis estudio de maestría.

A los profesores de la maestría por sus valiosas enseñanzas que me permitió tener una visión mas profunda de la ingeniería química.

A los sinodales de esta tesis: Dr. Carlos Escobar Toledo, Dr. Ricardo Aceves García, Dr. Julio Ricardo Landgrave Romero, Dr. Alfonso Durán Moreno, Dr. Reynaldo Sandoval Gonzáles por sus comentarios y críticas que ayudaron a enriquecer este trabajo.

A la M. en C. Rosa Maria Corona Flores por sus valiosos comentarios y correcciones sobre la redacción de la tesis.

Al Dr. Modesto Javier Cruz Gómez e Ing. Héctor Cruz Campa por proporcionarme los recursos y hacerme participe de este proyecto.

A las Ingenieras Químicas Fanny llamas y Esmeralda Ramírez por su apoyo y colaboración.

A la Refinería "General Lázaro Cárdenas" por haberme brindado la oportunidad de aplicar este proyecto en sus instalaciones.

A el grupo de análisis de riesgos de la facultad de química, residentes en la refinería "General Lázaro Cárdenas".

A la ingeniera en computación Susana Ortiz y Mary. Carmen Cruz por su ayuda en el servicio de cómputo.

DEDICATORIAS

A mis padres:

Ángel Rodríguez Rivas y Angelina Jiménez Coronado por heredarme sus grandes valores de honestidad, rectitud y congruencia. Por su incondicional apoyo en mi educación. Siempre tendrán un lugar especial en mi vida, los quiero mucho.

A mis hermanos y hermanas:

Yolanda, Marco Antonio, José Ángel, Ramón Octavio, Martha Estela, Jesús Remberto, Luis Armando, Alma Leticia, Maria Angélica, Joel, Jaime Enrique y Elsa Cristina. A todos ellos con todos mis respetos.

A Rosa Maria:

Mi amiga, pareja, confidente con la cual comparto sueños, ilusiones, sentimientos, gracias por todo tu apoyo.

RESUMEN

En este trabajo se presenta el desarrollo de una metodología cuantitativa simplificada, basada en la norma ANSI / ISA S84.01 y en el análisis de capas de protección (LOPA), cuyo propósito es evaluar la efectividad de las capas de protección independiente que son sistemas o acciones capaces de prevenir un escenario de consecuencias indeseables, independiente del evento inicial o de la acción de cualquier otra capa de protección asociado con el escenario y determinar si dichas capas son suficiente para llevar el riesgo a niveles aceptables en escenarios de alto riesgo potencial en una planta Reformadora de Naftas de la refinería "Lázaro Cárdenas" en Minatitlán Ver.

El método permite determinar el Nivel de Integridad de la seguridad (SIL) de un Sistema Instrumentado de Seguridad (SIS) en caso de que esta sea una opción conveniente o verificar el SIL requerido para un SIS ya instalado.

La metodología fue aplicada en escenarios que tienen clasificación de riesgo Inaceptable y riesgo indeseable, en interruptores automáticos (INTERLOCKS) de los calentadores a fuego directo, fuga de hidrógeno en los compresores y en los Sistemas Instrumentados de Seguridad propuestos en la instalación de Válvulas de Aislamiento de Activación Remota (VAAR) en la descarga de recipientes que manejan sustancias peligrosas.

El análisis de los resultados demuestra que en algunos de los escenarios hay una sobre estimación del riesgo potencial ya que en muchos de los casos el riesgo se mitiga al mejorar los programas de mantenimiento, condiciones de operación, instrumentación básica y el equipo de proceso.

En otros escenarios se observó que las capas de protección no son suficientes para mitigar el riesgo potencial por lo que se propusieron capas de protección adicionales o un Sistema Instrumentado de Seguridad.

Esta metodología ayudará a tomar una mejor decisión en la instalación de capas de protección o SIS y por lo tanto contribuir al abatimiento en la frecuencia de fallas e incidentes en una planta Reformadora de Naftas.

Además el método puede ser empleado en otras plantas de procesos si se determinan los criterios específicos para esa industria en cuestión.

CONTENIDO

ÍNDICE DE TABLAS.

ÍNDICE DE FIGURAS.

Lista de abreviaturas

API	Instituto Americano del Petróleo, (American Petroleum Institute).
AIChE	Instituto Americano de Ingenieros Químicos, (American Institute of Chemical Engineers).
BPCS	Sistemas del Control Básico del proceso, (Basic Process Control System).
CCPS	Centro para la Seguridad de los Procesos Quimicos, (Center For Chemical Process Safety).
EPA	Agencia de Protección Ambiental, (Environmental Protection Association).
ETA	Análisis de árbol de eventos, (Event Tree Analysis).
ESD	Paro de emergencia, (Emergency shut down)
FTA.	Análisis de árbol de fallas, (Fault Tree Analysis).
HAZOP	Análisis de riesgos y operabilidad, (Hazard and Operability).
IEC	Comisión Electrotécnica Internacional, (Internacional electrotechnical Comisión).
IPL	Capas de protección independiente, (Independent Protection Layer).
ISA	Sociedad Instrumentista de América, (Instrument Society of America).
LOPA	Análisis de capas de protección, (Layer of Protection Analysis).
LHSV	Espacio velocidad, relación volumétrica de la carga al reactor por hora entre volumen de catalizador en todos los reactores.
MTBF	Tiempo medio entre fallas, (Mean time between failures.)
MTTF	Tiempo medio de paro en falso, (mean time to failures.)
NFPA	Asociación Nacional de Protección contra Incendio, (National Fire Protection Association).
OSHA	Agencia de Seguridad y Salud Ocupacional, (Ocupational Safety and Health Administration).
P&ID	Diagrama de tubería y instrumentación, (Piping and Instrumentation Diagram).
PSM	Administración de Seguridad del Proceso, (Process Safety Management).
PLC	Control lógico programable, (Programming Logic Control).
PFD	Probabilidad de falla en demanda, (Probability of Failure on Demand).
PHA	Análisis de riesgos de procesos, (Process Hazard Analysis).

RMP	Programa de administración de riesgos, (Risk Management Program).
RNP	Reformadora de nafta pesada.
SIF	Función instrumentada de seguridad, (Safety Instrumented Function).
SIL	Nivel integral de la seguridad, (Safety Integrity Level).
SIS	Sistema instrumentado de seguridad, (Safety instrumented system)
VAAR	Válvula de aislamiento de activación remota.
S_{pfd}	Ordenes de magnitud de la probabilidad de falla en demanda
S_{add}	Valor de la efectividad requerida para determinar la estrategia de control de riesgos a implantar.
WHSV	Espacio velocidad, relación de peso de la carga al reactor por hora entre peso de catalizador en todos los reactores.

HIPÓTESIS

Mediante el desarrollo y la aplicación de una metodología de análisis cuantitativo simplificado, se puede minimizar el nivel de riesgo y las fallas generados en un escenario de alto riesgo potencial, sin sobre diseñar los sistemas de protección en una planta Reformadora de Naftas.

OBJETIVOS

Desarrollar una metodología de análisis cuantitativo simplificado, basado en el análisis de las capas de protección (LOPA) en una planta reformadora de naftas, que tenga el propósito de:

- Identificar y evaluar la efectividad de las capas de protección en un escenario de alto riesgo potencial obtenido por la técnica de análisis de riesgo y operabilidad (HAZOP) y que determine si las capas son suficientes para disminuir el riesgo hasta niveles aceptables.
- Justificar la necesidad de un sistema instrumentado de seguridad (SIS) en caso de que las capas de protecciones no sean suficientes para reducir un riesgo.
- Evaluar el nivel de integridad de la seguridad (SIL) de un sistema instrumentado de seguridad (SIL) propuesto o verificar el SIL requerido para un SIS ya instalado.

Además, se deben proponer los criterios de aceptabilidad de riesgos de acuerdo a los requerimientos de la organización.

Para alcanzar los objetivos propuestos se propone la siguiente secuencia de trabajo:

Capitulo 1 justificación del trabajo. Capitulo 2 se explica de manera resumida las técnicas de análisis de riesgos, del metodo (LOPA) y se da una explicación de las características de los sistemas instrumentados de seguridad incluyendo el nivel integral de la seguridad. Capitulo 3 resumen de la descripción del Proceso de reformado de Naftas. Capitulo 4 descripción y desarrollo de cada una de las etapas de la metodología cuantitativa simplificada. Capitulo 5 aplicaciones de la metodología con sus resultados. Capitulo 6 discusión y recomendaciones del trabajo. Capitulo 7 conclusiones.

ALCANCE

El método se aplicó en una planta reformadora de Naftas en operación continua de la refinería "Lázaro Cárdenas" de Minatitlán Ver.

CAPÍTULO 1.

INTRODUCCIÓN

CAPÍTULO 1

INTRODUCCIÓN

1.1 JUSTIFICACIÓN

El proyecto desarrollado en la presente tesis surge como una propuesta del área técnica de la refinería "Lázaro Cárdenas" de Minátitlán Ver. Debido a la necesidad de tener una herramienta que pueda evaluar los niveles de confiabilidad de los sistemas instrumentados de seguridad de la planta reformadora de nafta pesada, de una manera simple y efectiva, además de que esta nueva herramienta tenga la capacidad y los elementos necesarios para poder decidir si sus plantas requieren de sistemas instrumentados de seguridad adicionales u otro tipo de protecciones. Para el desarrollo de la metodología cuantitativa simplificada de este trabajo se utilizó una nueva técnica de análisis de riesgos que se basa en el análisis de las capas de protección (LOPA) y que cumple con los requerimientos de los objetivos propuestos de esta tesis.

Esta metodología se considera simplificada ya que para identificar los escenarios de alto riesgo potencial se basa en el metodo de análisis de riesgo y operabilidad (HAZOP) que es una técnica cualitativa. Sin embargo, se ha constatado que sus resultados, dado el enfoque cuantitativo del resto de la metodología; son bastante confiables, e incluso aceptados informalmente por compañías de seguros.

De la aplicación de la metodología cuantitativa simplificada se obtuvieron una serie de recomendaciones en donde se proponen nuevas capas de protección, o la modificación de las existentes en los escenarios de alto riesgo potencial. Así como la evaluación del SIL de los interruptores automáticos (interlocks) ubicados en calentadores a fuego directo e instalación de válvulas de activación remota (VAAR).

Los resultados del trabajo permiten decidir en que puntos es estrictamente necesario instalar un SIS, así como reducir la incidencia de accidentes ya que el personal de operación no estará sometido a exposiciones potenciales en escenarios de alto riesgo.

CAPÍTULO 2.

MARCO TEÓRICO

CAPÍTULO 2

MARCO TEÓRICO

2.1 ANTECEDENTES [2] [21] [20]

Los incendios, las explosiones y la liberación de gases tóxicos pueden causar la muerte o lesiones a trabajadores y otros ciudadanos, provocar la evacuación de comunidades enteras y afectar desfavorablemente al medio ambiente en general. Desastres que se conocen con nombres propios como "Basilea", "Bhopal", "Flixborough", "México" y "Seveso" han dado origen a las expresiones "riesgos mayores " y "control de riesgos de accidentes mayores"; en Bulgaria en noviembre de 1986, una explosión de cloruro de vinilo provocó la muerte de 17 personas y 19 heridos. En Bhopal, India, en 1984, una emisión de la sustancia química isocianato de metilo provocó más de 4000 muertos y más de 400,000 afectados. Dos semanas antes se había producido una explosión de gas natural en México, DF, que ocasionó la muerte de 650 personas y varios miles de heridos. En 1976, en Seveso, Italia, 30 personas resultaron heridas y 220,000 tuvieron que ser evacuadas debido al escape de la sustancia química dioxina. En Flixborough, Reino Unido, en 1974 una explosión de ciclohexano causo la muerte de 28 personas e hirió a 89. Las pérdidas económicas resultantes de cada uno de estos accidentes son mayores a 10^8 USD.

Existen varias industrias de proceso que por su naturaleza manejan grandes inventarios de sustancias inflamables, explosivas o tóxicas, o bien presentan condiciones de operación extremas (temperatura y presiones muy altas o muy bajas). Estas industrias se consideran peligrosas ya que potencialmente pueden ocurrir incendios, explosiones o dispersión de sustancias químicas tóxicas capaces de causar daños a los trabajadores, a la comunidad, al medio ambiente y a las mismas instalaciones.

La prevención y la lucha contra los riesgos mayores han pasado a ser una cuestión importante en todas las partes del mundo. Las posibilidades potenciales de que se produzca un accidente importante debido al aumento de la producción, almacenamiento y empleo de sustancias peligrosas implican la necesidad de un enfoque bien determinado y sistemático, si se quiere evitar grandes catástrofes. Por eso surge la necesidad de desarrollar nuevas tecnologías en el

ámbito de la seguridad que ayuden a eliminar y reducir los riesgos que se presentan en los procesos industriales.

2.2 ANÁLISIS DE RIESGOS DE PROCESO [22] [23]

Para poder decidir si un riesgo es o no aceptable, se requiere estimar de alguna forma su magnitud, lo que implica un análisis previo. Análisis de riesgo significa desarrollar una estimación cuantitativa del nivel de peligro potencial de una actividad y estimar el riesgo referido tanto a personas, propiedad y/o el medio ambiente. En términos de la magnitud del daño y la probabilidad de que tenga lugar. El análisis de riesgos es una disciplina que combina la evaluación de ingeniería del proceso con técnicas matemáticas que permiten realizar estimaciones de frecuencias y consecuencias de accidentes. Los resultados del análisis de riesgos se utilizan para la toma de decisiones, ya sea mediante la jerarquización de las estrategias de reducción o mitigación de riesgos o mediante la comparación con los niveles de riesgo fijados como objetivo en una determinada actividad.

El análisis de riesgos permite, dentro de los niveles de incertidumbre asociada a cada tipo de análisis empleado y a los datos disponibles, cuantificar el potencial de accidentes existentes en una determinada instalación o proceso y si éste se considera demasiado elevado, se deben proponer alternativas de solución para disminuirlo. Como es lógico cada una de ellas implicará un costo económico diferente, que también debe ser tomado en cuenta en la decisión final.

Las fuentes de datos principales utilizados en un análisis de riesgos para su ejecución son las siguientes:

- Propiedad del material (hoja de datos de seguridad de materiales) e información de toxicidad (toxicología e higiene industrial).
- Documentación y diagramas de flujo de proceso químico, incluyendo inventarios importantes y datos de flujo.
- Diagramas de tubería e instrumentación (P&ID).
- Especificaciones del equipo.

- Planos de distribución del sitio.
- Estrategias de control (sistemas de seguridad pasivos, contención, aislamiento, mitigaciòn.)
- Políticas de operación y mantenimiento.
- Procedimientos de operación.
- Prácticas de mantenimiento.
- Modificación de procesos.
- Historia operativa.
- Planes de respuesta a emergencia.

Los datos disponibles para un análisis de riesgos con frecuencia son incompletos o inadecuados. Por lo que la opinión de expertos es necesaria, en general para evaluar los datos existentes y su adecuación a un análisis de riesgos.

De manera conceptual el análisis de riesgos se desarrolla en diferentes etapas, que se mencionan a continuación.

- Definir el ámbito de estudio.
- Identificar y evaluar peligros.
- Analizar y cuantificar riesgos.
- Evaluar tolerancias.
- Volver a configurar y mitigar donde sea necesario; volver a calcular el riesgo.
- Revisar la tolerancia al riesgo (aceptabilidad); continuar la mitigación de ser necesario.

2.3 EVALUACIÓN CUANTITATIVA DE RIESGOS [24][6]

Los equipos que se utilizan en cualquier industria y en la industria química en particular, constan de una serie de componentes que se disponen de acuerdo a un diseño previo, las posibilidades de falla para una instalación son muchas. Puede existir una falla en la concepción inicial de la misma en su diseño o el equipo puede haberse utilizado en condiciones distintas a las que fue diseñado. Puede haber existido un defecto que no fue detectado en la etapa de construcción o bien la instalación puede ser utilizada indebidamente o sin el necesario mantenimiento, también pueden producirse fallas por causas externas o simplemente alguno de los componentes puede haber llegado al límite de desgaste que es capaz de soportar para seguir funcionando correctamente, etc.

La ingeniería de la confiabilidad es la rama de la ingeniería que trata de la relación de la confiabilidad con el correcto funcionamiento de sus componentes. Sus fundamentos se desarrollaron para fines militares a partir de la segunda guerra mundial, extendiéndose posteriormente, a la industria aeroespacial, nuclear y electrónica en general, después al resto de las industrias. Las fallas de un equipo ocurren como resultado de una interacción compleja de sus componentes individuales y las circunstancias de la operación del mismo, en ocasiones la falla puede deberse directamente a errores humanos, al mal diseño o falta de mantenimiento. En realidad, cualquier falla es en última instancia una falla humana, Puesto que todo equipo ha sido creado, instalado y utilizado por seres humanos, pero cuando se habla de fallas humanas como causa de un accidente suele entenderse que la falla está relacionada con una acción errónea directamente relacionada con el accidente.

La confiabilidad de un equipo se define como la probabilidad de que, bajo determinadas circunstancias, el equipo realice sus funciones dentro de un nivel de tolerancia esperado, durante un intervalo de tiempo determinado o de demanda.

Esta definición resalta tres puntos importantes acerca de la confiabilidad de los equipos como son:

- La probabilidad.
- Una función de exposición periódica.
- Una función que define la falla de un equipo.

Por lo tanto, la exposición periódica puede ser expresada en términos de una variable continua, tal como el tiempo o una función de variable discreta, tal como el número de demandas impuesto a una pieza de equipo. Como consecuencia, la confiabilidad de un equipo puede ser expresada como una función continua o discreta y usando la terminología desarrollada en probabilidad y estadística, la confiabilidad de un equipo o simplemente la confiabilidad pueden ser expresadas de la forma siguiente:

$$R(t) = 1-P(t) \qquad (1)$$

Donde R(T) es la confiabilidad como una función del tiempo, P(t) es la función probabilidad de falla como una función del tiempo y t es el tiempo.
La derivada de P(t), con respecto al tiempo dP(t)/dt, da una función de densidad con respecto al tiempo, también llamada función de densidad de falla (f(t)) .

$$f(t) = dP(t)/dt \qquad (2)$$

El producto f (t) •dt proporciona la probabilidad de que el sistema falle entre t y t+dt, supuesto que ha funcionado hasta el tiempo t. Análogamente, la probabilidad de que el sistema falle entre dos tiempos cualesquiera t_1 y t_2 viene dada por:

$$P(t_1, t_2) = \int_{t_1}^{t_2} f(t)dt \qquad (3)$$

La tasa de fallas instantáneas en una población de equipos o de componentes puede expresarse Como:

$$\mu(t)=-(1/N)*(dN(t)/dt) \qquad (4)$$

Donde N es el número de componentes que permanecen en funcionamiento a tiempo t y μ(t) es la tasa instantánea de fallas a tiempo t, con unidades de fallas por componente y por unidad de tiempo. La integración de la ecuación (4) entre 0 y t lleva a:

$$N = N_0 \exp(-\int_0^t \mu(t)dt) \qquad (5)$$

Donde N_0 es el número inicial de componentes funcionando a tiempo cero. Por lo tanto, la confiabilidad se define como:

$$R(t) = \exp(-\int_0^t \mu(t)dt) \qquad (6)$$

En el caso de que la tasa de falla sea constante, la ecuación (5) se convierte en:

$$N = N_0 \exp(-\mu t) \qquad (7)$$

La ecuación (7) corresponde a un tipo especial de distribución de probabilidades denominada distribución exponencial, que se caracteriza por un valor de μ constante. De acuerdo con las ecuaciones anteriores, la confiabilidad, probabilidad de falla y densidad de falla para una distribución exponencial viene dada por:

$$R(t) = e^{-\mu t} \qquad (8)$$

$$P(t) = 1 - e^{-\mu t} \qquad (9)$$

$$f(t) = \mu e^{-\mu t} \qquad (10)$$

A partir de la ecuación anterior es inmediato hallar el tiempo medio hasta el primer fallo como el primer momento de la función densidad de falla.

$$MTBF = \int_0^\infty tf(t)dt = 1/\mu \qquad (11)$$

Al usar la distribución exponencial es importante notar que la confiabilidad R(t) es función del tiempo de operación del componente y el tiempo medio entre fallas (MTBF). El MTBF es una medición promedio del tiempo hasta que el componente falle. Si un número grande de componentes idénticos fuera probado hasta fallar, el MTBF será calculado sumando el tiempo de operación hasta que fallen dividido por el número de equipos de prueba.

2.3.1 Tasa de falla de los equipos:

Las tasas de falla de los equipos pueden ser definidos por su exposición periódica con respecto al tiempo y con respecto a la demanda:

$\mu(t)$ = número de fallas del equipo con respecto al tiempo/número de piezas del equipo expuestas a la falla.

Donde t es tiempo.

Similarmente, una tasa de falla del equipo referido a la demanda puede ser definido como:

$\mu(n_D)$ = número de fallas del equipo con respecto a la demanda/número de piezas del equipo expuesto a la falla.

Donde n_D = representa el número de demandas

Para minimizar la incertidumbre en la estimación de la tasa de falla de las expresiones anteriores, únicamente se aplicaran en las piezas de equipo que trabajan en condiciones similares de operación y mantenimiento.

a) **La tasa de falla referida al tiempo**, es de manera frecuente presentada como el número de fallas por 10^6 hr, para equipos que están funcionando como podría ser; una bomba en operación, un trasmisor de presión o temperatura.

b) **La tasa de falla referida a la demanda**, se representa como el número de fallas por 10^3 demandas y son para equipos que están normalmente estáticos, pero que están bajo un intervalo de variación, como es el caso de un interruptor.

2.3.2 Factores importantes que influyen en la tasa de falla de los equipos [6] [7] [23]

Varios factores pueden influir en la tasa de falla de los equipos. Estos incluyen:

a) Descripción del equipo (tipo, tamaño, fronteras):

- **Tipo**; las fallas de los diferentes equipos depende del tipo de operación del equipo, ejemplo un equipo rotatorio se espera que sus fallas sean diferentes, a un recipiente de proceso y una línea de proceso. Las tasas de fallas son también diferentes dentro de cada clase de equipo.
- **Fronteras del equipo**; las fronteras necesitan ser muy bien definidas. La tasa de falla de una bomba incluye el motor, la transmisión, el eje, los sellos, la carcasa, el impulsor y el elemento de control que es diferente del caso en el que la frontera fuera solamente la bomba.
- **Tamaño del equipo**; esto en términos generales incluye la proporción de flujo, presión, potencia, etc. Los equipos pequeños pueden sufrir de problemas que no se pueden presentar en las máquinas grandes y viceversa.

b) Normas de diseño:

- Las normas de diseño requeridas en los equipos son generadas para prevenir recurrencias de fallas históricas de los equipos. Por lo tanto, los equipos diseñados bajo normas no se espera que fallen del mismo modo ni con la misma frecuencia, que los equipos diseñados fuera de estas normas.

c) Materiales de construcción:

- Mientras, se parte del supuesto que los materiales de construcción son seleccionados para ser compatibles con el proceso promedio, una diversidad de materiales puede ser aceptado para un servicio de operación dado. La tasa de falla de los equipos en tales servicios debe esperarse que difiera de acuerdo al material diferente que se ha utilizado.

d) Estrategias de operación:

- La operación continua bajo condiciones uniformes es algunas veces menos complicada que alternar el paro y arranque. Los ciclos de temperatura o presión, carga en el arranque, e incluso servicios en estado de espera pueden incrementar la tasa de falla de los equipos. Las estrategias de operación también consideran el nivel de entrenamiento y desempeño del personal de operación.

e) Medio ambiente interno:

- La temperatura, presión, vibración etc, de un proceso puede tener un efecto significativo en la confiabilidad de un equipo.

f) Medio ambiente externo:

- El medio ambiente externo tendrá un efecto variado en los diferentes sistemas. Los factores ambientales que tienen un efecto en la tasa de falla de los equipos incluye humedad, sales atmosféricas, altitud, polvo, luz solar, calor, etc.

g) Edad de trabajo del equipo:

- El tiempo de uso del equipo tiene una significativa influencia en la tasa de falla. Cuando se tiene una irregularidad en el mantenimiento y estrategias de reemplazo, la probabilidad de que el equipo falle se incrementará con el tiempo de trabajo.

Muchos de estos factores son considerados en el diseño, fabricación, instalación, arranque, operación y mantenimiento de los equipos para que la influencia de estos, sea controlada o en su caso eliminada.

2.4 MÉTODOS DE ANÁLISIS DE RIESGOS (BREVE DESCRIPCIÓN)

Todos los métodos y técnicas de riesgos, comparten la meta de identificar peligros en el proceso de manera sistemática y proporcionar un análisis preliminar, por lo general cuantitativo. De su significado relativo en términos de posibilidades y consecuencias ya que un peligro no identificado se puede convertir en un riesgo no controlable. Las técnicas enlistadas aquí son las de mayor uso; todas tienen valor para cumplir con los requerimientos de análisis de riesgos del proceso según las reglas de la Administración de Seguridad del Proceso de la Agencia de Seguridad y Salud Ocupacional (OSHA PSM), del Programa de Administración de Riesgos de la Agencia de Protección Ambiental (EPA RMP) y otros marcos importantes de la administración de la seguridad del proceso.

Si bien cada técnica varía en términos de datos específicos que necesitan recopilarse y en términos del tipo de análisis que proporcionan, todos trabajan partiendo de una base general de información similar, incluyendo puntos como:

- Cómo funciona la planta o el sistema.
- Planos y procedimientos detallados del proceso.
- Modos de fallas del equipo y sus efectos resultantes.
- Factores que contribuyen al error humano.

El análisis de riesgos se aplica en las diferentes etapas de evolución de la planta como son: Diseño, construcción, puesta en marcha, operación, paro, modificaciones / ampliaciones y desmantelamiento. Donde se puede aplicar una o más de las técnicas dependiendo de las necesidades y el rigor del análisis.

Los métodos de identificación de riesgos se dividen en tres categorías: métodos cualitativos, semi-cualitativos y cuantitativos y estos métodos se describen a continuación [24]:

MÉTODOS CUALITATIVOS [24]: Lista de verificación (CHECKLISTS), Qué pasa si (WHAT IF), Análisis de efectos y modos de falla (FMEA), Análisis de riesgos y operabilidad (HAZOP)

a) Lista de verificación (checklists):

Es un recordatorio útil que, por lo general se ha elaborado a través de los años por distintas personas y que permite comparar el estado de un sistema con una referencia externa, identificando de forma directa carencias de seguridad en algunos casos, o las áreas que requieren un estudio más profundo en otros.

Las listas de comprobación pueden aplicarse a la evaluación de equipos, materiales o procedimientos y el grado de detalle varía desde las listas generales a las que se elaboran para equipos, procesos o procedimientos muy específicos.

b) Análisis ¿qué pasa sí.....? "What if"

Es menos estructurado que otras técnicas de análisis de riesgos, debido a esta falta de estructuración, se requiere una mayor experiencia por parte de los integrantes del equipo humano que lo lleva a cabo, ya que de lo contrario, se podría tener omisiones importantes.
El objetivo de un análisis "WHAT IF" es considerar las consecuencias negativas de posibles sucesos inesperados. Utiliza la pregunta QUÉ PASARÍA SI, aplicada a desviaciones en el diseño, construcción, modificación y operación de instalaciones industriales. Las preguntas se realizan sobre áreas concretas (por ejemplo, seguridad eléctrica, protección contra incendio, instrumentación de un equipo determinado, almacenamiento, manejo de materiales, etc.) por un grupo de dos o tres expertos que poseen documentación detallada de la instalación, procedimientos de operación acceso a personal de la planta para proveer de información complementaria. Por lo general, de la aplicación de la pregunta QUE PASARÍA SI, se obtiene sugerencias de posibles sucesos iniciadores y fallas a partir de las cuales puede producirse una desviación peligrosa.

c) Análisis de efectos y modos de falla (FMEA):

Es una técnica adaptada de la industria aeroespacial mediante la cual el analista considera los diversos modos de fallas de partes del equipo y evalúa los efectos de estas fallas en el sistema o en la planta. Por ejemplo, una válvula de control puede fallar en la posición "abierto" o "cerrado", una bomba puede fallar al detenerse o al arrancar, un transmisor puede dar lecturas erróneas altas o bajas o un intercambiador de calor puede tener una fuga al fluir del proceso a servicio o de servicio a los laterales del proceso. La respuesta del sistema a una falla del equipo determina los efectos de un modo de falla. Las fallas de equipo pueden iniciar o contribuir a un accidente. Por ejemplo, la falla de un controlador de presión podría iniciar la falla de una válvula de alivio y contribuir a la ruptura de un recipiente. El modo de falla puede identificarse de la manera siguiente:

- Con una pérdida de función del componente (deja de actuar).
- Función prematura (actúa, antes de que se produzca la demanda).
- Función fuera de tolerancia, falla o característica física indeseada como por ejemplo, una fuga pequeña, observada durante una revisión (modo de falla incipiente).

En el análisis todos los modos conocidos de falla de los componentes se consideran por etapas y las consecuencias de la falla son analizadas y registradas.

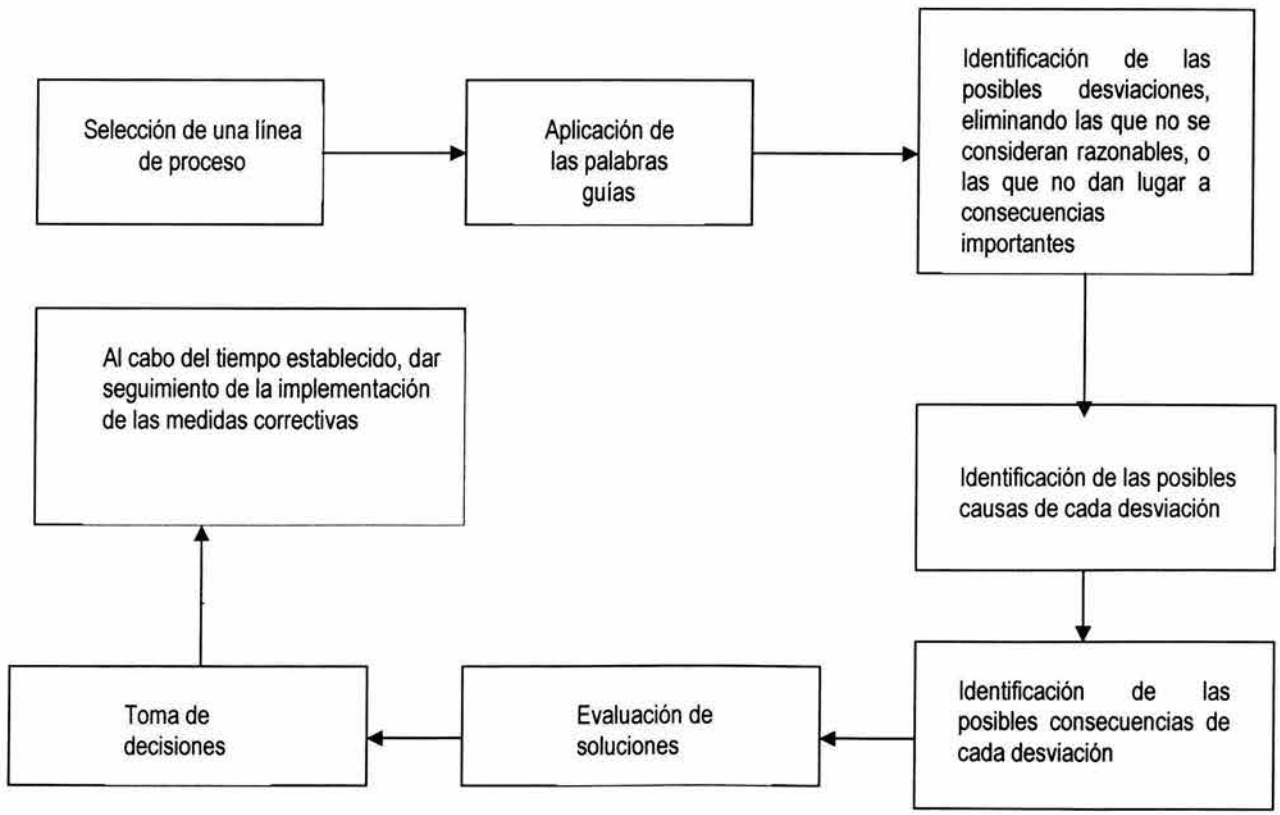
Se utilizan listas de verificación que identifican cada modo de falla posible para cada tipo de componente.

d) Análisis de riesgo y operabilidad (HAZOP)

Esta técnica (figura 2.0) fue desarrollada en el Reino Unido a mediados de la década de 1960 y tuvo una amplia utilización en 1970. La técnica fue definida en un código de la asociación de industriales químicos y está descrita en las guías de procedimientos de evaluación de peligros [5].

Un estudio HAZOP sirve para identificar problemas de seguridad en una planta y también es útil para mejorar la operabilidad de la misma. La suposición implícita de los estudios HAZOP es que los riesgos o los problemas de operabilidad aparecen sólo como consecuencia de desviaciones sobre las condiciones de operación que se consideran normales en un sistema dado y en una etapa determinada (arranque, operación en régimen estacionario, operación en régimen no estacionario, paro de planta). De esta manera, tanto si el análisis HAZOP se aplica en la etapa de diseño como si se realiza sobre una instalación ya construida, el procedimiento consiste en evaluar línea a línea y recipiente a recipiente, las consecuencias de posibles desviaciones en todas las unidades de un proceso continuo o en todas las operaciones de un proceso intermitente.

Figura 2.0 Representación gráfica de Técnica HAZOP [24]



La técnica HAZOP puede describirse como una lluvia de ideas estructuradas, realizadas por un equipo de ingenieros, operadores y diseñadores experimentados. En su formato básico, utiliza un protocolo formal de 7 palabras guías (tabla 2) para examinar todas las formas en que un sistema de proceso puede desviarse de su condición normal y operación más segura.

Estas palabras guías son: **NO, MÁS / MENOS, ADEMÁS DE, COMO PARTE DE, INVERSO Y EN VEZ DE.**

TABLA 2.0 PALABRAS GUÍAS

NO	No se consigue las intenciones en el diseño. Ejemplo: no hay flujo en una línea.
Más /menos	Aumento o disminución cuantitativa sobre la intención de diseño.
Además de	Aumento cualitativo. Se consigue las intenciones de diseño y ocurre algo más.
Parte de	Disminución cualitativa. Sólo parte de los hechos transcurre según lo previsto.
Inversión	Se obtiene el efecto contrario al deseado
En vez de	No se obtiene el efecto deseado. En su lugar ocurre algo completamente distinto.

Estas palabras han sido elegidas con cuidado para explorar toda desviación posible en un sistema dado, una vez identificada una desviación con estas características, el paso siguiente consiste en analizar sus causas, consecuencias y posibles acciones correctoras, llevándose un registro ordenado de todo ello, en algunos casos se requiere un análisis más profundo, que incluya, por ejemplo, una simulación por computadora del accidente para estimar sus consecuencias y/o un estudio formal de la probabilidad del suceso. En este caso, el equipo HAZOP puede recomendar un estudio más profundo antes de sugerir la implementación de medidas concretas. En otras muchas circunstancias el análisis HAZOP es suficiente para decidir la aplicación de medidas correctoras o incluso cambios de mayor impacto en el diseño. Por último, es preciso garantizar un registro sistemático de los resultados del análisis, lo que habitualmente se realiza en el formato tradicional en columnas.

MÉTODOS CUANTITATIVOS [24]: Análisis de Árbol de Fallas. (FTA), Análisis de Árbol de Eventos (ETA), Análisis de Confiabilidad Humana.

a) Análisis de árbol de fallas (FTA)

Los comienzos de la utilización en la industria química del análisis de árbol de fallas (faul tree analysis) se remonta a la década de los sesenta, tras el desarrollo de la técnica por parte de los Laboratorios Bell.

El análisis del árbol de fallas supone que un suceso no deseado (un accidente o una desviación peligrosa de cualquier tipo) ya ha ocurrido y busca las causas del mismo y la cadena de sucesos que puede hacer que tenga lugar. No necesariamente, todas las posibles causas y cadenas de evolución son identificadas, por lo que es recomendable combinar el análisis FTA con otras técnicas que aumenten la fiabilidad de la identificación, ya que sigue siendo válido el principio general de que los riesgos sin identificar son riesgos incontrolables.

El análisis de árbol de fallas es por lo tanto, un proceso deductivo que permite determinar como puede tener lugar un suceso particular. Como método de análisis de riesgos es de los más estructurados y puede aplicarse a un solo sistema o a sistemas interconectados.

En relación con las técnicas discutidas hasta ahora, el análisis FTA posee la ventaja adicional de servir no sólo para una identificación de peligros, sino para una cuantificación de los riesgos involucrados.

El FTA descompone un accidente en sus elementos contribuyentes, ya sean estos fallas humanas o de equipos de la planta, sucesos externos, etc. El resultado es una representación lógica en la que aparecen cadenas de sucesos capaces de generar el suceso culminante que ocupa la cúspide del árbol. En sistemas complejos es una técnica que requiere tiempo y experiencia, a pesar de ello se han desarrollado técnicas matemáticas que permiten la simplificación de árboles de fallas y existen en el mercado paquetes de computación que facilitan su construcción.

b) Análisis de árbol de eventos (ETA)

Evalúa las consecuencias que pueden tener lugar en un evento determinado. En este caso no interesa tanto estudiar como puede originarse el evento iniciador, sino cuáles son sus posibles resultados. Por lo tanto, en el análisis ETA se hace énfasis en un evento inicial que se supone que ocurrió y se construye un árbol lógico que conecta dicho evento inicial con los efectos finales, donde cada rama del árbol representa una línea de evolución que conduce a un efecto final (o a la ausencia de éste si una secuencia de circunstancias favorables es capaz de anular sus consecuencias). El análisis de árbol de eventos es adecuado para estudiar las posibles secuencias de evolución de los acontecimientos tras un accidente. Esto permite analizar los escenarios posibles y establecer entre ellos una jerarquía en cuanto a su gravedad y verosimilitud, seleccionar situaciones de emergencia para su evaluación cuantitativa y preparar respuestas a las mismas. El análisis de árbol de eventos se desarrolla de acuerdo con la secuencia siguiente:

- Identificación de eventos iniciadores relevantes.
- Identificación de las funciones de seguridad diseñadas para responder al evento iniciador.
- Construcción del árbol de eventos.
- Descripción de las cadenas de acontecimientos resultantes.

c) Análisis de confiabilidad humana

Un análisis de confiabilidad humana evalúa los factores que influyen en cómo se desempeñan los operadores, personal de mantenimiento, técnicos, ingenieros, supervisores y personal de planta. Puede utilizar uno de varios tipos de análisis de tareas que describen las características físicas y ambientales de una tarea, junto con las habilidades, conocimientos y capacidades requeridas para desempeñar la tarea con éxito. La técnica identifica situaciones que pueden causar accidentes y también puede utilizarse para trazar las causas de errores humanos.

Todos los análisis de confiabilidad humana tienen varias características comunes:

- Identificación de tareas desempeñadas (o, si la planta está en la etapa de diseño) por los operadores.
- Representación de cada tarea por algún método, como el dividir la tarea en componentes para identificar posibilidades de error y puntos de interacción con equipo de planta.
- Para resultados cuantificados, se utilizan los datos o estimados derivados de los registros históricos; como la identificación de cualquier técnica que cuente con su propia base de datos.
- Para la cuantificación de resultados, la identificación de la existencia de factores que conforman el desempeño que toman en cuenta la tensión la capacitación y la calidad de muestras y controles utilizados por los operadores.

MÉTODOS SEMI CUANTITATIVOS [24] [3]: Índice Dow y Mond, análisis de capas de protección (LOPA)

a) Índice Dow y Mond:

Proporciona un método directo y simple de estimar el riesgo global asociado con una unidad de proceso, así como de jerarquizar las unidades en cuanto a su nivel general de riesgo. No son, por lo tanto, sistemas que se utilicen para señalar riesgos individuales, sino que proporcionan un valor numérico que permite identificar áreas en las que el riesgo potencial alcanza un nivel determinado. Sobre estas áreas puede en caso necesario, aplicarse un análisis de riesgo más detallado, por lo que el valor obtenido para el índice de riesgo puede ser útil a la hora de decidir la profundidad del estudio. En todo caso, los índices de riesgo son útiles porque proporcionan una estimación rápida y bastante confiable del orden de magnitud de determinados riesgos en una unidad de procesos. El índice Dow, de incendio y explosión, tiene en cuenta aspectos relacionados con los riesgos inherentes del material, las cantidades manejadas, condiciones de operación, etc.

Estos factores son contabilizados de manera sucesiva para obtener una estimación del valor del índice, del área que pueden verse afectados por un accidente, el daño a la propiedad dentro de la misma y los días de operación perdidos por causas del accidente.

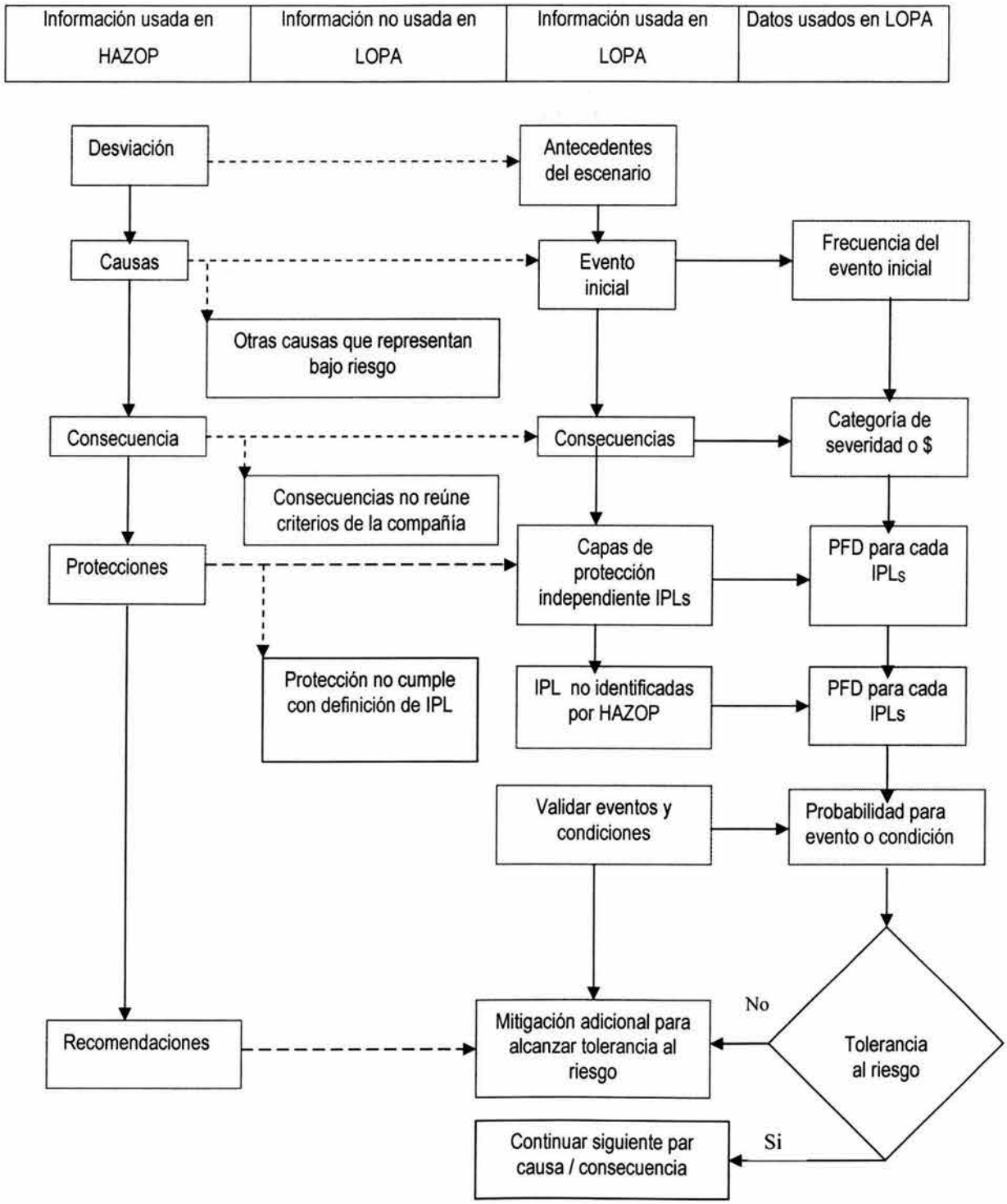
El índice Mond similar en muchos aspectos al anterior y que además incluye de manera especifica aspectos de toxicidad de materiales. Sin embargo, el índice Dow permite una estimación algo más fácil de visualizar debido al uso preferente de gráficas frente a ecuaciones y en su última edición tiene en cuenta, si bien de manera marginal, aspectos de toxicidad, con la inclusión de una penalización especifica.

2.5 Análisis de las capas de protección (LOPA) [3]:

LOPA es una forma simplificada de evaluación de riesgos (semi cuantitativa). Usa categorías de órdenes de magnitud para evaluar la frecuencia de eventos iniciales, gravedad de consecuencias y probabilidad de fallas de capas de protección independiente, con la finalidad de aproximarse al escenario de riesgo. Es una herramienta de análisis elaborada sobre la información desarrollada durante la evaluación de riesgos cualitativa, tal como un análisis de riesgos y operabilidad (HAZOP) y es implementada en el uso de una serie de reglas (figura 2.1).

Como muchos otros métodos de análisis de riesgos, el propósito primario de LOPA es determinar si hay suficientes capas de protección en un escenario de riesgo. Un escenario de riesgo requiere de una o más capas de protección que dependen de la complejidad del proceso y de la gravedad potencial de las consecuencias. Para un escenario dado, sólo una capa de protección debe ser trabajada con éxito para prevenir las consecuencias. Sin embargo, dado que ninguna capa es de total eficacia, suficientes capas de protección deberían ser proporcionadas para mitigar el riesgo de un accidente tolerable. LOPA proporciona una base consistente para juzgar si hay suficientes capas de protección independientes para controlar el riesgo de un accidente para un escenario dado. Si la estimación de riesgos de un escenario no es aceptable, deberán ser implementadas capas de protección adicionales. Pueden ser evaluadas también alternativas de diseño de seguridad inherente, LOPA no sugiere cuáles capas de protección adicionar en forma independiente o qué diseño seleccionar, pero ayuda a juzgar entre diferentes alternativas para mitigar un riesgo.

Figura 2.1. Método LOPA vs. HAZOP [3]



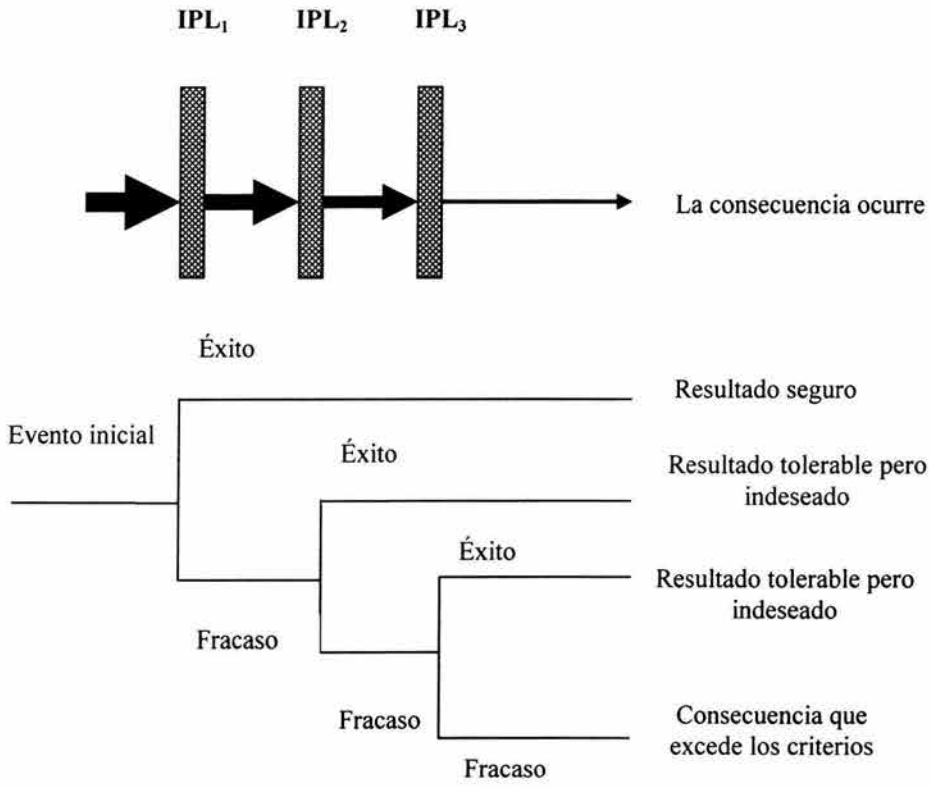
QUÉ HACE LOPA: Proporciona un método para evaluar el riesgo de un escenario de accidente.

- Está limitado a evaluar un simple par de causa-consecuencia para un escenario. Un par de causa –consecuencia es seleccionado para su análisis, este método determinará que ingeniería y controles administrativos (llamadas protecciones) cubren la definición de capas de protección independientes y entonces se estima como es el escenario de riesgo. Los resultados pueden ser extensivos para hacer juicios sobre los riesgos y ayudar a decidir de que magnitud es la reducción de riesgos adicional que se requiere para alcanzar un nivel de riesgo tolerable.

Otro camino para entender LOPA es analizar lo relativo a la evaluación de riesgos cuantitativos. En este contexto, un escenario LOPA representa un solo camino (se seleccionará la trayectoria de peores consecuencias) en el análisis de un árbol de eventos (Figura 2.2). Un árbol de eventos muestra todos los posibles resultados (consecuencias) de un evento inicial, para LOPA el análisis debe limitarse a la selección de la peor consecuencia.

En muchas aplicaciones de LOPA, el objetivo del analista es identificar todos los pares de causa-consecuencia que pueden exceder la tolerancia del riesgo. En otros, el análisis seleccionará el par causa-consecuencia que probablemente represente el más alto escenario de riesgo de muchos, que pueden ser similares al seleccionado.

Figura 2.2 comparación de análisis de árbol de eventos y LOPA [3]



LOPA es un método que cae entre un método cualitativo y cuantitativo y es aplicado cuando el analista decide si es la mejor herramienta para juzgar un riesgo. El objetivo es seleccionar escenarios que el analista crea representen el más significativo escenario de riesgos.

2.5.1 Uso de LOPA en el ciclo de vida del proceso

LOPA puede ser usado en cualquier punto del ciclo de vida de un proceso o un servicio, pero es más usado durante:

- La etapa de diseño, cuando se tiene el diagrama de flujo de proceso y el diagrama de tubería e instrumentación, se usa para examinar escenarios, generados por otras herramientas de análisis de riesgos de procesos, tales como HAZOP, WHAT-IF, CHECKLIST, etc; como parte del diseño de una función instrumentada de seguridad.
- Las modificaciones a un proceso existente o a sus sistemas de seguridad o control (ejem; administración al cambio).

2.5.2 Cuándo usar LOPA:

- LOPA es por lo regular aplicable después de la evaluación de riesgos cualitativo usando el escenario identificado por el equipo de análisis de riesgos.
- LOPA puede también ser aplicado cuando un equipo de evaluación de riesgos considera que un escenario es muy complejo para elaborar un juicio de riesgos razonable, usando criterios cualitativos, o las consecuencias son muy severas para contar con una apreciación de un análisis cualitativo.

El equipo de evaluación de riesgo puede juzgar el escenario complejo si ellos:

- No entienden el evento inicial lo suficiente bien.
- No entienden la secuencia de eventos.
- No entienden si las protecciones son verdaderas capas de protección independiente.

LOPA puede ser usado como una herramienta de protección antes de una evaluación de riesgos cuantitativa más rigurosa. Cuando es usado de esta forma, cada escenario que genere una consecuencia especifica o nivel de riesgo deberá pasar a través de un análisis LOPA y entonces ciertos escenarios serán designados para una evaluación de riesgos más estricta. Por lo tanto, la decisión para proceder a aplicar un método de evaluación cuantitativo está basado en el nivel de riesgo determinado por LOPA o basado en la opinión del analista de LOPA.

El espectro de herramientas (figura 2.1) de análisis de riesgo va de aplicaciones cualitativas a las rigurosas de métodos cuantitativos; los métodos cualitativos son usados para identificar escenarios y juzgar si el riesgo es tolerable, como es el caso de los métodos HAZOP, WHAT-IF, CHECKLIST, FMEA, cuya aplicación a problemas simples es bueno y a problemas complejos es pobre.

Las herramientas semí-cuantitativas (o herramientas cuantitativas simplificadas) como son LOPA, FMEA cuantificado, INDICE DOW de explosión y fuego, son usados para proporcionar estimación de riesgos en órdenes de magnitud, cuya aplicación a problemas simples es buena y en el caso de LOPA a problemas complejos es regular.

Las herramientas cuantitativas como son árbol de eventos, árbol de fallas, análisis de confiabilidad humana, son adecuadas para analizar escenarios de riesgos complejos y excesivas para analizar escenarios de riesgos simples.

TABLA 2.1 ESPECTRO DE HERRAMIENTAS PARA LA TOMA DE DECISIONES BASADA EN EL RIESGO [3]

Análisis	Cualitativo	Cuantitativo simplificado	Cuantitativo Simplificado	cuantitativo	cuantitativo
Técnica	HAZOP,FMEA Checklist, What-if	FMEA ,índice dow	**LOPA**	Estimación rigurosa con árbol de eventos	Árbol de eventos, árbol de fallas, análisis de confiabilidad humana.
Aplicado a problemas simples.	Bueno	Bueno	Bueno	Excesivo	Excesivo
Aplicado a problemas complejos.	pobre	pobre	Regular	regular	Bueno

En general, se piensa que si el analista de riesgos puede tomar una decisión de riesgos razonables al usar únicamente métodos cualitativos, entonces LOPA puede ser excesivo. Sin embargo, LOPA puede ser mucho más eficiente que los métodos cualitativos para determinar la eficiencia de las capas de protección. LOPA no puede ser usado para remplazar análisis cuantitativos. Si los modelos de comportamiento humano complejo o modelos de falla de equipo son requeridos para entender el riesgo de un escenario, entonces los análisis cuantitativos deben ser los más apropiados.

2.5.3 Cómo trabaja LOPA

Como todo método analítico, LOPA tiene reglas que pueden ser divididas en etapas:

Etapa 1. Identifica la consecuencia para proteger el escenario. Puesto que LOPA evalúa escenarios que han sido desarrollados en un estudio previo, la consecuencia es identificada durante un análisis de riesgos cualitativo (tal como un estudio HAZOP). En seguida el analista evalúa la consecuencia (incluyendo el impacto) y estima su magnitud.

Etapa 2. Selección de un escenario de accidente. LOPA es aplicada a un escenario que puede provenir de otro análisis (tal como un análisis cualitativo), pero el escenario deberá describir un simple par de causa consecuencia.

Etapa 3. Identificar el evento inicial del escenario y determinar la frecuencia del evento inicial (eventos por año). El evento inicial debe conducir a las consecuencias (falla de protecciones). La frecuencia debe considerar aspectos de fondo del escenario, tal como la frecuencia del modo de operación para el cual el escenario es válido. Muchas compañías proporcionan guías para estimar la frecuencia que tengan consistencia con los resultados de LOPA.

Etapa 4. Identificar las capas de protección independiente y estimar la probabilidad de falla en demanda de cada capa de protección. Algunos escenarios requerirán únicamente una capa de protección independiente, mientras otros escenarios de accidentes requerirán muchas capas de protección independientes o capas de protección independiente de muy baja probabilidad de falla en demanda, para alcanzar un riesgo tolerable para el escenario. El reconocimiento de la existencia de capa de protección que reúnan los requerimientos de capas de protección independientes para un escenario dado es posiblemente la parte más importante del método LOPA.

Etapa 5. Estimar el riesgo del escenario por combinación matemática de los datos de consecuencia, evento inicial y capas de protección independientes. Esto implica que otros factores pueden ser incluidos durante el cálculo, dependiendo de la definición de consecuencias. Incluyendo aproximaciones de métodos gráficos y formulas aritméticas.

Etapa 6. Evaluar el riesgo para alcanzar una decisión acerca del escenario en estudio.

2.5.4 Criterios en la estimación de gravedad de consecuencias

En LOPA, la gravedad de consecuencias es estimada en órdenes de magnitud y además se requiere mucho menos esfuerzo en su evaluación que los modelos matemáticos, también facilita la comparación de riesgos de diferentes escenarios.

LOPA determina varios tipos de análisis de consecuencias y define que éstas son el resultado indeseado de accidentes de un escenario. Una de las primeras decisiones que una organización debe hacer cuando selecciona e implementa LOPA es como define las consecuencias.

Algunas compañías estiman el impacto final en términos de daños o averías. Los más comunes escenarios de interés para LOPA en la industria de los procesos químicos son las pérdidas de energía o materiales peligrosos contenidos. La pérdida de materiales contenida puede ocurrir por una serie de mecanismos tal como fuga de un recipiente, ruptura de una tubería, disparo de una válvula de alivio. El material descargado puede ser un líquido, gas o sólido o una combinación de éstos. Si el material descargado es inflamable éste puede ocasionar un fuego y/o explosión. En caso de ignición inmediata de un gas presurizado, un calentamiento en la reacción puede llevarse acabo. En la ausencia de ignición inmediata, el material puede quedar disperso para formar una nube de vapor con una ignición tardada como una llamarada o explosión. El líquido derramado puede quemar como el fuego concentrado si este prende.

Si el material de escape es tóxico, el personal de planta o la comunidad puede estar expuesto a concentraciones insalubres.* La radiación por fuego, sobrepresion de explosiones y concentraciones tóxicas de escapes tóxicos son llamados efectos físicos.

Los efectos físicos tienen impacto en personas, medio ambiente, propiedades y pueden resultar en perdidas tal como lesiones, muerte, daños al medio ambiente y daños a la propiedad. En adición a este efecto inicial, esto puede ir seguido con pérdidas en la interrupción de los negocios, pérdida en la calidad de los productos, destrucción y pérdidas de credibilidad con la comunidad, clientes y accionistas.

El intervalo de consecuencias generadas en un escenario incluye; la descarga de materiales peligrosos, la dispersión de materiales peligrosos, efectos físicos generado por incendios, explosiones y descargas tóxicas y la pérdida por impacto físico de personas. Todas estas consecuencias son cuantificadas por algún método de estimación. Por ejemplo, una descarga puede ser medida en términos de la cantidad descargada; la dispersión en términos de la distancia /área (para una concentración especifica); así también se puede cuantificar la pérdida

en términos de número de lesiones y muertes, daños a propiedad, pérdidas financieras o pérdidas indirectas.

Aproximación de consecuencias por el método LOPA

La evaluación de consecuencias es una parte integral de cualquier metodología de evaluación de riesgos. Qué consecuencias y cómo serán evaluadas, esto depende de varios factores, incluyendo el riesgo asociado con el escenario del accidente, la metodología de evaluación de riesgos adoptada por la organización y los recursos que la organización está dispuesto a invertir para mejorar la estimación.

Una categorización de consecuencias debe ser desarrollada para usar LOPA. Una organización debe entender el nivel de gravedad de consecuencias, donde estas incluyan el nivel de gravedad de los derrames químicos, reacciones químicas incontrolables, descomposiciones, fuegos, y explosiones. Muchos escenarios con descargas químicas deben necesitar modelarse para determinar la gravedad potencial de cierto tipo de riesgos. La organización puede desarrollar sus propios modelos, aplicar otros ya conocidos o usar tablas que estén disponibles para establecer el nivel de gravedad.

Antes de implementar LOPA. La organización debe haber entendido las consecuencias de los derrames químicos, desarrollar estrategias para que el analista de riesgos entienda como aplicarlo en un análisis de escenarios, las pautas para la categorización de consecuencias se desarrollan de tal forma que el analista de LOPA rara vez necesite un modelo matemático.

Cualquier organización que implemente LOPA deberá considerar el nivel de detalle para su análisis de consecuencia ya que esta selección puede afectar el nivel de error y la efectividad requerida del análisis.

LOPA genera una serie de criterios para eventos de derrames genéricos y sus posibles resultados:

a) Algunas compañías utilizan este tipo de criterios para identificar y cuantificar el tipo y tamaño de las descargas químicas. Estos criterios de tolerancia al riesgo asumen que los derrames de ciertas magnitudes tienen una posible probabilidad de dañar el medio ambiente, a la gente o la producción.

Estos criterios son un ejemplo que incluye una simple aproximación para categorizar las consecuencias de descargas químicas. A cada consecuencia se le asigna una categoría numérica del 1 al 5, el nivel 5 como el más severo, estos criterios incluyen tres matrices:

- La tabla 2.2 Relaciona tamaño de la descarga química con las propiedades físicas y tóxicas (esto evita la necesidad de cuantificar los cálculos de dispersión, etc.)
- La tabla 2.3 relaciona plantas típicas y tipo de daños o pérdidas de producción para cada categoría de consecuencias.
- La tabla 2.4 relaciona factores de costo equivalente para cada categoría de consecuencias.

- **Tabla 2.2. Guía semí-cuantitativa para determinar la gravedad de un escenario de riesgo de acuerdo a la cantidad de sustancia derramada** [3]

Características de la sustancia derramada	0.5 a 5 kg.	5 a 50 kg.	50 a 500 kg.	500 a 5000 kg.	5000 a 50,000 kg.	Más de 50,000 kg.
Extremadamente tóxica, arriba del PE*	Crítico Categoría 3	Mayor Categoría 4	Catastrófico Categoría 5	Catastrófico Categoría 5	Catastrófico Categoría 5	Catastrófico Categoría 5
Extremadamente tóxica abajo del PE o altamente tóxica arriba del PE	Menor Categoría 2	Crítico Categoría 3	Mayor Categoría 4	Catastrófico Categoría 5	Catastrófico Categoría 5	Catastrófico Categoría 5
Altamente tóxica abajo del PE o inflamable arriba del PE	Menor Categoría 2	Menor Categoría 2	Crítico Categoría 3	Mayor Categoría 4	Catastrófico Categoría 5	Catastrófico Categoría 5
Inflamable abajo del PE	Despreciable Categoría 1	Menor Categoría 2	Menor Categoría 2	Crítico Categoría 3	Mayor Categoría 4	Catastrófico Categoría 5
Combustible líquido	Despreciable Categoría 1	Despreciable Categoría 1	Despreciable Categoría 1	Menor Categoría 2	Menor Categoría 2	Crítico Categoría 3

*PE = Punto de Ebullición a 1 atmósfera

Tabla 2.3. Guía semí-cuantitativa para determinar la gravedad de un escenario de riesgo de acuerdo a las consecuencias en la producción y en las instalaciones (3)

Tipo de planta	Daños mecánicos a equipos que cuentan con relevo o no son esenciales	Planta fuera de operación por menos de 1 mes	Planta fuera de operación entre 1 y 3 meses	Planta fuera de operación por más de 3 meses	Ruptura de un recipiente de 3000 a 10,000 gal a presión entre 100 y 300 psig	Ruptura de un recipiente de más de 10,000 gal a una presión de más de 300 psig
Planta grande, productos principales	Menor Categoría 2	Crítico Categoría 3	Mayor Categoría 4	Mayor Categoría 4	Mayor Categoría 4	Catastrófico Categoría 5
Planta pequeña, productos secundarios	Menor Categoría 2	Menor Categoría 2	Crítico Categoría 3	Mayor Categoría 4	Mayor Categoría 4	Catastrófico Categoría 5

Tabla 2.4. Guía semí-cuantitativa para determinar la gravedad de un escenario de riesgo de acuerdo al costo total de las consecuencias (3)

Costo total del evento	0 a 10,000 dls	10,000 a 100,000 dls	100,000 a 1,000,000 dls	1 a 10 millones de dls	Más de 10 millones de dls
Categoría de las consecuencias	Despreciable Categoría 1	Menor Categoría 2	Crítico Categoría 3	Mayor Categoría 4	Catastrófico Categoría 5

Note que los criterios de las tablas 2.3 y 2.4 son usados cuando el escenario no involucra una descarga de materiales o cuando la categoría de severidad de consecuencias para el escenario

es más alta en las tablas 2.4 que en la tabla 2.2 o cuando a juicios de los analistas la tabla 2.4 es la que mejor describen las consecuencias.

Ventajas de estos criterios de evaluación de consecuencias:

El método es simple y fácil de usar ya que el tamaño o propiedades de las descargas son relativamente fáciles de evaluar. No se requiere de un modelo caso por caso. Una descarga de cierto tamaño es asignada a cierto valor de consecuencias independiente del efecto eventual (fuego, explosión, descargas tóxicas, lesiones muertes, etc.). Los criterios para pérdidas de producción son simples de evaluar.

Cuando los criterios de tolerancia al riesgo de la organización se combinan con los criterios mostrados en las tablas 2.2, 2.3, 2.4, el método permite evaluar visualmente donde se tiene riesgos falsos en relación con las directrices de la organización.

Desventajas de estos criterios de evaluación de consecuencias:

Esto requiere de la aceptación de la tabla de categoría de consecuencias o el desarrollo de la tabla de categoría de consecuencias por un modelado básico. El modelado básico consume tiempo y requiere de un buen entendimiento de técnicas de modelación y de los procesos físicos.

El producto final no es presentado en términos de índice de costos/muerte/daño, por lo cual puede causar problemas de interpretación.

b) Criterio de estimación cualitativa con daños humanos:

Otros criterios utilizados para evaluar la gravedad de las consecuencias; es considerar el impacto final sobre el ser humano como la consecuencia de interés más importante. Para llegar a estos resultados se usan juicios puramente cualitativos de cada escenario. Las consecuencias humanas son estimadas por el analista de LOPA, que usa las experiencias pasadas, de conocimientos anteriores o modela acontecimientos similares.

La tabla 2.5 muestra la categorización de las consecuencias como resultado de estos criterios. Los resultados de los riesgos que generan daños y/o muerte pueden ser comparados directamente a los criterios de tolerancia al riesgo para un evento individual o para todos los eventos asociados con un proceso o planta y entonces comparar los criterios de tolerancia al riesgo del proceso o plantas.

Tabla 2.5. Guía semí-cuantitativa para determinar la categoría de consecuencias de acuerdo a la Estimación cualitativa con daños humanos (3)

Categorización Cualitativa	Receptor	Descripción de los efectos potenciales
Consecuencia Muy alta	Personal	Muerte o lesiones que producen discapacidad permanente
	Comunidad	Uno o más heridos graves
	Medio ambiente	Descargas significativas con impacto severo hacia el exterior de las instalaciones y con probabilidades de causar efectos a la salud inmediatos o de largo plazo
	Producción	Destrucción mayor o total de una o varias áreas de proceso con un costo estimado mayor a 10 millones de dólares o pérdidas significativas de producción
Consecuencia alta	Personal	Uno o más heridos graves
	Comunidad	Uno o más heridos leves
	Medio ambiente	Descargas significativas con impacto severo al medio ambiente
	Producción	Daño mayor a una o varias áreas de proceso con un costo estimado mayor a 1 millón de dólares o algo de pérdida de producción
Consecuencia Media	Personal	Lesiones leves con posible suspensión de labores
	Comunidad	Quejas de la población cercana por olores o ruido
	Medio ambiente	Notificación de o a las autoridades ambientales o violación de permisos como resultado de emisiones
	Producción	Varios equipos dañados con un costo estimado mayor a 100,000 dólares y con pérdidas mínimas de producción
Consecuencia Baja	Personal	Lesiones leves sin suspensión de labores
	Comunidad	Sin daños, peligros o molestias en la población
	Medio ambiente	Evento intrascendente, sin notificaciones o violación de permisos
	Producción	Daños menores a algún equipo, con un costo menor de 100,000 dólares y sin pérdida de producción

Las ventajas de estos criterios son:

- Es sencillo de entender; mucha gente tiende a entender mejor las consecuencias en términos de los daños en lugar de la expresión de riesgo en términos del tamaño de la descarga.
- Comparación directa con las directrices del corporativo para un riesgo que genere daños y/o muerte o riesgos de una cierta pérdida monetaria.

Desventajas de estos criterios:

Implícitamente asume la probabilidad de ignición para una descarga inflamable, la probabilidad de daños y el que una persona esté presente en el área de riesgo, esto puede sobreestimar o subestimar el riesgo por muerte.

La tabla 2.5 son aún menos precisas (más subjetivas) que las tablas de categorización de descargas tales como las indicadas en las tablas 2.2, 2.3, 2.4

La estimación de la gravedad de las consecuencias puede variar entre diferentes analistas, al menos que una guía o criterios sean proporcionados por la compañía.

c) Criterios al utilizar estimaciones cualitativas, daños humanos y ajustes de probabilidades después de descarga.

Alternativamente, el analista LOPA puede al inicio estimar la magnitud de una descarga en forma cualitativa similar a lo indicado en la tabla 2.5 y después ajustar la frecuencia del evento para la probabilidad de que:

- El evento resultará en una nube tóxica o inflamable.
- Cuando una nube inflamable o fuente de ignición esté presente.
- Un individuo esté presente cuando el evento ocurra.
- Un individuo experimentará una consecuencia fatal (o perjudicial).

Las ventajas de este método son:

- Es sencillo de entender; mucha gente tiende a entender mejor las consecuencias en términos de los daños en lugar de la expresión de riesgo en términos de magnitud de la descarga.
- Comparación directa con las directrices de la compañía; muchas compañías ya han establecido directrices para caso de riesgos de daños o muerte.
- Ajuste de frecuencia; el ajuste de frecuencia puede dar una mejor estimación del riesgo por daños humanos.

Desventajas del método:

- Las simplificaciones hechas al evaluar las probabilidades de los eventos subsecuentes a la descarga. Los resultados de eventos del mundo real han demostrado ser significativamente mayores y menores que aquellos calculados por el analista. Sin embargo, si las aproximaciones consistentes son usadas, es razonable esperar que esté método resaltará escenarios con alto riesgo.
- La estimación de la gravedad de las consecuencias puede variar entre diferentes analistas, al menos que algunas directrices sean proporcionadas por la organización.
- Este método necesitaría ser ampliado para dirigir el impacto comercial o riesgo económico.

Parámetros extras para alcanzar la probabilidad del estado de impacto en el que los resultados deben ser incluidos en los cálculos de riesgos y estos pueden cambiar con el tiempo (dependiendo del número de gente o cambio de ubicación).

d) Criterios con estimación cuantitativa y daños humanos.

Este método es similar a las estimaciones cualitativas con error humano, pero usa análisis detallados para determinar los efectos en individuos y equipo. El método involucra el uso de modelos matemáticos (modelos computarizados complejos). Para simular las descargas, las subsecuentes dispersiones, y efectos térmicos, explosivos o tóxicos.

Las ventajas de estos criterios son:

- Se tiene un grado mayor de certeza acerca de la predicción de las consecuencias.
- Comparación directa con las directrices de la corporación.

Desventajas de estos criterios:

- Aunque los programas modelados son mucho más sofisticados que los métodos estimados, los resultados de los eventos reales han sido significativamente menores y mayores que aquellos calculados por analistas. los resultados modelados son afectados por las condiciones de descarga, estabilidad atmosférica, dirección de vientos, tiempo de ignición, etc. Hay miles de posibles permutaciones a considerar. Inevitablemente sólo unos cuantos representan casos que pueden ser seleccionados.
- El nivel de sofisticación requerido para modelar las consecuencias de un escenario es más desproporcionado que el usado para estimar el orden de magnitud de la frecuencia por método LOPA.
- El entrenamiento, experiencia y esfuerzo requerido para aplicar el modelo puede ser prohibitivo y estos análisis son aplicados a escenarios que ya han sido juzgados para tener posibles resultados fatales potenciales.

2.5.5 Identificacion de eventos iniciales

Para LOPA, cada escenario tiene un evento inicial simple. Los eventos iniciales son agrupados en tres tipos:

- Eventos externos; incluyen fenómenos naturales tales como temblores, hurácanes, inundaciones, terrorismo, accidentes mayores en instalaciones.
- Falla de equipo; estos pueden ser clasificados en fallas en los sistemas de control; defecto de software, falla de componentes de BPCS (sistemas de control básico de proceso), y fallas en los soportes de control como aire de instrumentos, electricidad etc. Fallas mecánicas; ocasionadas por desgaste, fatiga, corrosión. Vibración, defectos de diseño/fabricación/especificaciones y mantenimiento inadecuado que incluye sustitución

de materiales inapropiados, condiciones de operaciones extremas como sobrepresiones y altas o bajas temperaturas.

- Fallas humanas; causas relacionadas a fallas humanas; como errores por omisión de operación, mantenimiento de respuesta crítica, error de programación.

2.5.6 Estimacíon de frecuencias [23].

La frecuencia del evento inicial es normalmente expresada en eventos por año. Algunas fuentes usan otras unidades, tal como eventos por cada 10^6 horas.

El estimado de frecuencia puede ser validado al compararlo con datos de fallas de fuentes de la industria para un componente determinado del proceso. En términos generales, un estimado de frecuencia se basa en datos de la experiencia histórica de la propia compañía o dentro de su industria. Hace referencia a fuentes de información más amplia, como bases de datos de otro sector industrial, en cuanto a la experiencia histórica de un determinado equipo puede indicar problemas con el estimado. Al hacerlo, el analista necesita reconocer y registrar el hecho de que el equipo cubierto por estas bases de datos esté siendo utilizado para propósitos que no son precisamente equivalentes a sus usos en la industria de procesos.

Existen tres fuentes para datos de frecuencia (tabla 2.6):

- **Datos históricos específicos del sitio**. Estos datos pocas veces están disponibles para todo el equipo del proceso en un sitio, pero pueden encontrarse para puntos específicos. Sus mejores aplicaciones son para problemas observados con frecuencia. Una aplicación prometedora de los datos del sitio es su uso, combinado con datos genéricos, con técnicas estadísticas bayesianas para generar un mejor estimado de frecuencia que una base de datos única.
- **Datos genéricos históricos promedio de la industria**. Se dispone de datos genéricos para una amplia gama de equipos del proceso, pero como su nombre indica, los datos son un promedio de muchos sitios y de muchos procesos. Una vez adquiridos, se convierten en un uso muy eficiente (una tabla de revisión es adecuada para casos de

fallas "genéricas") y permiten el análisis de riesgos de todo el sitio, incluyendo cientos de casos, de fallas a realizar con eficiencia y en repetidas ocasiones. Por su naturaleza, no representa bien al equipo u operaciones que difieren de manera significativa a partir del promedio del cual se derivaron los datos.

- **Técnicas predictivas**. Estas se basan con frecuencia en técnicas de árbol de fallas o árbol de eventos de fallas, con un análisis adicional de acontecimientos de modo común, confiabilidad humana y externa. Estas técnicas pueden ser muy extensos en recursos y por lo tanto son más adecuadas para análisis de riesgos de problemas específicos. Estos se debe a que estas técnicas muestran con claridad la importancia relativa de mecanismos específicos y pueden diseñarse estrategias de mitigación para atender a los principales contribuyentes. También son útiles para volver a analizar riesgos de alta clasificación derivados de datos genéricos, para confirmar los mecanismos importantes y diseñar protecciones apropiadas.

Tabla 2.6 Comparación de técnicas de estimación de frecuencias [23]

MÉTODO DE ESTIMACION DE FRECUENCIAS	VENTAJAS	DESVENTAJAS
Datos específicos Del sitio	a) Mejores datos para ese sitio. b) Los datos tienen alta credibilidad.	a) Con frecuencia, bases estadísticas pequeñas. b) Puede no ser valido después de cualquier cambio. c) es poco probable que incluya acontecimientos raros o catastróficos.
Datos históricos Genéricos.	a) Disponible para una amplia gama de tipos de equipos. b) Las bases de datos tienen antecedentes conocidos para los cuales las ventajas y deficiencias son comprendidas. c) Poco costoso.	a) Puede ser inexacto para características específicas del sitio. b) Nuevas tecnologías o circunstancias pueden hacer inválidos los datos históricos.
Técnicas de predicción	a) Pueden evaluar modos de fallas muy específicos, que no atienden debidamente los datos genéricos. b) Los mecanismos de fallas se muestran con claridad, permitiendo medidas de mitigación y beneficios a ser evaluados con claridad. c) Resultados cualitativos valiosos.	a) Costosos y lentos en sus aplicaciones. b) No adecuado para grandes números de evaluaciones de acontecimientos principales. c) Muchas suposiciones pueden quedar ocultas en el árbol. d) Las secuencias de tiempo son difíciles de tratar. e) Las técnicas de predicción están más sujetas a errores o prejuicios del analista que el enfoque genérico.

Expresión de tasa de falla (tabla 2.7) [3]:

Hay varios caminos para expresar tasas de falla en la aplicación del método LOPA. El método usado debe ser consistente con el diseño y criterios básicos de la metodología LOPA. El método incluye:

- Sistema logarítmico.
- Sistema decimal.
- Notación científica.

Tabla 2.7 Formas de expresar la tasa de falla [3]

DENOMINACIÓN	Tasa de falla
Decimal	0.01 /año
Notación científica	$1x10^{-2}$ /año
Exponente	1E-2 /año
Logarítmica (Órdenes de magnitud)	2 /año

Valores cualitativos, tales como, baja, media, o alta o categorías 1, 2, o 3, son algunas veces usadas en versiones de eventos simples de LOPA,

2.5.7 Identificación de las capas de protección independientes (IPL).

Una capa de protección independiente es un dispositivo, sistema o acción, la cual es capaz de prevenir un escenario de consecuencias indeseables, independiente del evento inicial o de la acción de cualquier otra capa de protección asociada con el escenario. La efectividad e independencia de un IPL deben ser verificadas.

La diferencia entre un IPL y una protección es muy importante. Una protección es cualquier sistema, dispositivo o acción que probablemente interrumpirá la cadena de eventos continuos una vez que inició el evento. Sin embargo, no puede cuantificarse la efectividad de algunas protecciones debido a la falta de datos, la duda acerca de la independencia o efectividad u otros factores.

La efectividad de un IPL es cuantificada en términos de la Probabilidad de Falla en Demanda (PFD), el cual es definido como la probabilidad de que un sistema (en este caso la IPL) fallará al ejecutar una función especifica ante una demanda. Es un número sin dimensiones entre 0 y 1. El valor más pequeño de la PFD, indica que es más grande la reducción en frecuencias de las consecuencias para un evento inicial dado, es decir indica una protección con muy alta efectividad

Todas las IPL's son protecciones, pero no todas las protecciones son IPL's. Como ellas actúen y que efectividad hay en reducir las frecuencias o consecuencias de un evento inicial, así como las

características de estas capas y si ellas están reconocidas como capas de protección independiente son los elementos que se consideran en el método LOPA.

El método LOPA considera como capas de protección independientes de un proceso a los siguientes sistemas, dispositivos, o acciones.

a) Diseño del proceso.

En muchas compañías, se sabe que algunos escenarios no pueden ocurrir cuando el diseño del equipo de proceso es seguro. Por ejemplo, los equipos podrían diseñarse para resistir una presión máxima para un escenario en particular, para un tamaño del lote limitado, bajos niveles de inventarios, etc., los escenarios son eliminados inherentemente por características de diseño de procesos seguros.

La seguridad inherente (18) es una aproximación para la prevención de pérdidas durante el diseño de plantas de proceso. Se ha demostrado que, al considerar el costo de vida de un proceso y su operación una aproximación de seguridad inherente puede permitir una opción óptima de costos. La aplicación de la seguridad inherente en etapas tempranas del diseño del proceso rendirá los mejores resultados con respecto al proceso seleccionado, diseño conceptual y de ingeniería.

b) Sistemas de Control Básico de Proceso (BPCS) [3]

- Forma parte integral de las plantas de proceso para el control de sus variables, se encarga de restablecer las condiciones de operación fijadas para la eficiente y segura operación de las plantas, recibe el valor de la variable, la compara con el valor deseado (set point) y actúa para corregir la desviación.
- Es el sistema de control que continuamente monitorea y controla el proceso en las operaciones de la planta día a día. Puede ser considerada como una capa de protección si no está asociada con el evento inicial considerada en el escenario.

- Los sistemas de control básico de proceso (BPCS), que incluye los controladores manuales, es el primer nivel de protección durante la operación normal. El BPCS está diseñado para mantener el proceso en una región de operación segura. La operación normal de un lazo de control de los BPCS puede ser acreditado como un IPL si éste reúne los requerimientos apropiados. La falla de los sistemas de control básico del proceso puede considerarse como una causa o evento inicial de un escenario de riesgo. Cuando se considera usar los BPCS como una IPL, se debe evaluar la efectividad de los accesos y sistemas de seguridad tal como el error humano que puede degradar el desempeño de los BPCS.
- El BPCS puede estar formado de combinaciones de lazos simples de controladores neumáticos, lazos simples de controladores eléctricos, controladores lógicos programables (PLC´S) y sistemas de control distribuido (DCS´S). Ejemplos de funciones de control incluidos en BPCS son controladores en cascada, paro/arranque de bombas. también conocidos como controladores de regulación básica.

Este sistema es muy importante en la determinación de la tasa de demanda de los sistemas de protección. Debe minimizarse la probabilidad de que cualquier falla simple en el BPCS lleve a una demanda del SIS. Todos los modos de falla previsibles deben ser identificados del modo que se consideren en el diseño del sistema de protección.

En instalaciones de producción se pueden implementar funciones protectoras poco críticas (en base al análisis de riesgos) en el BPCS siempre que se cumpla que la integridad de seguridad no sea tan elevada como para implantar un SIS en áreas en las cuales es más que suficiente el BPCS, de otro modo el sistema de control debe ser diseñado como un sistema de seguridad.

c) Alarmas Críticas e Intervención Humana.

Estos sistemas son el segundo nivel de protección durante la operación normal y serán activadas por el BPCS. La acción o decisión que ejecuta el operador por la activación de las alarmas, puede confirmarse como un IPL cuando varios criterios son satisfechos para evaluar la efectividad de la acción. El nivel de confiabilidad está supeditado a la intervención y destreza del

personal de planta, por lo que es importante tener una capa de mayor confiabilidad cómo un sistema instrumentado de seguridad (SIS) que garantice la prevención o minimice los incidentes o consecuencias. Los procedimientos y el entrenamiento de la compañía pueden mejorar el desempeño humano en el sistema, pero por si mismas no son considerados como IPL.

d) Sistema Instrumentado de Seguridad (SIS).

Un SIS es una combinación de sensores, solucionadores lógicos, y elementos finales de control con un nivel de integridad de la seguridad específico, que al detectar condiciones irregulares en el proceso, tienen la función de llevar al proceso a condiciones más seguras, estos sistemas también reciben el nombre de interruptor automático (INTERLOCK) de seguridad, alarmas criticas de seguridad o sistemas de paro de emergencia y pueden desempeñar una o más funciones instrumentadas de seguridad. Un SIS es funcionalmente independiente del BPCS. Normalmente, se considera que un SIS es un IPL y que el diseño del sistema, el nivel de redundancia la cantidad y tipo de prueba determinarán la PFD del SIS.

Cada una de las funciones instrumentadas de seguridad del SIS tendrá su propio valor de PFD basado en:

- El número y tipo de sensores, solucionadores lógicos y elementos finales de control.
- El intervalo de tiempo entre pruebas funcionales periódicas de los componentes del sistema.
- El cumplimiento de reducción al riesgo de una función instrumentada de seguridad es definida en términos de su PFD.

Las normas internacionales han agrupado las funciones instrumentadas de seguridad por su aplicación en la industria de los procesos químicos en categorías llamadas niveles de integridad de la seguridad, y estas son definidas como:

SIL1 $1x10^{-1} \leq PFD < 1x10^{-2}$ estas funciones instrumentadas de seguridad son implementadas con un sensor simple, solucionador lógico y un elemento final de control.

SIL2 $1x10^{-2} \leq PFD < 1x10^{-3}$ estas funciones instrumentadas de seguridad son redundancias completas del sensor, solucionador lógico y el elemento final de control.

SIL3 $1x10^{-3} \leq PFD < 1x10^{-4}$ estas funciones instrumentadas de seguridad son normalmente redundancias completas del sensor a través del solucionador lógico y el elemento final de control esto requiere de cuidados de diseño y frecuente corrección de pruebas para alcanzar valores bajos de PFD. Muchas compañías tienen un número limitado de SIL3 debido a los altos costos asociados con la arquitectura.

SIL4 $1x10^{-4} \leq PFD < 1x10^{-5}$ estas funciones instrumentadas de seguridad están incluidas en la norma IEC61508 y 61511, pero tales funciones son difíciles de diseñar y mantener por lo tanto no son usadas en LOPA.

e) Protecciones físicas (sistemas de relevo).

Estos dispositivos (válvulas de relevo, discos de ruptura, etc.), cuando son del tamaño, diseño y mantenimiento adecuado son IPL's que pueden proporcionar un alto grado de protección contra la sobrepresion en la industria limpia. Sin embargo, su efectividad puede ser perjudicial al infringir las normas o servicios corrosivos de protección ambiental. Por ejemplo, si la actividad de inspección y mantenimiento son de baja calidad. Además, si el flujo de la válvula de relevo es descargado a la atmósfera, se pueden tener consecuencias indeseables que puedan afectar el medio ambiente.

f) Protecciones después de relevo (sistema de contención)

Estas capas de protección independiente (diques, cortina de vapor, sistema de drenaje, arrestadores de flama y detonación, etc.) son dispositivos pasivos que proporcionan un alto nivel de protección si tienen un diseño y mantenimiento correcto. Aunque su tasa de falla es baja, la posibilidad de falla debería ser incluida en el escenario. Además, si los sistemas de espuma, sistemas de detección de gas. etc., reúnen los requerimientos de capas de protección independiente, entonces algunos créditos deben ser tomados en cuenta para estos dispositivos en escenarios específicos.

g) Plan de respuesta de emergencia de la planta.

Estos sistemas (brigadas contra incendio, servicios de evacuación, sistemas manuales contra inundaciones, etc.) no son considerados como IPL ya que son activados después de iniciada los eventos y hay también muchas variables (ejemplo; demoras en el tiempo) que afectan su efectividad total para la mitigación de un escenario.

h) Plan de respuesta de emergencia a la comunidad.

Estas medidas que incluyen evacuación de la comunidad no son consideradas como capas de protección independientes ya que son activadas después de iniciada los eventos y hay también muchas variables que afectan su efectividad para la mitigación de un escenario. Estas no proporcionan ninguna protección para el personal de planta.

2.5.8 Características complementarias de las capas de protección independientes (IPL):

A) Para ser considerado una IPL como tal, el dispositivo, sistema, o acción debe ser:

- **Eficaz;** debe ser efectivo para prevenir consecuencias indeseadas asociadas con el escenario. En LOPA, la efectividad de una capa de protección independiente para reducir la frecuencia de una consecuencia es cuantificada usando su PFD. La determinación de los valores específicos o aproximados de PFD de una IPL es una parte importante del proceso LOPA. Una IPL se espera que opere de manera eficaz, pero cualquier sistema puede fallar, el valor más bajo de PFD le corresponderá el valor de seguridad más alto, indicando la condición que operará correctamente. Los valores de PFD son por lo general representados como los valores más cercanos en órdenes de magnitud. Se debe determinar si una protección es una IPL y evaluar el valor apropiado de la PFD para la IPL. Una buena ayuda para evaluar la efectividad de IPL es que la capa debe ser: bastante grande, rápida y fuerte.
- **Independiente** del evento inicial y de los componentes de cualquier otro IPL ya existentes para el mismo evento, el método LOPA evalúa el efecto del evento inicial, o que otras IPL, no interactúen con una IPL específica y a consecuencia de ésta

degrade su capacidad para desempeñar sus funciones. Su independencia requiere que la IPL sea independiente de: la ocurrencia o consecuencia del evento inicial y de la falla de cualquier componente de una IPL ya existente en el mismo escenario.

- **auditable**; la supuesta efectividad en términos de la prevención de consecuencias y PFD debe ser capaz de ser validada de alguna manera (por documentación, revisión, pruebas, etcétera). Un componente, sistema o acción debe ser auditable para demostrar que reúne los requerimientos de mitigación de riesgos establecidos por el método LOPA en las IPL. La revisión del proceso debe confirmar que la IPL es efectiva para prevenir las consecuencias si esta funciona como fue diseñada. La revisión deberá también confirmar que el diseño de la IPL, su instalación, pruebas de funcionalidad y sistemas de mantenimiento son adecuadas para alcanzar la PFD específica para la IPL. Las pruebas funcionales deben confirmar que todos los componentes de una IPL (sensores, solucionador lógico, elementos finales de control) son operables y que reúnen los requerimientos de LOPA para ser aplicados. La revisión del proceso deberá documentar las condiciones de las IPL encontradas, cualquier modificación hecha desde la pasada revisión y resolver cualquier corrección que sea requerida.

b) Las capas de protección pueden ser empleadas para prevenir o minimizar el efecto de incidentes y se clasifican en:

- **Activas.** Las capas de protección independientes activas son requeridas para moverse de una condición a otra en respuesta a un cambio de una propiedad del proceso (tal como temperatura o presión) o una señal de otro origen (tal como un interruptor). Una IPL comprende generalmente:

  1. Un sensor de algún tipo (instrumento, mecánico, o humano).
  2. Un proceso ejecutor de decisiones (solucionador lógico).
  3. Una acción (automática, mecánica, o humana).

- **Pasivas**. Las capas de protección independientes pasivas no requieren tomar una acción determinada para alcanzar la función de reducir los riesgos (reducen la frecuencia de

eventos de altas consecuencias). Estas IPL alcanzan la función de reducir los riesgos si su diseño mecánico es correcto y si es construido, instalado y mantenido correctamente, como es el caso de los diques, cuarto de control central (Bunker), arrestadores de detonación o flama. Estos dispositivos están diseñados para prevenir consecuencias indeseadas (derrames, edificaciones y equipos protectores contra; daños de explosión, fallas debido a la exposición al fuego en recipientes o tubería, en ondas de detonación o fuego a través de sistemas de tubería). Si los sistemas son diseñados adecuadamente pueden ser aceptados como capas de protección independientes con un alto nivel de confianza y reducirán de manera significativa la frecuencia de eventos con consecuencias de mayores potenciales.

- **Preventivas** (antes del evento) vs. **Mitigación** (después del evento); cuando consideramos que una IPL reducirá el riesgo asociado en un escenario es importante tener un claro entendimiento de que la IPL está diseñada para eso. Algunas IPL son diseñadas para prevenir el escenario de ocurrencia. Otras protecciones son diseñadas para reducir la severidad de las consecuencias del evento inicial, la mitigación de IPL reduce la frecuencia de los escenarios de consecuencias altas, ejemplo de mitigación de daños de la capas de protección independientes son los dispositivos de relevo de presión que son diseñados para prevenir la ruptura catastrófica de un recipiente, pero cuya operación satisfactoria puede resultar en otras consecuencias (segundo escenario). Por ejemplo, si es un dispositivo de relevo que emite materiales tóxicos o inflamables a la atmósfera, provocará que el analista considere si el riesgo asociado con el segundo escenario es aceptado o no. Si el riesgo fue considerado injusto, entonces el analista determinará si las capas de protección adicionales son requeridas para reducir la frecuencia de emisión del dispositivo de relevo a la atmósfera. Alternativamente, un analista deberá considerar si la emisión de la válvula de relevo será enviada a un desfogue o tanque neutralizador, para reducir el riesgo.

2.5.9 Protecciones no consideradas como IPLS.

En la Tabla 2.8. Se muestran las protecciones que no son consideradas como Capas de Protección Independientes.

Tabla 2.8. Ejemplos de Protecciones no consideradas como IPLs [3]

Protecciones no consideradas como IPL's	Comentarios.
Entrenamiento y Certificación	Estos factores pueden ser considerados en la evaluación del PFD con la acción del operador, pero por si solos no son considerados como IPLs.
Procedimientos.	Estos factores pueden ser considerados en la evaluación del PFD con la acción del operador, pero por si solos no son IPLs.
Inspecciones y Revisiones	Estas actividades se supone que están en lugar de las evaluaciones de riesgo y son la base para juzgar la determinación de la PFD. La revisión e inspección afecta la PFD de cierto IPL's. Prolongando los intervalos de inspección y prueba puede incrementar la PFD de una capa de protección independiente.
Mantenimiento	Esta actividad se supone que esta en lugar de las evaluaciones de riesgos y son la base para juzgar la determinación de la PFD. El mantenimiento afecta la PFD de cierto IPL's.
Comunicaciones	Es básico que exista una buena comunicación en la planta. Una mala comunicación afecta la PFD y de cierta forma las IPL's.
Señales	Las señales por si solas no son IPLs. Si las señales son ignoradas, inciertas u ocultas, entonces las señales afectan a la PFD de ciertas IPLs.
Protección contra incendio	Estas protecciones no son consideradas a menudo como una IPL como es un evento posterior para muchos escenarios, su disponibilidad y efectividad puede ser afectada por la explosión y fuego. Sin embargo, si una compañía puede demostrar que reúne los requisitos de una IPL, para un escenario dado, este puede ser usado como una capa (ejemplo; si en la activación de un sistema son usados tuberías de plástico o interruptores frágiles.

2.6 DEFINICIÓN Y FUNDAMENTOS DEL NIVEL DE INTEGRIDAD DE LA SEGURIDAD (SIL) EN LOS SISTEMAS INSTRUMENTADOS DE SEGURIDAD. (1) (10) (11) (14) (18)

El concepto del SIL se define como el nivel de desempeño en la operación necesaria para lograr el objetivo de seguridad de proceso del usuario. Para la industria de procesos se consideran tres niveles diferentes y se clasifican sobre la probabilidad de falla en demanda/factor de reducción del riesgo.

La determinación del nivel de integridad de la seguridad (SIL) de una instalación o sistema debe ser definido en base a un análisis cuantitativo o semi cuantitativo previó el cual puede ser realizado por la compañía que diseña el SIS o por otra instancia, ya que el nivel de integridad de la seguridad está en función de la confiabilidad y exactitud de los resultados de dicho análisis. Un problema potencial con los métodos cualitativos es que sus resultados con frecuencia, son subjetivos y no reproducibles, es decir, diferentes organizaciones pueden revisar el mismo proceso y proporcionar requerimientos de SIL muy diferentes entre si. Hay dos tipos de SIL, objetivo y de diseño.

El SIL OBJETIVO es la cantidad de reducción al riesgo con la cual contribuye una función instrumentada de seguridad y que se debe alcanzar como parte de la reducción de riesgo total para una función de seguridad. El propósito de seleccionar un SIL objetivo es especificar la reducción de riesgo requerido, es decir, la diferencia entre los niveles de riesgo existente y tolerable, en términos de SIL. Para la aplicación de esto se debe tener definido el nivel de riesgo tolerable para las instalaciones en estudio.

Se debe determinar el SIL para cada función de seguridad y no debe determinarse de manera global para un proceso o instalación, pues esto implicaría considerar los extremos superiores e inferiores en los valores asignados del SIL y se tendría como resultado deficiencias si el SIL es bajo o bien, una sobre especificación si se establece un SIL alto en el diseño del SIS.

Para establecer el nivel requerido de integridad del sistema de seguridad se deben considerar los siguientes parámetros:

- La severidad de las consecuencias si el sistema de seguridad falla al operar en demanda.
- La probabilidad de que el personal sea expuesto al riesgo.
- Medidas de mitigación para reducir las consecuencias del evento de riesgo.
- La frecuencia con la cual el sistema de seguridad se requiere que funcione.

El nivel integral de la seguridad se puede definir como una medida de la reducción del riesgo proporcionado por la función instrumentada de seguridad (SIF) basada en 3 niveles y cada uno de estos niveles está representado en órdenes de magnitud de reducción al riesgo.

A cada función instrumentada de seguridad se le asigna un SIL, el SIS por si mismo no tiene asignado un SIL, es decir el equipo no tiene asignado un SIL.

El SIL DE DISEÑO O REALIZADO es el SIL del diseño del software y hardware de la función instrumentada de seguridad (SIF) determinado y verificado por cálculos cuantitativos.

El concepto del SIL de diseño con respecto a la norma ISA S84.01 está referido a una medida del funcionamiento de los SIS relacionado sin más con los dispositivos que abarcan el SIS. Esta medida se limita a la integridad del dispositivo, configuración y los incidentes comunes inherentes al diseño específico del SIS. No se relaciona en forma explícita con la matriz de causa y efecto, sino que se relaciona con los dispositivos utilizados para prevenir un incidente específico. Además, el SIL no es una característica de un dispositivo específico. Es una característica del sistema que incluye; dispositivos de entrada de información, solucionador lógico y dispositivos de salida.

El SIL se define como la probabilidad (del SIS) para fallar ante una demanda. Una demanda ocurre siempre que el proceso alcancé la condición de disparo y hace que el SIS tomé la acción correctiva.

Debe ser entendido que el SIL y la disponibilidad son representaciones estadísticas de la integridad del SIS cuando ocurre la demanda del proceso. La aceptación de un SIL 1 significa que el nivel del peligro o riesgo económico es bajo y que un SIS con una disponibilidad de 90%

(o 10% de incidente) es aceptable. Por ejemplo, considere la instalación de un SIS con un SIL 1 para el incremento del nivel de líquido dentro de un tanque. La disponibilidad de 90% significaría que cada 10 veces que el nivel alcanzará el punto de nivel alto, habría un incidente predicho del SIS y el desbordamiento subsiguiente del tanque.

Las designaciones del nivel de integridad de la seguridad se pueden correlacionar a la probabilidad para fallar y a los requisitos de la disponibilidad del SIS según lo indicado en la (tabla 2.9) especificada por la norma ISA S84.01 y IEC 61511.

Tabla 2.9. SIL vs PFD [1]

SIL	Probabilidad de falla en demanda	Disponibilidad de la seguridad	% de incidentes
1	10E-1 a 10E-2	90.0-99.00	10 a 1
2	10E-2 a 10E-3	99.0-99.90	1 a 0.1
3	10E-3 a 10E-4	99.90-99.99	0.1 a 0.01

El concepto del SIL representa un factor importante en la actitud de la industria hacia el diseño de los sistemas de seguridad. SIL es la base del diseño para todas las decisiones de la ingeniería relacionadas con la función de seguridad. Cuando el diseño es completo debe ser validado contra el SIL.

En contraparte se puede decir que no hay regulaciones que asignen o asistan a la asignación de un SIL a los procesos determinados u operaciones químicas. Además, no hay regulaciones o estándares a seguir que recomienden SIL's específicos para ciertos peligros del proceso. La asignación del SIL es una decisión corporativa o de compañía basada en la gerencia de riesgos y la filosofía de la tolerancia del riesgo. La advertencia es que en el sentido legal los ingenieros deben aplicar buenas prácticas de ingeniería o metodologías aceptables de ingeniería. Esto significa que las compañías deben diseñar sus SIS para ser constantes con el funcionamiento de las unidades de proceso dentro de sus propias compañías y en otras compañías similares. Así los niveles de seguridad deben ser realizados con cuidado y ser documentados a conciencia.

La selección del SIL es una actividad que requiere la integración del diseño del proceso existente y el análisis de riesgos del proceso. Requiere la implicación de la ingeniería de proceso, gerencia de seguridad del proceso y sistemas de control.

Es importante hacer notar que el concepto de SIL sólo aplica a los Sistemas Instrumentados de Seguridad, los cuales consisten:

- En un sistema formado por uno o varios sensores, que se localizan físicamente en lugares estratégicos, entre estos se encuentran los dispositivos del sistema de detección, alarmas visibles y audibles (detectores de flama, gas tóxico, gas combustible), los dispositivos del sistema automatizado de la red de agua contra incendio y los dispositivos del sistema de operación del proceso (interruptores de alta y baja presión, transmisores inteligentes de presión), los sensores del SIS deben estar separados del BPCS, de lo contrario se puede ver comprometido la integridad del sistema de seguridad. Los sensores deben de estar conectados directamente al sistema lógico, no deben estar conectados a cualquier otro sistema que no sea parte del SIS.
- Uno o varios solucionadores lógicos (eléctricos \ electrónicos o electrónicos programables). El solucionador lógico debe estar diseñado a una falla segura en caso de pérdida de energía o bien cuando falla el sistema o alguno de sus componentes clave. Se debe dimensionar el solucionador lógico de acuerdo a lo solicitado por la empresa y al SIL correspondiente, se debe proporcionar datos de MTTF del solucionador lógico, tasa de falla, el listado de los modos de falla no revelado y la frecuencia con que ocurren fallas identificadas, así como especificar el método utilizado y la fuente de dichos datos.
- Uno o varios elementos finales de control, que son todos los elementos finales que se encuentran instalados para las funciones de respuesta, producto de la filosofía de operación, tales como actuadores automáticos de válvulas de corte, válvulas solenoides, válvulas de seguridad y desfogue, interruptores de arranque y paro de bombas, equipo de servicio, alumbrado, etc. Las válvulas deben seleccionarse de acuerdo a las condiciones específicas del proceso y la función deseada. Otros factores a considerar son: los requerimientos de corte, la experiencia que se tenga con las válvulas, modos de

falla de la válvula, procedimientos operativos que disminuyan su efectividad, estos factores junto con la tasa de falla, el material de fabricación, entre otros deben ser claramente documentados.

Por lo tanto, el concepto de SIL no se aplica a sensores o válvulas por sí mismas, o bien sistemas de control básico de proceso (lazos de control) que no sean independientes y específicos para funciones de seguridad.

Los requerimientos de integridad, es decir, el nivel de integridad de cada función de seguridad del SIS debe ser usado para establecer una arquitectura aceptable del sistema para lograr el nivel de desempeño, seguridad e integridad requerido para que el SIS ejecute las funciones necesarias.

Diseño y arquitectura del SIL

La arquitectura del sistema indica el arreglo e interconexiones de los componentes o módulos del SIS. La selección de esta es una actividad que debe desarrollarse durante el diseño conceptual del sistema. La arquitectura del SIS tiene un impacto directo en su integridad global de seguridad, al influenciarse asimismo en su confiabilidad. La selección de la arquitectura del SIS debe incluir las siguientes etapas:

- Selección de diseño energizado o desenergizado para disparo.
- Selección de redundancias idénticas o diversas para los sensores, solucionadores lógicos y elementos finales del control del SIS.
- Selección de redundancias para las fuentes de potencias y de suministro de energía al SIS.
- Selección de los componentes de la interfase con el operador.
- Selección de las interfases de comunicación entre el SIS y otros subsistemas.

La arquitectura de los sistemas instrumentados de seguridad para cada función instrumentada de seguridad debe ser seleccionada específicamente para determinar el SIL requerido (ejemplo; la arquitectura seleccionada puede ser uno de uno (1oo1), uno de dos (1oo2) ó dos de tres, etc.).

Un SIS puede utilizar arquitecturas (ejemplo; 2oo3 para sensores, 1oo1 para solucionadores lógicos, 1oo2 para elemento final de control) por la razón de que pueden incluir diferentes:

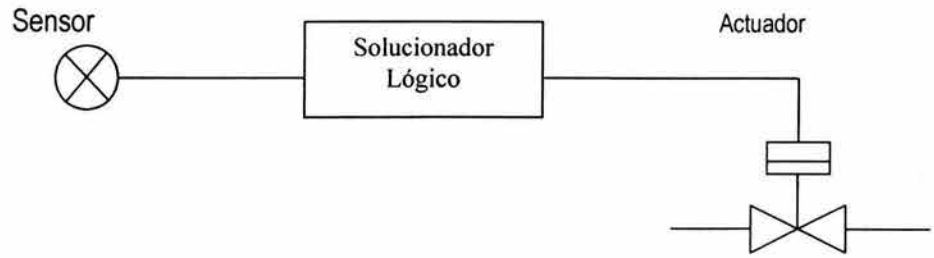
- SILs en el mismo SIS.
- Requerimientos de prueba.
- Confiabilidad de equipo y modo de fallas ; y
- Usuarios de interfases.

El usuario debe determinar las tasas de falla de los componentes del sistema, intervalos de pruebas, redundancias, etc. Y evaluar cada SIS en específico y validar su desempeño.

La arquitectura que puede reunir los requerimientos de desempeño del SIL incluye:

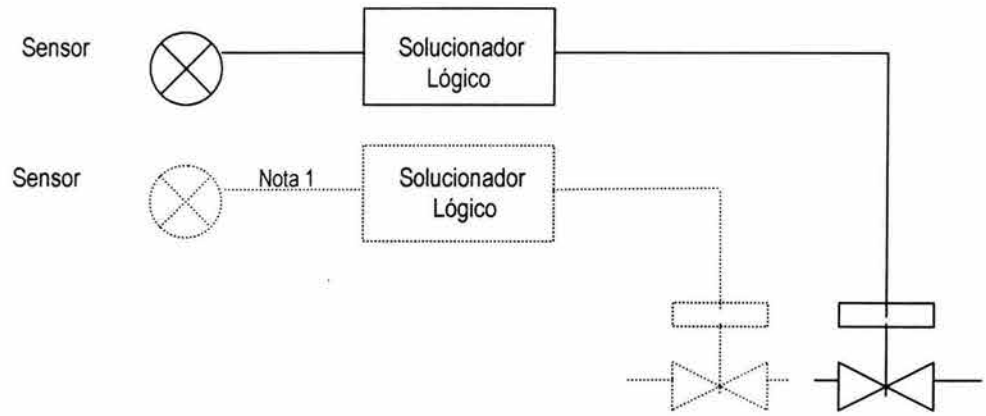
SIL 1.- una arquitectura 1oo1 (figura 2.3) con un sensor simple, un solucionador lógico simple, un elemento final de control.

Figura 2.3 Arquitectura SIL 1[1]

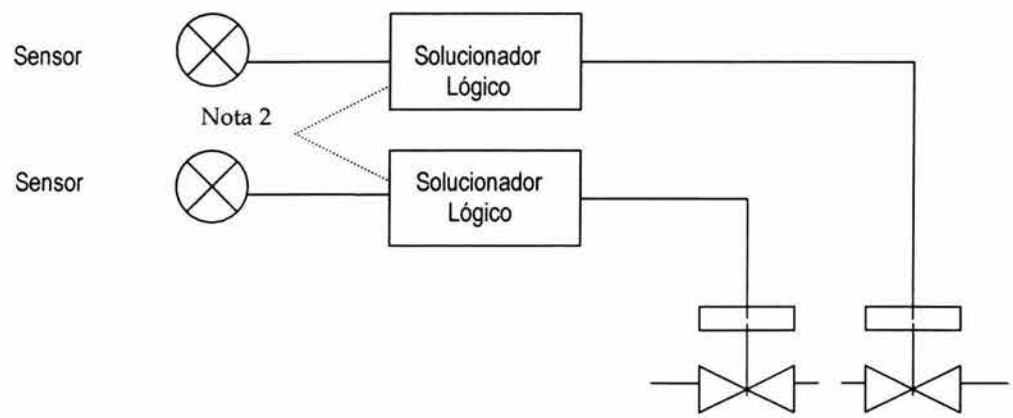


SIL 2.- demanda más diagnósticos generalmente incluye redundancias del solucionador lógico y sensores (figura 2.4), con redundancias del elemento final de control.

Figura 2.4 Arquitectura SIL 2(1)



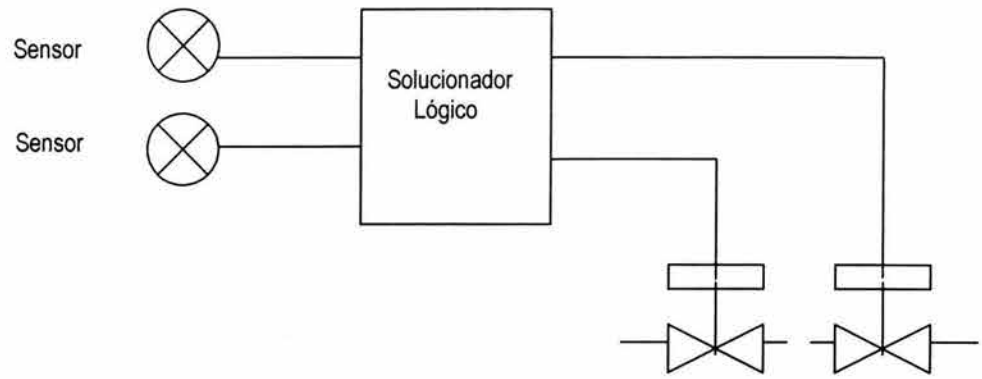
Nota 1: Los sensores, solucionadores lógicos y/o elementos finales pueden ser redundantes como requisitos disponibles.



Nota 2: La ejecución de 2 idénticos SIS de SIL 1 pueden no ser igual que un SIS de SIL 3.

SIL 3.- Dos distintos y diversos arreglos 1oo1, cada uno con sus propios sensores, solucionadores lógicos (figura 2.5), y elemento final de control. El arreglo1oo1 será conectado en un esquema 1oo2. La redundancia, separaciones diversas y diagnósticos exhaustivos son considerados como aspectos significativos de un SIL 3.

Figura 2.5 Arquitectura SIL 3[1]



Solucionador lógico requeridos para encontrar el SIL

El usuario debe determinar las tasas de falla de los componentes del sistema, intervalos de pruebas, redundancias, etc. y evaluar cada SIS en específico y validar su desempeño.

2.7 ANTECEDENTES QUE JUSTIFICAN EL DESARROLLO DE UNA METODOLOGÍA CUANTITATIVA SIMPLIFICADA [1].

En 1996 se aprobó la norma ISA S84.01 "Aplicaciones de Sistemas Instrumentados de Seguridad para las Industrias de Proceso" [1]. Esta norma identifica todos los pasos del ciclo de vida de los Sistemas Instrumentados de Seguridad (SIS) pero no define los métodos para realizar algunos de los pasos, ya que su objetivo únicamente es definir los requerimientos de los Sistemas Instrumentados de Seguridad, los pasos del ciclo de vida que no se definen se mencionan a continuación:

1. Ejecución del diseño conceptual del proceso, incluyendo la filosofía de operación, el equipo de proceso y el sistema básico de control del proceso, se toma también en consideración las condiciones ambientales del lugar (está fuera del alcance de la norma).
2. Análisis de peligros y evaluación de riesgos del proceso, este paso está comprometido con la identificación de los eventos peligrosos para un proceso y evaluar el nivel de riesgo involucrado. (está fuera del alcance de la norma).
3. Asignación de capas de protección NO-SIS, una vez que los peligros y riesgos han sido identificados, se utiliza la tecnología apropiada (incluye la modificación de equipo y procesos) para eliminar el peligro, mitigar sus consecuencias o reducir la probabilidad de el evento riesgoso. (está fuera del alcance de la norma).
4. En seguida una evaluación es hecha para determinar si un número adecuado de capas de protecciones NO-SIS son requeridas. Lo deseable es proporcionar un número apropiado de capas de protección NO-SIS, tal que las capas de protección SIS no sean requeridas. (está fuera del alcance de la norma).
5. Si un SIS es requerido, la siguiente etapa es establecer los requerimientos para el SIS, definiéndolo con un nivel de integridad de la seguridad (SIL) objetivo. (está fuera del alcance de la norma).

Resumiendo en el ciclo de vida, la norma ISA S84.01 señala que antes de definir el Nivel de Integridad de la Seguridad (SIL) de un SIS se debe realizar un análisis de riesgos, utilizar capas

de protección que no sean SIS para prevenir los peligros identificados o reducir los riesgos, para finalmente determinar si es necesario utilizar un SIS y definir el SIL requerido.

CAPÍTULO 3.

DESCRIPCIÓN DE LA PLANTA REFORMADORA DE NAFTA PESADA

DESCRIPCIÓN DE LA PLANTA REFORMADORA DE NAFTA PESADA NO. 2 (U-500). [12] [15] [18]

3.1. Generalidades

La planta Reformadora de Naftas No. 2 (U-500), se encuentra ubicada en el Área No. 5 de la Refinería "Gral. Lázaro Cárdenas "de Minatitlán Veracruz.

La ingeniería básica de la planta Reformadora la desarrolló la compañía Universal Oil Products (UOP) y la ingeniería de detalle y construcción la elaboró el Instituto Mexicano del Petróleo (IMP).

3.2. Descripción del proceso.

La planta realiza un proceso de reformación catalítica, que emplea un catalizador selectivo para convertir, en presencia de hidrógeno, naftas o gasolinas de cadena abierta, en componentes de alto octano.

En esta unidad de proceso se emplean una serie de cámaras de reacción catalítica que utilizan camas móviles (que pueden ser de lecho fijo) de catalizador, una sección de estabilización y los circuitos de intercambio de calor para aprovechar el calor de los productos de la reacción. Se usan calentadores para completar los requerimientos adicionales de calor, para regenerar el catalizador gastado parcialmente gastado de los reactores, puede operar en combinación con esta planta, una unidad de regeneración de catalizador.

En la sección de reacción la carga se mezcla con una corriente de gas de recirculación rico en hidrógeno, se calienta en los cambiadores en los calentadores y se carga a los reactores, en los cuales se mejora el número de octano de la nafta o gasolina.

La unidad tiene calentadores entre cada uno de los reactores para suministrar el calor que necesitan las reacciones. Después del intercambio de calor el efluente que proviene del último reactor se enfría y entra al separador de baja presión donde se separa la corriente líquida de la corriente gaseosa rica en hidrógeno. La corriente gaseosa después de pasar a través del compresor de gas de recirculación, se combina con el líquido bombeado desde el separador de

baja presión. Esta corriente combinada de gas y de hidrocarburos se enfría antes de entrar al separador de productos. En el separador de productos el gas rico en hidrógeno se separa de los hidrocarburos condensados (líquidos).

La mayor parte de la corriente del gas se recircula a los reactores con la extracción de una pequeña corriente de gas para mantener la presión del sistema. La corriente líquida sirve de carga al estabilizador. La alimentación a la Unidad se pretrata en una sección de secado de nafta. Aún cuando los venenos del catalizador se van a tratar se debe mencionar que el ácido sulfhídrico, oxígeno, agua o amoníaco en grandes cantidades no son deseables. También las sales metálicas ó sólidos disueltos del tipo cáusticos pueden ser dañinos. Si la carga se encuentra dentro de la especificación en su intervalo de ebullición y contaminantes no se necesita ninguna otra preparación especial.

a) Química del proceso.

El reformado catalítico es una serie de reacciones que tienen como fin, aumentar el número de octanos en la gasolina, siendo estas reacciones del tipo de "deshidrociclización". En el reformado catalítico, el cambio en el punto de ebullición de los hidrocarburos que sufren la reacción de reformación es pequeño, ya que las moléculas no se craquean, sino que su estructura se reordena para formar compuestos aromáticos de mayor octanaje. Como se ve, el reformado catalítico aumenta principalmente, el octanaje de la gasolina más que su rendimiento. Las materias primas características de los reformadores catalíticos son las gasolinas directas pesadas y las naftas. Estas se componen de cuatro grupos de hidrocarburos:

- Parafinas.
- Olefinas.
- Naftenos.
- Aromáticos.

La carga de alimentación debe estar hidrotratada para bajar el contenido de azufre y nitrógeno a menos de 0.5 ppm, saturar todas las olefinas y remover los metales, los halógenos y los

compuestos oxigenados. El intervalo de ebullición de las naftas tiene una temperatura final de ebullición (TFE) mínimo de 77°C (170°F) y un punto final máximo de 205°C (400°F). Mientras, más alto sea el TFE, sin sobrepasar los 205 °C, se obtendrá un reformado con mayor número de octano.

Las parafinas y los naftenos experimentan dos tipos de reacciones cuando se convierten en componentes de mayor octanaje: deshidrociclización e isomerización. La facilidad y la probabilidad de ambas reacciones se lleven a cabo aumenta con el número de átomos de carbono en las moléculas y es debido a esta razón que solo se utilicen gasolinas pesadas como alimento al reformador ya que la gasolina ligera se compone en mayor proporción de parafinas de bajo peso molecular que tienden a romperse en butano y otras fracciones más ligeras y no resulta económico procesar esta corriente en un reformador catalítico. Los hidrocarburos mas pesados que la gasolina directa pesada son craqueados con hidrógeno y dan lugar a excesivos depósitos de carbón sobre el catalizador.

b) Reacciones.

Como en cualquier serie de reacciones químicas complejas, existen reacciones que dan lugar a productos indeseables además de los esperados. Las condiciones de reacción deben escogerse de modo que favorezcan las reacciones deseables e inhiban las indeseables. Las reacciones deseables en un reformador catalítico conducen a la formación de aromáticos o isoparafinas, tal como se ve:

- Las parafinas se isomerizan y en cierto grado se convierten en naftenos y los naftenos se convierten en aromáticos.
- Las olefinas se saturan para formar parafinas, que luego reaccionan.
- Los naftenos se convierten en aromáticos.
- Los aromáticos permanecen sin cambio.

Las reacciones que conducen a la formación de productos indeseables incluyen:

- La desalquilación de cadenas laterales sobre naftenos y aromáticos para formar butanos y parafinas más ligeras.
- Craqueo de parafinas y naftenos para formar butano y parafinas más ligeras.

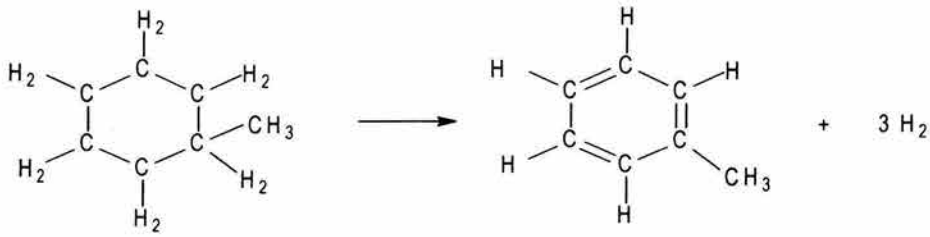
Las cuatro principales reacciones que ocurren durante el reformado son:

- Deshidrogenación de naftenos a compuestos aromáticos.
- Deshidrociclización de parafinas a compuestos aromáticos.
- Isomerización.
- Craqueo con hidrógeno.

c) Reacciones de deshidrogenación.

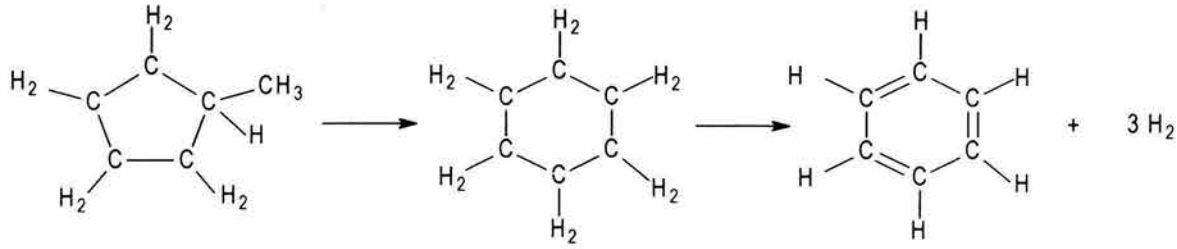
Las reacciones de deshidrogenación son altamente endotérmicas y dan lugar a un descenso en la temperatura a medida que la reacción se lleva a cabo. Además, las reacciones de deshidrogenación poseen velocidades de reacción altas, lo que hace preciso el uso de intercambiadores de calor entre los lechos catalíticos para mantener la corriente de hidrocarburos a temperaturas altas para que las reacciones tengan lugar a velocidades adecuadas. Las principales reacciones de deshidrogenación son:

- Deshidrogenación de alquilciclohexanos a aromáticos.



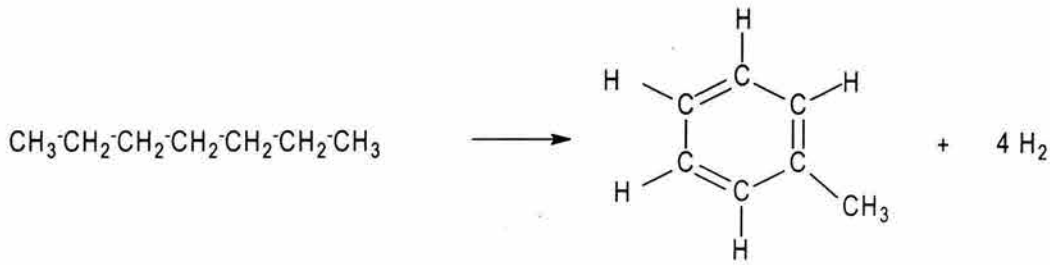
Metilciclohexano Tolueno

- Deshidroisomerización de alquilciclopentanos a aromáticos.



Metilciclopentano Ciclohexano Benceno

- Deshidrociclización de parafinas a aromáticos.



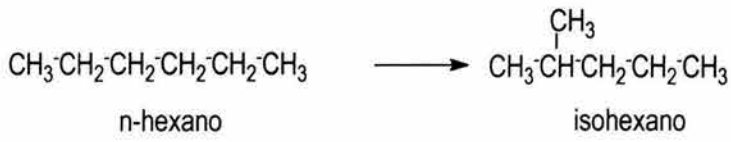
n-heptano Tolueno

La deshidrogenación de los derivados del ciclohexano es una reacción mucho más rápida que cualquiera de las reacciones de deshidroisomerización de alquilciclopentanos o de deshidrociclización de parafinas. Sin embargo, las tres reacciones son necesarias para obtener una concentración alta de compuestos aromáticos, necesaria en el producto final para lograr un alto octanaje.

d) Reacciones de isomerización.

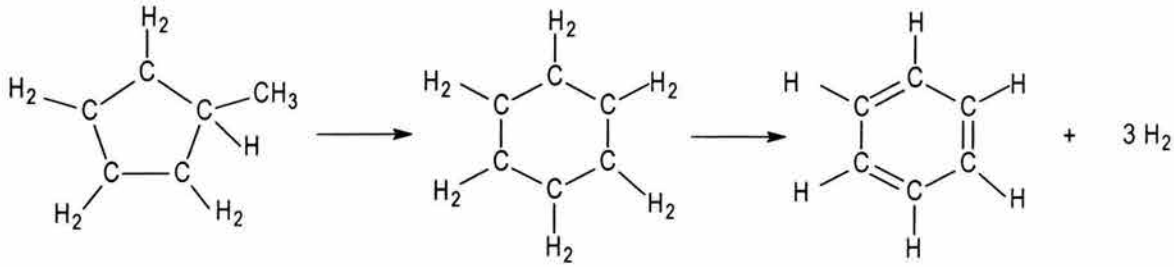
La isomerización de parafinas y ciclopentanos normalmente, da lugar a productos de más bajo octanaje que el obtenido con su conversión a compuestos aromáticos. Sin embargo, hay un aumento sustancial sobre el de los compuestos no isomerizados. Son reacciones muy rápidas y con pequeños efectos caloríficos.

- Isomerización de parafinas normales a isoparafinas.



n-hexano isohexano

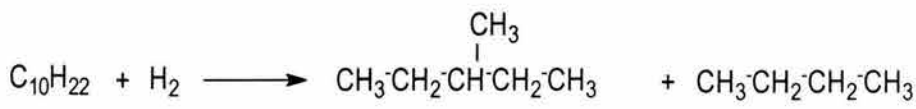
- Isomerización de alquilciclopentanos a ciclohexanos, más su consecuente conversión a benceno.



Metilciclopentano Ciclohexano Benceno

e) Reacciones de craqueo con hidrógeno.

Las reacciones de craqueo con hidrógeno son exotérmicas y dan lugar a la producción de hidrocarburos más ligeros y productos gaseosos. Son reacciones lentas y por lo tanto la mayor parte del craqueo con hidrógeno tiene lugar en la última sección del reactor. Las principales reacciones de craqueo con hidrógeno implican el rompimiento y la saturación de las parafinas.



n-decano i-hexano n-butano

La concentración de parafinas en el material de carga determina la extensión de la reacción de craqueo con hidrógeno pero la fracción relativa de isómeros producidos en cualquier grupo del mismo peso molecular es independiente del material de carga.

f) Catalizadores de reformado [15]

Los procesos de reformado se clasifican en continuos, cíclicos y semiregeneradores, dependiendo de la frecuencia de regeneración del catalizador. El proceso consta de lo siguiente: la carga tratada previamente y el hidrógeno reciclado se calientan de 496 °C a 524 °C antes de entrar al primer reactor. En éste, la reacción principal es la deshidrogenación de naftenos a compuestos aromáticos y dado que ésta reacción es muy endotérmica, la temperatura desciende de manera considerable. Para mantener la velocidad de reacción, los vapores se vuelven a calentar antes de pasar por el catalizador del segundo reactor. A medida que la carga atraviesa los reactores, las velocidades de reacción descienden, los reactores resultan mayores y el recalentamiento necesario resulta ser menor. De manera general para proporcionar el grado deseado de reacción se necesitan tres reactores, y sus necesarios calentadores de carga a fuego directo antes de cada reactor para hacer alcanzar a la carga la temperatura de reacción.

La carga procedente del último reactor se enfría y los vapores se condensan dando lugar a productos líquidos. Los gases ricos en hidrógeno se separan de la fase líquida y el líquido procedente del separador se envía a una columna de fraccionamiento para que sea debutanizado o depentanizado. La corriente de gas rica en hidrógeno se divide en una corriente de hidrógeno reciclado y en una producción secundaria de hidrógeno neto que se utiliza en las operaciones de tratamiento con hidrógeno, de hidrogenación o como combustible.

La presión de operación del reformado y la razón hidrógeno–carga son el vínculo entre la obtención de rendimiento máximo, tiempos de operación grandes entre regeneraciones y una operación estable. Normalmente, es necesario operar bajo presiones de 9 a 34 atmósferas, razones de carga de 5 – 8 moles de hidrógeno/mol de hidrocarburo y relaciones de espacio velocidad volumétrica en el área de 2 a 3.

Todos los catalizadores de reformado de uso general, hoy en día contienen platino soportado sobre una base de sílice o de aluminio–sílice. En muchos casos el renio se combina con el platino para formar un catalizador más estable, que permite operar a presiones más bajas. El platino está ideado para utilizarlo en la zona catalítica para las reacciones de hidrogenación y deshidrogenación y la alúmina clorada proporciona una zona ácida para las reacciones de isomerización, ciclización y craqueo con hidrógeno.

La actividad de un catalizador de reformado es función del área, del volumen del poro y del contenido en platino y compuestos con cloros activos. La actividad del catalizador se reduce durante el funcionamiento por los depósitos de coque y las pérdidas de cloruros. La actividad del catalizador se puede restablecer por la oxidación a alta temperatura de carbón que se depósita en su superficie, seguida por una cloración, operación conocida como regeneración.

3.3. Variables del proceso.

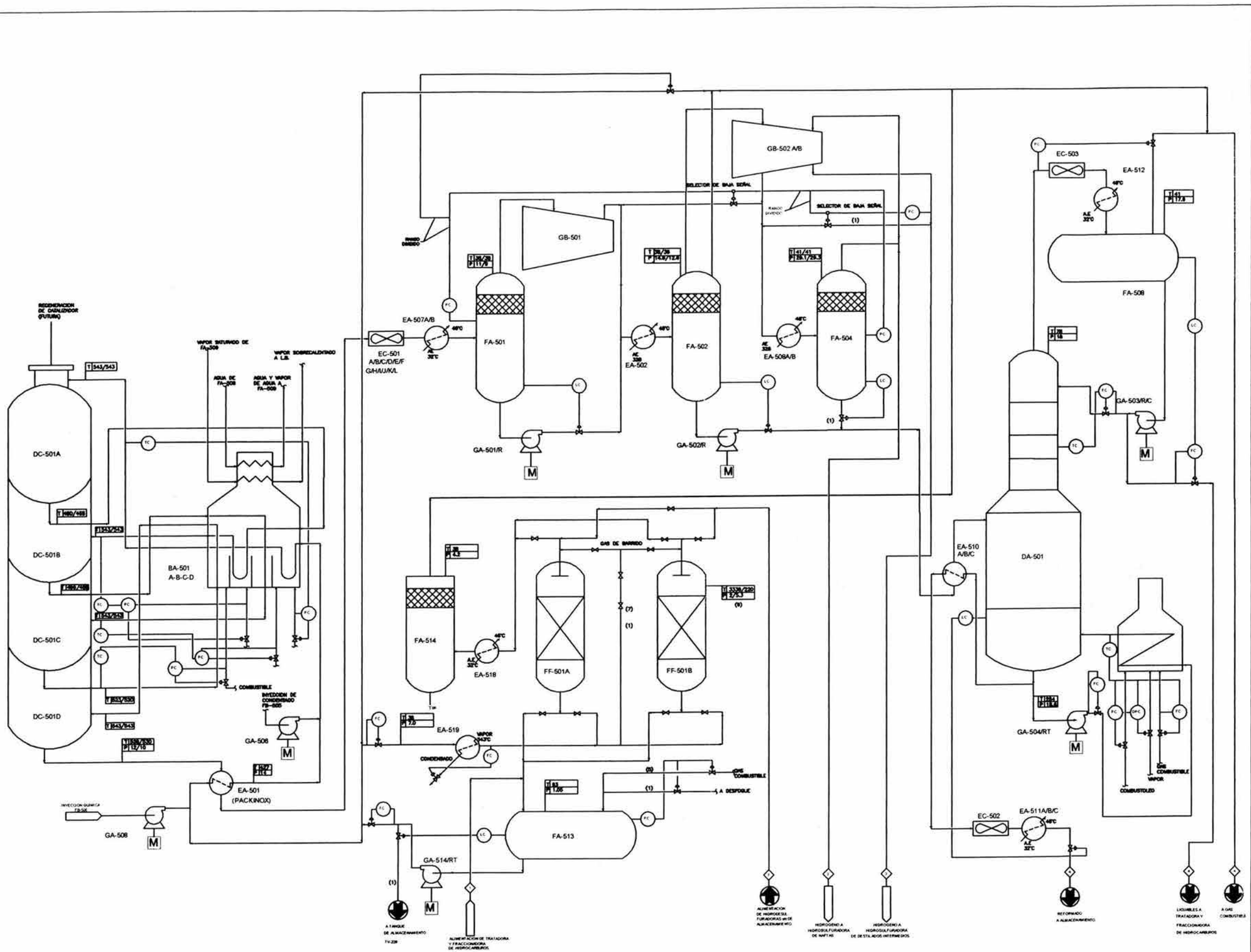
La finalidad de esta sección es explicar el comportamiento las variables de operación del proceso de reformación y sus efectos en la calidad y cantidad de los productos que se van a obtener.

En forma general las principales variables de proceso son:

- **Temperatura de reacción**.- Es una variable importante que influye directamente en la calidad de los productos de reformacion, el catalizador se puede trabajar en un amplio intervalo de operación (470 °C a 520 °C). Al incrementar la temperatura se obtendrá un reformado de mayor índice de octano, por otro lado la velocidad de hidrodesintegración se incrementa linealmente con el aumento de temperatura. Mientras que las velocidades de desintegración y deshidrociclizacion se incrementan logarítmicamente, así mismo mientras mayor sea la temperatura de reacción al catalizador éste desactivara más rápidamente, por el carbón depósitado en él. La temperatura de operación se define como la sumatoria de los valores obtenidos al multiplicar la fracción peso de catalizador de cada reactor por su correspondiente temperatura de entrada. La temperatura de operación se incrementa durante el tiempo de corrida para dar la calidad de producto requerido (índice de octano o producción de aromáticos).
- **Presión**.- Se toma como base un mismo índice de octano del reformado y se observa que al disminuir la presión del sistema se incrementa la producción de reformado a hidrógeno, por lo que se requiere una menor temperatura, pero también aumenta la velocidad de carbonización del catalizador.

- **Espacio velocidad**.- el espacio velocidad es la relación del flujo de nafta procesada entre la cantidad de catalizador empleado. Cuando el flujo de nafta y el catalizador se miden en unidades volumétricas se está obteniendo el valor de LHSV y si se mide en unidades de peso se obtiene el WHSV. El incremento del espacio velocidad disminuye el índice de octano del reformado por ser menor el tiempo de contacto de la carga con el catalizador, lo cual se puede contrarrestar con un incremento de temperatura. El descenso de espacio velocidad favorece la estabilidad del catalizador obteniendo un ciclo de vida más prolongado, siempre y cuando la masa velocidad no sea menor de 400 Lbs/hrpie^2 , respecto a los rendimientos de productos éstos no se afectan considerablemente al variar el espacio velocidad.
- **Relación hidrógeno/hidrocarburo (H_2/HC)**.- se define como las moles de hidrógeno recirculado por mol de naftas que se alimenta al reactor. El hidrógeno es necesario en el proceso de reformacion para mantener la estabilidad del catalizador, la función del hidrógeno es retirada del catalizador y de los productos de la policondensacion, Por lo tanto, al disminuir la relación molar H_2/HC se disminuye la vida útil del catalizador (los valores normales son 5-8 moles H_2 /mol HC).
- **Tipo de carga**.- En forma general las propiedades más importantes que definen el tipo de carga que se va a procesar son: el análisis PONA, la destilación ASTM-D86 y el tipo y concentración de contaminantes, debido a que afectan la operación del catalizador. La severidad del proceso queda definida por el mayor o menor contenido de naftenos en la carga, ya que la operación menos severa será con cargas de alto contenido de éstos.

DFP



LISTA DE EQUIPO

CLAVE	SERVICIO	CARACTERISTICAS
HORNOS		
BA-501 A/D	CALENTADOR DE REFORMACION	86.70MM KCAL/h
BA-502	CALENTADOR DE FONDOS DESBUTANIZADORA	4.08 MM KCAL/h
TORRE		
DA-501	TORRE DESBUTANIZADORA	1370 mm D-I 2130 mm D-I 22710 mm D-I
REACTORES		
DC-501A/D	REACTORES DE REFORMACION CAMBIADORES DE DE CALOR	60.3m3 DE CATALIZADOR
EA-501	PRECALENTADOR DE CARGA	42.06 MM Kcal/h
EA-502	ENFRIADOR DE ALTA PRESION	1.32 MMKcal/h
EA-507	SEGUNDO ENFRIADOR EFLUENTE DEL REACTOR	1.86 MMKcal/h
EA-508A/B	CONDENSADOR DEL INTERFRIDO DEL COMPRESOR GB-502	0.68 MMKcal/h
EA-510A/D	PRECALENTADOR CARGA DESBUTANIZADORA	12.39MMKcal/h
EA-511A/C	SEGUNDO ENFRIADOR EFLUENTE	0.72MMKcal/h
EA-512	SEGUNDO CONDENSADOR DESBUTANIZADORA	
EA-518	ENFRIADOR DE GAS DE REGENERACION	0.139X1.25MMKcal/h
EA-519	CALENTADOR DE GAS DE REGENERACION	0.139X1.25MMKcal/h
EC-501A/L	PRIMER ENFRIADOR EFLUENTE DEL REACTOR	13.30MMKcal/h
EC-502	PRIMER ENFRIADOR FONDOS DESBUTANIZADORA	1.37MMKcal/h
EC-503	PRIMER CONDENSADOR DESBUTANIZADORA	1.48MMKcal/h
RECIPIENTES		
FA-501	SEPARADOR DE BAJA PRESION	3440mmD-S8100mmT-T
FA-502	SEPARADOR DE PRODUCTOS DE REFORMACION	2280mmD-S8100mmT-T
FA-504	TANQUE DE SUCCION SEGUNDA ETAPA COMPRESOR GB-502	915mmD-S2740mmT-T
FA-508	ACUMULADOR DE REFLUJO TORRE DESBUTANIZADORA	1525mmD-S4130mmT-T
FA-513	TANQUE DE CARGA	2743mmD-S5791mmT-T
FA-514	SEPARADOR DE CONDENSADO DE GAS DE REGENERACION	762mmD-S1854mmT-T
DESHIDRATADORES		
FE-501A/B	SECADOR DE MATIZ	1981mmD-S8182mmT-T
BOMBAS		
GA-501/R	BOMBA DEL SEPARADOR DE BAJA PRESION	227 1LPM,ΔP=7.2Kpc
GA-502/R	BOMBA DE ALIMENTACION DESBUTANIZADORA	2338LPM,ΔP=10.3Kpc
GA-503/R/C	BOMBA DE REFLUJO DESBUTANIZADORA	1003LPM,ΔP=4.3Kpc
GA-504/RT	BOMBA DE FONDOS DESBUTANIZADORA	3142LPM,ΔP=6.8Kpc
GA-506	BOMBA DE INYECCION DE CONDENSADO	1.02LPM,ΔP=16.5Kpc
GA-508	BOMBA DE INYECCION QUIMICA	25.8LPM,ΔP=16.5Kpc
GA-514/RT	BOMBA DE CARGA	3633LPM,ΔP=13.6Kpc
COMPRESORES		
GB-501	COMPRESOR DE RECIRCULACION	2263BHP REQUERIDOS
GB-502A/B	COMPRESOR DE HIDROSOLO PRODUCTO	2194BHP REQUERIDOS

Universidad Nacional Autónoma de México (UNAM)
Facultad de Química

TITULO DEL DIBUJO: DIAGRAMA DE FLUJO DE PROCESO UNIDAD REFORMADORA DE NAFTAS 5/1RB AREA 5

NUMERO DE DIBUJO: U-500-008

REVISIONES: REV. 0

CAPÍTULO 4.
METODOLOGÍA

CAPÍTULO 4

METODOLOGÍA

4.1 JUSTIFICACIÓN DE APLICACIÓN DE LA METODOLOGÍA CUANTITATIVA SIMPLIFICADA A LA PLANTA REFORMADORA DE NAFTAS:

La reformación catalítica es diseñada para seguridad máxima de operación de la persona y para protección del catalizador y equipo. Un aspecto del reformado que genera preocupación en la seguridad es la presencia de grandes volúmenes de hidrógeno a altas presiones y Naftas altamente inflamables.

El hidrógeno es un gas flamable. Es incoloro, inodoro, insípido y no tóxico. A presión atmosférica la temperatura de ignición de la mezcla hidrógeno-aire es reportada, tan bajo como 932^{0}F (500^{0}C).el peligro más serio del hidrógeno es en el intervalo de limite de flamabilidad en aire, de 4.1-74 %.

El hidrógeno arde en aire con una flama azul pálida que es aproximadamente invisible a la luz del día. Las fugas de las corrientes que contienen hidrógeno en una unidad reformadora son fugas generadas en las bridas de los intercambiadores o tuberías. Los operadores están concientes de estos peligros y tienen cuidado de los incendios de hidrógeno, especialmente durante el arranque.

Incidentes mayores ocurren en la falla o ruptura de equipo o líneas y la descarga de grandes volúmenes de hidrógeno en la atmósfera. Aunque, los operadores están capacitados para manejar tales emergencias. El procedimiento usual es disparar los quemadores del calentador, parar las bombas de carga del reactor y despresurizar la unidad al sistema de desfogue.

Otras emergencias que no son descargas de hidrógeno a la atmósfera, son la pérdida de aire de instrumento, electricidad, o vapor. Cuando esto ocurre, la circulación de hidrógeno continúa para proteger al catalizador lo más posible.

Debido a las características de los inventarios que se manejan y las condiciones de operación, la planta Reformadora de Naftas, representa un riesgo para Recursos Humanos, Medio Ambiente y la producción.

Por estas razones y además con el propósito de evaluar la confiabilidad de los sistemas instrumentados de seguridad de la planta y en base a lo indicado en la norma ISA S84.01 donde menciona que el método para desarrollar las primeras 5 etapas del ciclo de vida de los SIS está fuera del alcance de ésta norma y que se deja al criterio de las compañías el desarrollo de éstas etapas , es que se propone la siguiente metodología semí-cuantitativa basada en el análisis LOPA (Layers of Protection Analysis) [3], la cual se describe a continuación.

4.2 DESCRIPCIÓN DE LA METODOLOGÍA [3] [5] [6] [14]

Los incidentes ocurren cuando se combina un evento iniciador con la falla de las capas de protección del proceso aplicables, siendo su frecuencia igual a la frecuencia de los eventos iniciales (los cuales presentan demandas a los sistemas de protección) y la probabilidad de que éstos fallen simultáneamente ante estas demandas. Dependiendo de la gravedad de las consecuencias potenciales del incidente se establece un criterio de aceptabilidad de riesgos en base a una frecuencia máxima aceptable.

Al evaluar semí-cuantitativamente la frecuencia de las demandas y la probabilidad de falla bajo demanda de las capas de protección, se puede determinar si las protecciones son suficientes de acuerdo a los criterios establecidos. Si las protecciones para un escenario de riesgo no son suficientes, se deben evaluar capas de protección adicionales entre las cuales se puede utilizar un Sistema Instrumentado de Seguridad (SIS), en este caso el método permite determinar fácilmente el SIL objetivo cuyo propósito específico es medir la reducción de riesgo requerido, es decir, la diferencia entre los niveles de riesgo existente y tolerable.

4.3 ETAPAS DE LA METODOLOGÍA:

- Definir los criterios de aceptabilidad de riesgos.
- Identificar los eventos peligrosos y evaluar su gravedad.
- Identificar los eventos iniciales y calcular la frecuencia.
- Identificar las capas de protección independientes aplicables y calcular su efectividad.
- Determinar la frecuencia esperada del evento peligroso considerando las capas de protección independientes.
- Determinar la necesidad de capas adicionales de protección y determinar el SIL requerido si un SIS es recomendado.

4.3.1 Definir los criterios de aceptabilidad de riesgos

¿Qué nivel de riesgo es aceptable?

Cada compañía puede contestar en forma diferente esta pregunta. Definir los criterios de aceptación de riesgos propuesto en la metodología semí cuantitativa de este proyecto no sólo es una de las etapas más difíciles del método sino una de las más importantes. Ya que estos criterios proporcionan una base consistente para determinar el nivel (y posiblemente el tipo) de protecciones requeridas para prevenir o mitigar un evento riesgoso. Al proponer los criterios de aceptabilidad de riesgos se debe contemplar que se tenga un equilibrio entre los costos de la producción y el costo (económico, social, imagen de la compañía, etc.) de los accidentes. Si estos criterios son muy severos podrían en un momento dado resultar incosteables y con protecciones innecesarias, es decir la compañía en este caso no tendría accidentes pero los gastos en control de riesgos serian excesivos. Se puede tener el caso contrario, donde los criterios sean poco rigurosos, aquí se estaría obligado a invertir pocos recursos económicos en el control de riesgos pero a expensas de los accidentes que seguro ocurrirían, la compañía estará expuesta a riesgos sustanciales que pueda dejar devastadoras pérdidas.

Varios métodos son usados para definir los criterios de aceptación de riesgos en función de la frecuencia con que la compañía quiere o puede permitir tener un accidente mayor (un fallecimiento) en sus instalaciones.

Las compañías pueden usar criterios establecidos por agencias gubernamentales (el cuál es frecuentemente inconsistente) o pueden comparar los riesgos de procesos de algunos riesgos comunes encontrados. Algunas compañías adoptan otros criterios cuando tales criterios son confiables. **Sin embargo, en muchos casos las compañías desarrollan sus propios criterios.**

Algunos de los factores a considerar cuando se definen criterios propios deben incluir:

- Los peligros en el personal de planta.
- Impacto a la comunidad e imagen publica.
- Daños al medio ambiente.
- Los daños a propiedades y sus pérdidas económicas.

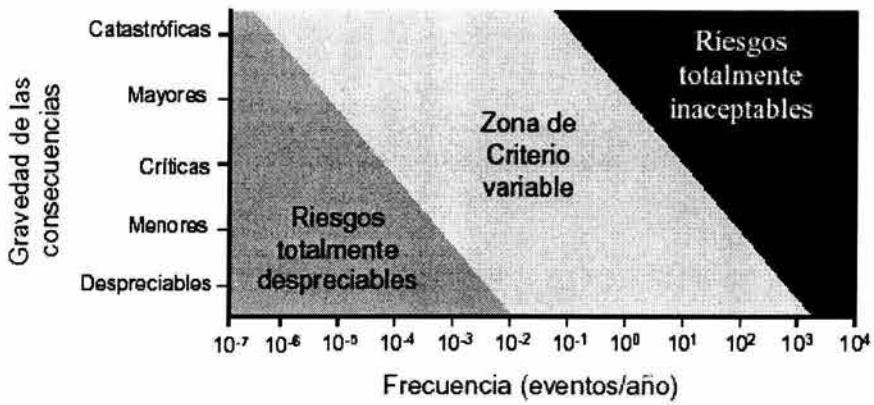
El riesgo puede ser definido como la combinación de frecuencia de ocurrencia de un evento y la severidad de consecuencias. Muchas compañías representan los criterios de aceptación de riesgos con una matriz (ó familia de matrices) que correlaciona la severidad del evento peligroso a una frecuencia aceptable de ocurrencia.

La metodología en este proyecto involucra cambiar una frecuencia de aceptación máxima de ocurrencia con respecto a una severidad de consecuencias especifica a una referencia que llamaremos frecuencia umbral (frecuencia máxima permitida para cada nivel de severidad de consecuencias de un escenario de riesgo). Donde la frecuencia umbral (F_t) para cada categoría de consecuencias correlaciona directamente los criterios de aceptación de la compañía.

De acuerdo a datos publicados [3][5][6] sobre criterios de aceptabilidad de riesgos en instalaciones industriales (figura 3.0) y de información disponible de PEMEX, se pueden obtener 3 zonas en un diagrama frecuencia – gravedad:

- **Riesgos totalmente inaceptables**: Todos los criterios concuerdan en que en esta zona las acciones para reducir o mitigar los riesgos son obligatorios y urgentes.
- **Riesgos totalmente despreciables**: Todos los criterios concuerdan en que en esta zona no se requieren o no es conveniente realizar acciones para reducir o mitigar los riesgos.
- **Zona de criterio variable**: En esta zona los diversos criterios difieren en cuanto hasta dónde es obligatorio o conveniente realizar acciones para reducir o mitigar los riesgos y la urgencia con que éstas acciones deben ser realizadas. Esta es la zona en la que cada compañía deberá elegir qué tanto es práctico reducir o mitigar los riesgos.

Figura 4.0. Representación de las criterios de aceptabilidad de riesgos en un diagrama frecuencia – gravedad. [3][5][6]



Los valores límites de estas zonas, así como el criterio utilizado en este análisis, se muestran en la tabla (3.0):

Tabla 4.0 Frecuencias límites de la zona de criterio variable para cada categoría de consecuencias y frecuencias máxima aceptable utilizada.[25][3][5][6]

Gravedad de las consecuencias	Frecuencia límite inferior (eventos/año)	Frecuencia límite superior (eventos/año)	Frecuencia máxima aceptable (criterio utilizado en el análisis) (eventos/año)
Categoría 5 Catastrófico	1/1,000,000	1/10	1/30,000
Categoría 4 Mayor	1/100,000	1	1/3000
Categoría 3 Crítico	1/10,000	10	1/300
Categoría 2 Menor	1/1,000	100	1/30
Categoría 1 Despreciable	1/100	1000	1/3

Para simplificar el análisis, se ha dado un valor a cada intervalo de frecuencias de acuerdo al orden de magnitud (exponente) en incrementos de 0.5 órdenes de magnitud.

En la siguiente tabla se muestran estos valores:

Tabla 4.1. Valores de frecuencia para eventos con probabilidades de ocurrir en la vida útil de una planta de proceso. [25][3][5][6]

Intervalo de frecuencias (eventos /año)	Valor de frecuencia (F)	Tiempo observado entre eventos (años)	Número de eventos esperados en 30 años	Implicación de utilizar este valor como criterio de aceptabilidad
> 1000	11	<0.001 (<9 horas)	3,000 a 10,000	Seguramente ocurrirá un evento cada 4 días o menos
300 a 1000	10.5	0.001 (9 horas) a 0.003 (1 día)	1,000 a 3,000	Seguramente ocurrirá un evento cada 4 a 12 días
100 a 300	10	0.003 (1 día) a 0.01 (4 días)	300 a 1,000	Seguramente ocurrirá un evento cada 12 a 37 días
30 a 100	9.5	0.01 (4 días) a 0.03 (12 días)	100 a 300	Seguramente ocurrirá un evento cada 37 días a 4 meses
10 a 30	9	0.03 (12 días) a 0.1 (37 días)	30 a 100	Seguramente ocurrirá un evento cada 4 meses a 1 año
3 a 10	8.5	0.1 (37 días) a 0.3 (4 meses)	10 a 30	Seguramente ocurrirá un evento cada 1 a 3 años
1 a 3	8	0.3 (4 meses) a 1	3 a 10	Seguramente ocurrirá un evento cada 3 a 10 años
0.3 a 1	7.5	1 a 3	1 a 3	Seguramente ocurrirá un evento en 10 a 30 años

intervalo de frecuencias (eventos /año)	Valor de frecuencia (F)	Tiempo observado entre eventos (años)	Probabilidad de un evento en 30 años	Implicación de utilizar este valor como criterio de aceptabilidad
0.1 a 0.3	7	3 a 10	95% a 100%	Muy alta probabilidad de ocurrir un evento en 30 años
0.03 a 0.1	6.5	10 a 30	63% a 95% (>2/3)	Alta probabilidad de ocurrir un evento en 30 años
0.01 a 0.03	6	30 a 100	26% a 63% (1/4 a 2/3)	Probabilidad media de ocurrir un evento en 30 años
$3x10^{-3}$ a $1x10^{-2}$	5.5	100 a 300	10% a 26% (1/4 a 1/10)	Baja probabilidad de ocurrir un evento en 30 años
$1x10^{-3}$ a $3x10^{-3}$	5	300 a 1000	3% a 10%	< a 1 oportunidad en 10 de ocurrir un evento en 30 años
$3x10^{-4}$ a $1x10^{-3}$	4.5	1,000 a 3,000	1% a 3%	
$1x10^{-4}$ a $3x10^{-4}$	4	3,000 a 10,000	0.3% a 1%	< a 1 oportunidad en 100 de ocurrir un evento en 30 años
$3x10^{-5}$ a $1x10^{-4}$	3.5	10,000 a 30,000	0.1% a 0.3%	
$1x10^{-5}$ a $3x10^{-5}$	3	30,000 a 100,000	0.03% a 0.1%	< a 1 oportunidad en 1000 de ocurrir un evento en 30 años
$3x10^{-6}$ a $1x10^{-5}$	2.5	100,000 a 300,000	0.03% a 0.01%	
$1x10^{-6}$ a $3x10^{-6}$	2	300,000 a 1,000,000	0.01% a 0.003%	< a 1 oportunidad en 10,000 de ocurrir un evento en 30 años
$3x10^{-7}$ a $1x10^{-6}$	1.5	1,000,000 a 3,000,000	0.003% a 0.001%	
$< 3x10^{-7}$	1	> 3,000,000	Menor a 0.001%	< a 1 oportunidad en 100,000 de ocurrir un evento en 30 años

La razón de dividir las frecuencias en dos partes es debido a que la probabilidad de al menos un evento en 30 años (aproximadamente la vida útil de una planta de proceso) es 100% para

frecuencias mayores 0.3 eventos / año, es decir, es prácticamente seguro que ocurrirán uno o más eventos en este período. En frecuencias menores a 0.3 se manejan probabilidades menores al 100% de un evento en 30 años. Para verificar esto basta con saber que:

$$P = 1 - e^{-f \cdot T} \qquad (12)$$

Donde:

P = Probabilidad de un evento

f = Frecuencia observada

T = Tiempo

En base a estas tablas se asigna un valor de frecuencia umbral (F_t) para cada categoría de consecuencias:

Tabla 4.2. Valores de frecuencia umbral para cada categoría de consecuencias. [25][3][5][6]

Gravedad de las consecuencias	Frecuencia máxima aceptable (eventos/año)	Valor de frecuencia umbral (Ft)
Categoría 5 - Catastrófico	1/30,000	3
Categoría 4 - Mayor	1/3000	4
Categoría 3 - Crítico	1/300	5
Categoría 2 - Menor	1/30	6
Categoría 1 - Despreciable	1/3	7

4.3.2 Identificar los eventos peligrosos y evaluar su gravedad

A partir de un estudio HAZOP se seleccionan los escenarios de mayor riesgo potencial para ser considerado por esta metodología. El riesgo potencial es el riesgo de un escenario, sin considerar las capas de protección existentes, evaluado cualitativamente mediante una matriz de riesgos.

De acuerdo con la información disponible en las consecuencias señaladas en el estudio HAZOP se debe clasificar la gravedad de las consecuencias para poder asignar una frecuencia umbral al escenario estudiado.

La siguiente tabla muestra la aplicación de la descripción de consecuencias potenciales de cada categoría basada en las guías semí-cuantitativas de las tablas 2.2, 2.3, 2.4, 2.5 para determinar la gravedad de un escenario como se muestra en el capitulo 3.

Descripción de los efectos potenciales de acuerdo a la categoría de consecuencias:

Tabla 4.3. Descripción de los efectos potenciales de acuerdo a las consecuencias. (3) (25)

Gravedad	Receptor	Descripción de los efectos potenciales
Categoría 5 Catastrófico	Personal	Muerte o lesiones que producen discapacidad permanente
	Comunidad	Uno o más heridos graves
	Medio ambiente	Descargas significativas con impacto severo hacia el exterior de las instalaciones y con probabilidades de causar efectos a la salud inmediatos o de largo plazo
	Producción	Destrucción mayor o total de una o varias áreas de proceso con un costo estimado mayor a 10 millones de dólares o pérdidas significativas de producción
Categoría 4 Mayor	Personal	Uno o más heridos graves
	Comunidad	Uno o más heridos leves
	Medio ambiente	Descargas significativas con impacto severo al medio ambiente.
	Producción	Daño mayor a una o varias áreas de proceso con un costo estimado mayor a 1 millón de dólares o algo de pérdida de producción
Categoría 3 Crítico	Personal	Lesiones leves con posible suspensión de labores
	Comunidad	Quejas de la población cercana por olores o ruido
	Medio ambiente	Notificación de o a las autoridades ambientales o violación de permisos como resultado de emisiones
	Producción	Varios equipos dañados con un costo estimado mayor a 100,000 dólares y con pérdidas mínimas de producción
Categoría 2 Menor	Personal	Lesiones leves sin suspensión de labores
	Comunidad	Sin daños, peligros o molestias en la población
	Medio ambiente	Evento intrascendente, sin notificaciones o violación de permisos
	Producción	Daños menores a algún equipo, con un costo menor de 100,000 dólares y sin pérdida de producción
Categoría 1 Despreciable	Personal	Sin lesiones o suspensión de labores
	Comunidad	Sin daños, peligros o molestias a la población
	Medio ambiente	Evento intrascendente, sin notificaciones o violación de permisos.
	Producción	Daños menores a algún equipo, con un costo menor de 10,000 dólares y sin pérdida de producción

4.3.3 Identificación de los eventos iniciales y determinación de su frecuencia.

Los eventos iniciales de un escenario están señalados en las causas de un escenario de un análisis HAZOP. Su frecuencia se puede determinar a partir de la frecuencia cualitativa, sin considerar protecciones, utilizada en la matriz de evaluación de riesgos. Este dato se debe cotejar con los intervalos presentados en la literatura para validarlo. Una buena fuente de información son datos de confiabilidad de equipos de proceso publicados por el CCPS del AICHE (3) (7).

Al igual que con la frecuencia umbral se asigna un valor relacionado con el orden de magnitud al cual se llamará frecuencia del evento inicial (F_i) de acuerdo a la siguiente tabla.

Tabla 4.4 Valores de frecuencia para el evento inicial. (25)(5)(7)

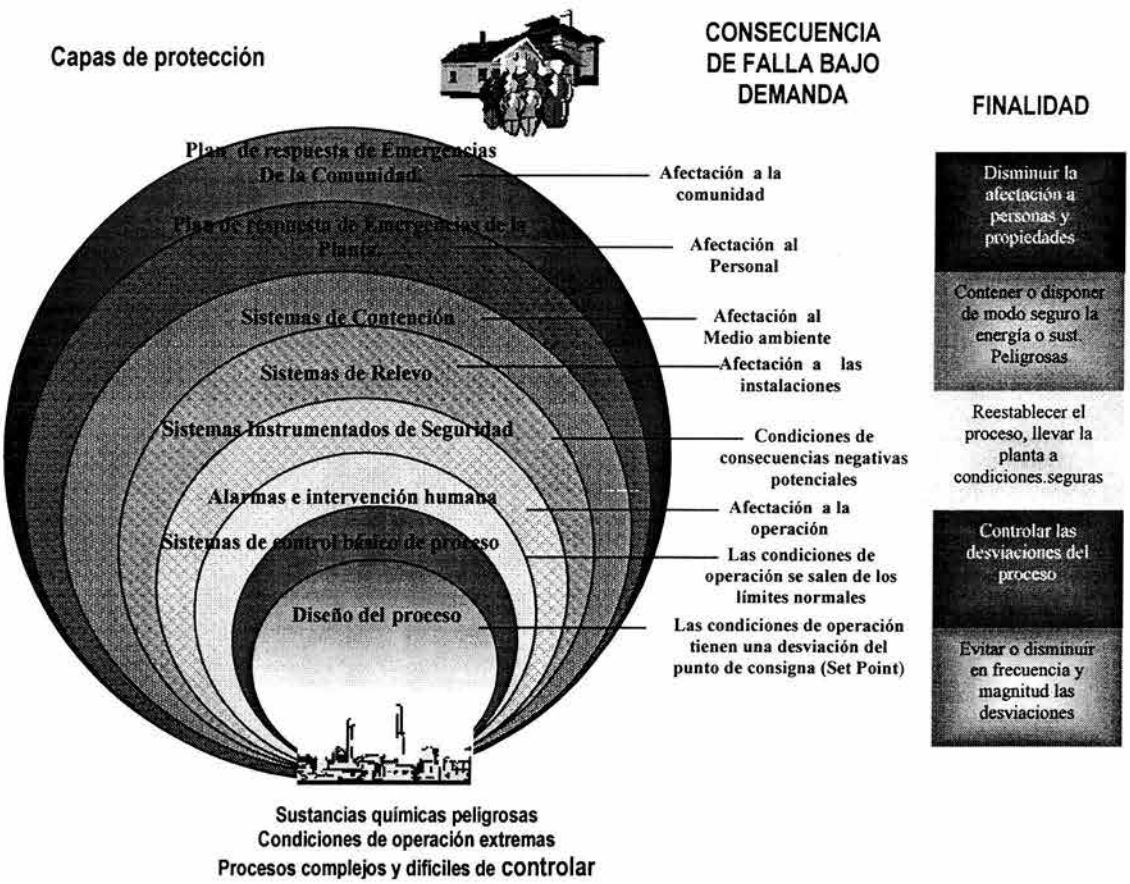
Valor de frecuencia del evento inicial (F_i)	intervalo de frecuencias (eventos/año)	Tiempo observado entre eventos	Guía cualitativa
11	>1000	Menos de 9 horas	Continuo
10.5	300 a 1000	Entre 9 y 29 horas	Varias veces por día
10	100 a 300	Entre 29 horas y 4 días	Diario
9.5	30 a 100	Entre 4 y 12 días	Semanal
9	10 a 30	Entre 12 y 37 días	Mensual
8.5	3 a 10	Entre 37 días y 4 meses	Muy frecuente
8	1 a 3	Entre 4 meses y 1 año	Frecuente
7.5	0.3 a 1	Entre 1 y 3 años	Ocasional
7	0.1 a 0.3	Entre 3 y 10 años	Raro (ya ocurrió hace tiempo)
6.5	0.03 a 0.1	Entre 10 y 30 años	Posible (no se tienen registros pero puede ocurrir)

4.3.4 Identificar las capas de protección independientes aplicables al escenario y evaluar su efectividad.

Identificación de capas de protección independientes (figura 3.1):

El método LOPA define las capas de protección independientes (CPI) como dispositivos, sistemas o acciones capaces de prevenir el que un escenario continúe hacia consecuencias indeseables independientemente del evento inicial y de la acción o falla (sin fallas de causa común) de cualquier otra capa de protección asociada con el escenario. Como se explican en el capitulo 2, sección 2.4.7.

Figura 4.1 Capas de protección de un proceso, finalidad y consecuencias de fallas bajo demanda [3]



Para efectos de esta metodología sólo se considerarán como capas de protección independientes las siguientes:

1. Alarmas e intervención humana
2. Sistemas instrumentados de seguridad
3. Sistemas de relevo
4. Sistemas de contención

Las fallas en las capas de diseño del proceso y sistemas de control básico de proceso por lo regular son la causa o evento inicial considerado en cada escenario por lo cual estas capas quedan representadas dentro del valor de la frecuencia del evento inicial. Por otra parte, las capas de programas de respuesta a emergencias no se consideran en esta metodología, pues el objetivo es no llegar a necesitar estas capas de protección.

Evaluación de la efectividad de cada capa (tabla 3.5):

La evaluación de la efectividad de cada una de las capas de protección independiente se lleva a cabo mediante la calificación de un valor o índice relacionado con el orden de magnitud de la Probabilidad de Falla en Demanda (S_{PFD}) de las mismas capas como se detalla en la siguiente tabla:

Tabla 4.5 valores de probabilidad de falla en demanda [14]

Valores de Probabilidad de Falla en Demanda (S_{PFD})	intervalo de Probabilidad	Número de fallas esperadas basadas en 1,000 demandas
0	~1	~1000
0.5	~1 a ~0.3	300 a ~1000
1	~0.3 a 0.1	100 a 300
1.5	0.1 a ~0.03	30 a 100
2	~3 x 10-2 a 1 x 10-2	10 a 30
2.5	1 x 10-2 a ~3 x 10-3	3 a 10
3	~3 x 10-3 a 1 x 10-3	1 a 3
3.5	1 x 10-3 a ~3 x 10-4	Oportunidad de 100% a 30% de una falla
4	~3 x 10-4 a 1 x 10-4	Oportunidad de 30% a 10% de una falla
4.5	1 x 10-4 a ~3 x 10-5	Oportunidad de 10% a 3% de una falla
5	~3 x 10-5 a 1 x 10-5	Oportunidad de 3% a 1% de una falla

El índice S_{PFD} permite traducir la probabilidad de falla bajo demanda en un valor fácil de manejar cuya magnitud es proporcional a la efectividad de la protección. De esta manera, un valor cercano a cero de S_{PFD} indica una protección con muy baja efectividad y altas probabilidades de fallar en caso de que se le necesite, y viceversa.

Los valores de S_{PFD} (tabla 3.6) se pueden determinar a partir de los datos publicados en las referencias 3, 7y 20, entre otras. A continuación se muestran algunos valores representativos:

Tabla 4.6 valores típicos de S_{pfd} para algunos elementos representativos de proceso [7][20][3]

Elemento de proceso	S_{PFD} típico
Bomba centrífuga accionada por motor eléctrico (relevo)	2
Válvula de no-retorno (check)	3
Válvula manual	4
Válvula motorizada	2.5
Válvula neumática	3
Válvula solenoide	3
Sistema de agua contra-incendio (motor diesel)	2
Sistema de agua contra-incendio (motor eléctrico)	1.5
Válvula de relevo (PSV) de resorte	4
SIS con SIL 1	2
SIS con SIL 2	3
SIS con SIL 3	4
Respuesta humana a una alarma de proceso (procedimiento simple y claro, con más de 30 minutos para responder, poco estrés)	1.5
Respuesta humana con poco tiempo para responder (menos de 5 minutos) en situaciones de alto estrés (situaciones complejas)	0.5

Estos valores típicos requerirán un ligero ajuste a la hora de ser utilizados en esta metodología, ya que existen factores que afectan la tasa de falla de los equipos y por lo tanto, reducen la efectividad de las capas de protecciones existentes. [6] [7] [23] los factores se mencionan en el capitulo 2, sección 2.4.2 de éste trabajo.

Obtención de la efectividad total de las capas de protección

Una vez identificadas las capas de protección independientes y calculadas en cuanto a su efectividad se deberán sumar los valores S_{PFD} individuales para obtener la efectividad total de las protecciones (Es), donde:

$$E_s = \Sigma S_{PFD} \quad (13)$$

4.3.5 Determinar la frecuencia esperada de las consecuencias considerando las capas de protección independientes

El valor de la efectividad total de las protecciones (E_s) se usa para calcular el valor de la frecuencia esperada de las consecuencias considerando las capas de protección independientes, a la cual se llamará frecuencia reducida (F_r)

$$F_r = F_i - E_s \quad (14)$$

4.3.6 Determinar la necesidad de capas adicionales de protección y determinar el SIL requerido si un SIS es recomendado.

Una vez obtenida la frecuencia reducida (F_r) es necesario compararla con la frecuencia umbral (F_t) para el escenario seleccionado:

- Si $F_r \leq F_t$, entonces **las protecciones son suficientes** para el escenario de riesgo en cuestión (si $F_r << F_t$, entonces hay un sobrediseño de acuerdo a los criterios de aceptabilidad).
- Si $F_r > F_t$, entonces **las protecciones son insuficientes** para el escenario de riesgo en cuestión (la efectividad de las protecciones no alcanza para reducir la frecuencia del evento inicial hasta el valor de frecuencia máxima aceptable del escenario)

Cuando $F_r > F_t$, es necesario calcular la efectividad (reducción de frecuencia) requerida (S_{add}) para determinar la estrategia de control de riesgos a implementar:

$$S_{add} = F_r - F_t \quad (15)$$

De acuerdo al valor de S_{add} se pueden tener 3 casos:

Caso 1: $S_{add} \leq 1$

En caso de que ya haya capas de protección aplicables al escenario (normalmente este es el caso), es prudente recomendar mejorar la efectividad de éstas capas (por ejemplo: los programas de mantenimiento más frecuentes y sistematizados pueden mejorar la confiabilidad de las protecciones ya existentes; la respuesta de los operadores puede ser razonablemente mejorada con capacitación y entrenamiento). En caso de no haber capas de protección aplicables al escenario, tratar de implementar alguna capa de protección que no sea un SIS.

Caso 2: $1.5 \leq S_{add} \leq 4$

Si es posible agregar capas no-SIS adicionales, entonces hay que sugerir las capas de protección posibles y mejorar la efectividad de las existentes, re-evaluar el sistema para determinar si esto es suficiente. Si NO es posible agregar más capas no-SIS, entonces hay que proponer mejoras en las capas de protección existentes e instalar un SIS

Caso 3: $S_{add} > 4$

El valor de S_{add} es muy elevado y una protección SIS no sería suficiente para mitigar el riesgo, por lo cual primero es recomendable evaluar el diseño de los equipos y/o del proceso para buscar soluciones de alta efectividad y segundo, implementar varias capas de protección SIS y no SIS hasta llevar el riesgo a niveles aceptables.

En caso de resultar conveniente el uso de un Sistema Instrumentado de Seguridad (SIS), el SIL requerido se determinará, volviendo a evaluar el valor de S_{add} después de considerar las otras alternativas no-SIS y utilizando la siguiente tabla (3.7):

Tabla 4.7 determinación del SIL requerido a partir del valor S_{ADD} [25] [14]

S_{add}	PFD correspondiente	SIL requerido
1.5 – 2	10^{-1} - 10^{-2}	1
2.5 – 3	10^{-2} - 10^{-3}	2
3.5 – 4	10^{-3} - 10^{-4}	3

CAPÍTULO 5.

RESULTADOS

RESULTADOS

5.1 APLICACIÓN DE METODOLOGIA

La metodología de análisis cuantitativo simplificado se aplicó en la planta reformadora de Nafta pesada de la refinería de Minatitlán Veracruz, en este capitulo se analizan los resultados al aplicar dicha metodología.

El propósito fundamental en este capitulo es comprobar si la metodología propuesta es aplicable y es útil para minimizar las fallas de los escenarios en estudio.

En este estudio se clasifica el riesgo potencial (sin considerar las protecciones o considerando que todas fallen) y se clasifica el riesgo actual (considerando las protecciones) de cada escenario de manera cualitativa.

La metodología se apoya en una técnica de análisis cualitativo (HAZOP) para identificar los eventos de alto riesgo, como es el caso de escenarios que tienen clasificación de riesgos Inaceptables (A) y riesgos Indeseables (B), dando prioridad a aquellos en los que se pueden producir explosiones, incendios o liberación de sustancias tóxicas.

Se hace un análisis semi-cuantitativo (por orden de magnitud) de la frecuencia y la gravedad del riesgo potencial de cada escenario seleccionado.

La metodología incorpora la identificación de capas de protección independiente y evalúa su efectividad (riesgo reducido) a través de su probabilidad de falla en demanda (PFD) respectiva. Propone criterios (frecuencia umbral) para decidir si el escenario tiene capas de protección suficientes o requiere de capas de protección adicional o en un caso determinado proponer sistemas instrumentados de seguridad que incluyan válvulas de activación remota como elemento final de control.

Además, tiene el potencial para evaluar los niveles integrales de la seguridad (SIL) de los sistemas instrumentados de seguridad (SIS) propuestos o existentes.

En caso de que desee determinar el SIL de un SIS ya instalado se puede proceder evaluando el escenario de riesgo sin considerar el SIS como capa de protección. El valor del riesgo reducido correspondiente dará como resultado el nivel SIL requerido para ese escenario en estudio.

No siempre es necesario contar con una gran cantidad de capas de protección o sistemas SIS. Una gran cantidad de escenarios de riesgos pueden resolverse al mejorar el diseño del proceso y la instrumentación para disminuir con esto la magnitud y frecuencia de las desviaciones en el proceso y hacer menos críticos los sistemas de seguridad.

Básicamente la metodología se aplicó a:

- Escenarios de alto riesgo (clasificación A y B)
- Escenarios con interruptores automáticos (interlocks) existentes
- Escenarios con sistema instrumentados de seguridad propuesto (Sistemas con detectores de fuego, con válvula de aislamiento de activación remota).
- Escenario con sistema instrumentado de seguridad propuesto (Sistema automático de alarma para detección de fuego y/o por atmósferas riesgosas).

Se presenta la metodología resumida con la definición de cada una de las variables en el siguiente formato para su mejor entendimiento:

ESTUDIO #: Referido a la secuencia del análisis (Determinación del SIL).	
Escenario #: Es un evento no planeado o secuencias de eventos que resultan de una consecuencia no deseada. Referirlo al escenario de mayor riesgo potencial del estudio HAZOP (Anexo B)	
Causa:	**Es lo que hace que un incidente o accidente ocurra. Referirlo al escenario del estudio HAZOP (Anexo B).**
Efecto:	**Es el daño leve o grave, producto de un incidente o accidente. Referirlo al escenario del estudio HAZOP (Anexo B).**

NOMBRE DE LA PLANTA:	**Caso de estudio.**
NODO: Es una subdivisión de un sistema de proceso, que tiene un origen, en donde comienzan nuevas propiedades del material procesado y un destino, en donde nuevamente hay un cambio de propiedades. Referirlo al escenario del estudio HAZOP (Anexo B).	

Circuito:	Sección de la planta claramente definida por el equipo multidisciplinario. Referido al escenario del estudio HAZOP (Anexo B).		
Producto:	Referido al indicado en el nodo (Anexo B)		
Localizado en Diagrama(s):	No. de diagrama correspondiente al análisis HAZOP.		
DESVIACIÓN:	Son las palabras guías que indican una modificación cualitativa o cuantitativa de los parámetros a analizar. Referido al escenario del estudio HAZOP (Anexo B).		
EVENTO RIESGOSO:	Determinación de un evento hipotético en el cual se toma en consideración la ocurrencia de un accidente bajo condiciones determinadas, que puede traer consecuencias al personal, al medio ambiente, a las instalaciones y/o alteración a la actividad normal del proceso. Definiendo mediante la aplicación de modelos matemáticos y criterios acordes a los característicos de los procesos y/o materiales, las zonas potenciales afectadas. Referido al escenario del estudio HAZOP (Anexo B).		
Clase de Gravedad de Consecuencia:	Esta es una evaluación "cualitativa", que los miembros del equipo deben determinar. Esta referido a la tabla 4.0 y tabla 4.3.	Descripción de los efectos potenciales de acuerdo a la gravedad de consecuencias. Esta referido a la tabla 4.3	
Frecuencia al Umbral (F_t):	Frecuencia máxima permitida para cada nivel de gravedad de consecuencias de un escenario de riesgo, en órdenes de magnitud. Referirse a tabla 4.2	Correlaciona directamente los criterios de aceptación de la compañía. Referirse a tabla 4.2	
EVENTO INICIAL:	Es el resultado de varias causas subyacentes tales como eventos externos, fallas de equipos, o fallas humanas. Referido al escenario del estudio HAZOP (Anexo B).		
Frecuencia del Evento inicial (F_i):	Se determina a partir de la frecuencia cualitativa, sin considerar protecciones. Referirse a tabla 4.4 y tabla 4.1	Tiempo observado entre eventos. Referirse a tabla 4.1 y tabla 4.4	
CAPAS DE PROTECCIÓN:		PFD	S_{PFD}

	Dispositivo, sistema o acciones capaces de prevenir el que un escenario continué hacia consecuencias indeseadas. Referirse a figura 4.1	Probabilidad de falla en demanda de capas de protección. Referirse a Anexo A	Orden de magnitud de PFD. Referirse a tabla 4.5 y tabla 4.6
Efectividad de las Capas (E_s): $\sum S_{PFD}$	Ecuación 13		
Frecuencia Reducida (F_r): $F_i - E_s$	Ecuación 14		
Protecciones adicionales (S_{add}): $F_r - F_t$	Ecuación 15		

CONCLUSIÓN: Aplicar los criterios de la metodología sección 4.3.6	
ALTERNATIVAS DE SOLUCIÓN:	Las alternativas de solución dependerán de las conclusiones. a) las capas de protección son suficientes. b) Se requieren capas de protección adicional y de que tipo deben de ser no-SIS o SIS. Referirlo a la sección 4.3.6

¿Se recomienda un SIS?	
Justificación de la recomendación:	Si no es posible agregar más capas no-SIS, entonces hay que proponer mejoras en las capas de protección existentes o en caso dado instalar un SIS. Referirse a sección 4.3.6.
DETERMINACION DEL SIL	
Justificación:	Si un SIS es requerido, se evaluará el SIL. Referirlo a la tabla 4.7

5.1.1 Eventos de alto riesgo (clasificación A y B).

ESTUDIO # 1.	
Escenario 31.	
Causa:	Contaminación de la carga de azufre.
Efecto:	Daños irreversibles al catalizador.

NOMBRE DE LA PLANTA:	Planta reformadora de Naftas 2 (U-500)
NODO: 2. Tanque de balance de carga FA-513, bombas GA-514 A/R, intercambiador EA-501, Calentador de carga BA-501 A/B/C/D, reactor DC-501 A/B/D hasta entrada a solenoide EC-501.	
Circuito:	Circuito de calentamiento y reacción.
Producto:	Nafta pesada
Localizado en Diagrama(s):	U500-001 Y 002

DESVIACIÓN:	Baja conversión de reformado en los reactores DC-501 A/B/C/D.		
EVENTO RIESGOSO:	Daños irreversibles al catalizador, producto fuera de especificaciones (bajo octano), disminución de la producción de hidrógeno.		
Clase de Gravedad de Consecuencia:	Crítico	Pérdidas mínimas en la producción.	
Frecuencia al Umbral (F_t):	5	Máxima aceptable, 1/300 eventos por año.	
EVENTO INICIAL:	Contaminación de la carga de azufre.		
Frecuencia del Evento inicial (F_i):	8	Frecuente (Ha ocurrido más de una vez al año. Evento observado entre 0.3 y 1 año.)	
CAPAS DE PROTECCION:		**PFD**	**S_{PFD}**
	Procedimiento para el reajuste de condiciones de operación cuando se detecta carga contaminada. Análisis rutinario de azufre en la carga, análisis rutinarios de acetato de plomo.	10E-1	1.5
Efectividad de las Capas (E_s): $\sum S_{PFD}$	1.5		
Frecuencia Reducida (F_r): $F_i - E_s$	8.0 – 1.5 = 6.5		
Protecciones adicionales (S_{add}): $F_r - F_t$	6.5 – 5.0 =1.5		

CONCLUSIÓN: El valor de S_{add} es positivo por lo que se requiere de protecciones no SIS adicionales para cumplir con los criterios de aceptabilidad de riesgos. El problema está referido a problemas operacionales.	
ALTERNATIVAS DE SOLUCIÓN:	Para mitigar el evento no deseado y reducir la frecuencia del evento inicial se recomienda, realizar estudio técnico-económico para la instalación de guardas de azufre en la línea de recibo de carga liquida. Solicitar e instalar analizador continuo de azufre, en la línea de recibo de carga liquida, con la finalidad de desviar la carga y no contaminar la planta. Solicitar e instalar analizador de octano en línea, en la salida de producto final a tanque de almacenamiento.

¿Se recomienda un SIS?	NO
Justificación de la recomendación:	El evento no deseado está referido a problemas de operación del proceso y es por ese conducto por el cual se debe solucionar.

DETERMINACIÓN DEL SIL	No aplica
Justificación:	No aplica el SIL ya que no se requiere un sistema instrumentado de seguridad.

ESTUDIO # 2.	
Escenario 37.	
Causa:	Arrastre de hidrocarburos en el gas de recirculación por: operación deficiente de filtros coalescedores, falla en el calentamiento del gas de arrastre, problemas de condensación en el sistema de reacción.
Efecto:	Daños a los internos del reactor. Posible paro de planta.

NOMBRE DE LA PLANTA:	Planta reformadora de Naftas 2 (U-500)
NODO: 2. Tanque de balance de carga FA-513, bombas GA-514 A/R, intercambiador EA-501, Calentador de carga BA-501 A/B/C/D, reactor DC-501 A/B/D hasta entrada a solenoide EC-501.	
Circuito:	Circuito de calentamiento y reacción.
Producto:	Nafta pesada
Localizado en Diagrama(s):	U500-001 Y 002

DESVIACIÓN:	Alta presión diferencial en el reactor DC-501 A/B/C/D		
EVENTO RIESGOSO:	Posibles daños a los internos del reactor, disminución de la producción de hidrógeno, posible paro de planta con cambios y/o cribado de catalizador.		
Clase de Gravedad de Consecuencia:	Mayor	Daños mayores a una ò varias áreas de proceso , con algo de pérdida de producción	
Frecuencia al Umbral (F_t):	4.0	Máxima aceptable, 1/3000 eventos por año.	
EVENTO INICIAL:	Arrastre de hidrocarburos en el gas de recirculación por: operación deficiente de filtros coalescedores, falla en el calentamiento del gas de arrastre.		
Frecuencia del Evento inicial (F_i):	8	Frecuente (Ha ocurrido más de una vez al año. Evento observado entre 0.3 y 1 año.)	
CAPAS DE PROTECCIÓN:			
		PFD	**S_{PFD}**
	Alarma por alta temperatura en la zona de reacción, manual de operación del modulo CCR.	1.98E-2	2.0
	Toma de lectura de campo y de bunker de presión del gas hidrógeno, con paro de la unidad CCR por no tener flujo de gas hidrógeno proveniente del compresor booster.	10E--1	1.5
Efectividad de las Capas (E_s): $\sum S_{PFD}$	2.0 + 1.5 = 3.5		
Frecuencia Reducida (F_r): $F_i - E_s$	8.0 – 3.5 = 4.5		
Protecciones adicionales (S_{add}): $F_r - F_t$	4.5 - 4.0 = 0.5		

CONCLUSIÓN: El valor de S_{ADD} es ligeramente positivo por lo que no se requieren capas de protección adicional.	
ALTERNATIVAS DE SOLUCIÓN:	Desde el punto de vista de proceso; se requiere mantener y garantizar los niveles de flujo de hidrógeno en esta etapa por lo que se recomienda adquirir un compresor booster para reemplazar al GB-502B.

¿Se recomienda un SIS?	NO
Justificación de la recomendación:	Las protecciones en conjunto son suficientes. Sin embargo, se recomienda dar mantenimiento preventivo a los filtros coalescedores y soloaires.

DETERMINACIÓN DEL SIL	No aplica
Justificación:	No aplica un SIL, puesto que no se requiere de un SIS, y el $S_{add} = 0.0$ se encuentra por debajo del intervalo para sugerirlo.

ESTUDIO # 3.	
Escenario 48.	
Causa:	Disparo del compresor GB-501.
Efecto:	Paro de planta.

NOMBRE DE LA PLANTA:	Planta reformadora de Naftas 2 (U-500)
NODO: 3. Soloaire EC-501, condensador EA-507 A/B, separador de baja presión FA-501 hasta la succión del compresor de recirculación.	
Circuito:	Circuito de calentamiento y compresión de gas de recirculación.
Producto:	Reformado, hidrógeno e hidrocarburos gaseosos condensables y no condensables.
Localizado en Diagrama(s):	U500-003

DESVIACION:	Alta presión en el separador de baja presión FA-501		
EVENTO RIESGOSO:	Carbonización del catalizador en el reactor DC-501 A/D y en el interior de los serpentines de calentador BA-501 A/D, paro de planta.		
Clase de Gravedad de Consecuencia:	Mayor	Daños mayores a una ò varias áreas de proceso , con algo de perdida de producción	
Frecuencia al Umbral (F_t):	4.0	Máxima aceptable, 1/3000 eventos por año.	
EVENTO INICIAL:	Disparo del compresor GB-501.		
Frecuencia del Evento inicial (F_i):	8	Frecuente (Ha ocurrido más de una vez al año. Evento observado entre 0.3 y 1 año.)	
CAPAS DE PROTECCION:		**PFD**	**S_{PFD}**
	Válvula de alivio del FA-501, PSV-502 y su línea de directo.	1E-2	2.0
	interruptor automático (Interlock) de disparo del calentador BA-501 A/D y corte de carga liquida	1E-2	2.0
	PIC-524, actuando la PV-524 B enviando a desfogue a gas combustible.	3E-3	2.5
Efectividad de las Capas (E_s): $\sum S_{PFD}$	2.0 + 2.0 + 2.5 = 6.5		
Frecuencia Reducida (F_r): $F_i - E_s$	8.0 - 6.5 = 1.5		
Protecciones adicionales (S_{add}): $F_r - F_t$	1.5 - 4.0 = -2.5		

CONCLUSIÓN: El valor de S_{add} es negativo, por lo que las capas de protección son suficientes en el sistema.	
ALTERNATIVAS DE SOLUCIÓN:	Se recomienda eficientar el programa de mantenimiento preventivo de instrumentos y mecánico del compresor GB-501

¿Se recomienda un SIS?	NO (ya existe)
Justificación de la recomendación:	Las protecciones en conjunto son suficientes.

DETERMINACIÓN DEL SIL	No aplica
Justificación:	No aplica un SIS, puesto que no se requiere de un sistema instrumentado de seguridad, y el S_{add} = -2.5 no esta en el intervalo para sugerirlo.

ESTUDIO # 4.	
Escenario 58.	
Causa:	Baja presión del vapor de alimentación a la turbina.
Efecto:	Posible paro de planta.

NOMBRE DE LA PLANTA:	Planta reformadora de Naftas 2 (U-500)
NODO: 4. Compresor GB-501.	
Circuito:	Circuito de compresión de gas de recirculación
Producto:	Reformado, hidrógeno e hidrocarburos gaseosos condensables y no condensables.
Localizado en Diagrama(s):	U500-003

DESVIACIÓN:	Baja presión de descarga del compresor GB-501.		
EVENTO RIESGOSO:	Carbonización y formación de ligeros, en el reactor. Posibles daños al compresor, con posibilidad de fuga de gas recirculación en el sello, Inestabilidad (surge) del compresor, Posible paro de planta.		
Clase de Gravedad de Consecuencia:	Mayor	Daños mayores a una o varias áreas de proceso , con algo de pérdida de producción	
Frecuencia al Umbral (F_t):	4.0	Máxima aceptable, 1/3000 eventos por año.	
EVENTO INICIAL:	Baja presión del vapor de alimentación a la turbina		
Frecuencia del Evento inicial (F_i):	8	Frecuente (Ha ocurrido más de una vez al año. Evento observado entre 0.3 y 1 año.)	
CAPAS DE PROTECCIÓN:		**PFD**	**S_{PFD}**
	Alarma y disparo (calentador BA-501 A/D) por bajo flujo de gas de recirculación	1E-2	2.0
	Indicador de presión del vapor a la turbina en tablero de control, indicador de presión en pantalla de SCD del cabezal de suministro, reajuste de carga, procedimiento a falla del compresor GB-501 en la planta U-500.	10E-1	1.5
Efectividad de las Capas (E_s): $\sum S_{PFD}$	2.0 + 1.5 = 3.5		
Frecuencia Reducida (F_r): $F_i - E_s$	8 - 3.5 = 4.5		
Protecciones adicionales (S_{add}): $F_r - F_t$	4.5 - 4.0 = 0.5		

CONCLUSIÓN: El valor de Sadd es ligeramente positivo, por lo que no se requiere de capa de protección adicional para mitigar el riesgo en cuestión.	
ALTERNATIVAS DE SOLUCIÓN:	Para mitigar la probabilidad del evento no deseado se recomienda completar la segunda capa de protección, agregando sistema de alarma por baja presión en el cabezal de suministro de vapor a la planta seguido de un procedimiento por falla de vapor en la planta U-500, sistema existente.

¿Se recomienda un SIS?	NO
Justificación de la recomendación:	Instalando la alarma en el cabezal de Baja presión la efectividad de las protecciones es suficiente para el escenario de riesgo en cuestión.

DETERMINACION DEL SIL	No aplica
Justificación:	No aplica un SIS, puesto que no se requiere de un sistema instrumentado de seguridad, y el S_{add} = 0.5 no esta en el rango para sugerirlo.

5.1.2 Escenarios con interruptores automáticos (interlocks) existentes, indicando su sistema.

ESTUDIO # 5.	
Escenario 12.	
Causa:	Falla en FIC-509 con válvula automática cerrada.
Efecto:	Daños a los internos del calentador. Posible paro de planta.

NOMBRE DE LA PLANTA:	Planta reformadora de Naftas 2 (U-500).
NODO: 2. Tanque de balance de carga FA-513, bombas GA-514 A/R, intercambiador EA-501, Calentador de carga BA-501 A/B/C/D, reactor DC-501 A/B/D.	
Circuito:	Circuito de calentamiento y reacción.
Producto:	Nafta pesada.
Localizado en Diagrama(s):	U500-001 y 002

DESVIACIÓN:	Menos flujo de carga liquida en la descarga de las bombas GA-514/R y los reactores DC-501 A/B/D/D.		
EVENTO RIESGOSO:	Carbonización en el interior de los serpentines, alta temperatura en la salida del calentador de carga, paro de planta, producto final fuera de especificaciones.		
Clase de Gravedad de Consecuencia:	Mayor	Daños mayores a una o varias áreas de proceso y algo de pérdidas en la producción.	
Frecuencia al Umbral (F_t):	4.0	Máxima aceptable, 1/3000 eventos por año.	
EVENTO INICIAL:	Falla en FIC-509 con válvula automática cerrada		
Frecuencia del Evento inicial (F_i):	7.5	Ocasional (Ha ocurrido varias veces durante la vida de la planta. Evento observado entre 1 y 3 años.)	
CAPAS DE PROTECCION:		**PFD**	**S_{PFD}**
	Pasar el control de la válvula automática a manual, bloqueo de la automática y uso de la línea de directo, con indicador de flujo en el SCD.	9.0E-1	0.5
Efectividad de las Capas (E_s): $\sum S_{PFD}$	0.5		
Frecuencia Reducida (F_r): $F_i - E_s$	7.5 - 0.5 = 7.0		
Protecciones adicionales (S_{add}): $F_r - F_t$	7.0 - 4.0 = 3.0		

CONCLUSIÓN: El valor de S_{add} es positivo por lo que se requiere de protecciones adicionales para cumplir con los criterios de aceptabilidad de riesgos.	
ALTERNATIVAS DE SOLUCIÓN:	Para disminuir la posibilidad de que se tengan altas temperaturas y que pueden ocasionar daños al catalizador por formación de depósitos de carbón, debido al bajo flujo de carga liquida en la descarga liquida de las bombas. Es indispensable instalar: sensores, solucionador lógico y elemento final de control que suspenda la operación del calentador inmediatamente, por bajo flujo y alta temperatura.

¿Se recomienda un SIS?	SI (ya existe interruptor automático (interlock))
Justificación de la recomendación:	Se requiere un sistema de protección de respuesta rápida que evite la escalacion del evento no deseado (alta temperatura a la salida de calentador). Además se requiere una alarma y sistema de disparo del calentador por bajo flujo de la carga.

DETERMINACIÓN DEL SIL	Aplica
Justificación:	Aplica un SIL, puesto que se requieren de dos sistemas instrumentado de seguridad, con un valor de S_{add} = 1.5 cada uno correspondiente a un valor de **SIL = 1** respectivamente

INTERRUPTOR AUTOMÁTICO (INTERLOCK) UY-518 (Alta temperatura)

- TAH-502/508/512/ a TSH-503/501/507/510 manda señal solenoide UY-518.
- UY-509 manda cerrar la válvula de corte rápido FV-518. BA-501 A/D.

INTERRUPTOR AUTOMÁTICO (INTERLOCK) UY-509 (Bajo flujo de la carga)

- PSL-509 manda señal solenoide UY-509.
- UY-509 manda cerrar la válvula de corte rápida FV-509.
- El PSL-509 manda también señal al interlock para disparo del calentador BA-501 A/D.

ESTUDIO # 6.	
Escenario 29.	
Causa:	Bajo flujo de hidrógeno de recirculación al calentador BA-501 A/D.
Efecto:	Daños a los internos del calentador. Posible paro de planta.

NOMBRE DE LA PLANTA:	Planta reformadora de Naftas 2 (U-500).
NODO: 2. Tanque de balance de carga FA-513, bombas GA-514 A/R, intercambiador EA-501, Calentador de carga BA-501 A/B/C/D, reactor DC-501 A/B/D hasta entrada a solenoide EC-501.	
Circuito:	Circuito de calentamiento y reacción.
Producto:	Nafta pesada.
Localizado en Diagrama(s):	U500-001 Y 002

DESVIACION:	Alta temperatura en la salida del calentador de carga combinada BA-501 A/B/C/D hasta entrada a soloaire EC-501		
EVENTO RIESGOSO:	Carbonización en el interior de los serpentines y del catalizador, alta temperatura en la salida del calentador de carga, paro de planta, producto final fuera de especificaciones.		
Clase de Gravedad de Consecuencia:	Mayor	Daños mayores a una o varias áreas de proceso y algo de pérdidas en la producción.	
Frecuencia al Umbral (F_t):	4.0	Máxima aceptable, 1/3000 eventos por año.	
EVENTO INICIAL:	Bajo flujo de hidrógeno de recirculación al calentador		
Frecuencia del Evento inicial (F_i):	7.5	Ocasional (Ha ocurrido varias veces durante la vida de la planta. Evento observado entre 1 y 3 años).	
CAPAS DE PROTECCION:		**PFD**	**S_{PFD}**
	Alarmas de alta temperatura en la salida de los calentadores, y en el hogar inferior, superior y chimenea y por bajo flujo de gas de recirculación, FAL-510. Procedimiento de paro de emergencia de la planta.	1.98E-2	2.0
Efectividad de las Capas (E_s): $\sum S_{PFD}$	2.0		
Frecuencia Reducida (F_r): $F_i - E_s$	7.5 - 2.0 = 5.5		
Protecciones adicionales (S_{add}): $F_r - F_t$	5.5 - 4.0 = 1.5		

CONCLUSIÓN: El valor de S_{add} es positivo por lo que se requiere de protecciones adicionales para cumplir con los criterios de aceptabilidad de riesgos.	
ALTERNATIVAS DE SOLUCIÓN:	Para disminuir la posibilidad de que se tengan altas temperaturas y que pueden ocasionar éstos daños al catalizador por formación de depósitos de carbón y serpentines del catalizador, debido al bajo flujo de hidrógeno de recirculación al calentador. Es indispensable instalar: sensores, solucionador lógico y elemento final de control que suspenda la operación del calentador inmediatamente, contar con un programa de mantenimiento preventivo adecuado del sistema de enfriamiento con aire (soloaire) y condensación.

¿Se recomienda un SIS?	SI (ya existe interruptor automático (interlock)).
Justificación de la recomendación:	Se requiere un sistema de protección de respuesta rápida que evite la escalacion del evento no deseado (alta temperatura a la salida de calentador).

DETERMINACIÓN DEL SIL	Aplica.
Justificación:	Aplica un SIL, puesto que se requiere un sistema instrumentado de seguridad, y el valor de Sadd = 1.5 corresponde a un valor de **SIL = 1**.

INTERRUPTOR AUTOMÁTICO (INTERLOCK) FSL-510:

- FSL-510A manda señal, disparo de bomba GA-514.
- PSL-509 manda señal solenoide UY-509.
- UY-509 manda cerrar la válvula automática FV-509.

El PSL-509 manda también señal al interruptor automático (interlock) para disparo del calentador BA-501 A/D.

ESTUDIO # 7.	
Escenario 83.	
Causa:	Baja presión de la red de gas combustible.
Efecto:	Incumplimiento al programa de producción.

NOMBRE DE LA PLANTA:	Planta reformadora de Naftas 2 (U-500).
NODO: 7. Zona de agotamiento de la torre DA-501, bomba GA-504 A/R, calentador BA-502 y retorno al fondo de la torre DA-501.	
Circuito:	Circuito de estabilización.
Producto:	Reformado estabilizado.
Localizado en Diagrama(s):	U500-006

DESVIACIÓN:	Baja temperatura en el fondo de la torre DA-501.		
EVENTO RIESGOSO:	Posible aumento de nivel en el fondo de la torre DA-501, reformado fuera de especificaciones, pérdida de producción por disminución de carga, menor producción de destilado en la torre DA-501.		
Clase de Gravedad de Consecuencia:	Mayor	Daños mayores a una o varias áreas de proceso , con algo de pérdida de producción	
Frecuencia al Umbral (F_t):	4.0	Máxima aceptable, 1/3000 eventos por año.	
EVENTO INICIAL:	Baja presión de la red de gas combustible.		
Frecuencia del Evento inicial (F_i):	7.5	Ocasional (Ha ocurrido varias veces durante la vida de la planta. Evento observado entre 1 y 3 eventos por años).	
CAPAS DE PROTECCION:		PFD	S_{PFD}
	Verificación de la presión en manómetro, indicadores de temperatura en la salida del calentador, compensación al suministro de gas combustible con gas de campo.	10E-1	1.5
Efectividad de las Capas (E_s): $\sum S_{PFD}$	1.5		
Frecuencia Reducida (F_r): $F_i - E_s$	7.5 - 1.5 = 6.0		
Protecciones adicionales (S_{add}): $F_r - F_t$	6.0 - 4.0 = 2.0		

CONCLUSIÓN: El valor de S_{add} es positivo por lo que se requiere de protecciones adicionales para cumplir con los criterios de aceptabilidad de riesgos.

ALTERNATIVAS DE SOLUCIÓN:	Se recomienda, para la baja presión del gas combustible un sistema que dispare el calentador BA-502 para eliminar problemas subsecuentes. Además se debe contar con las refacciones adecuadas y a la mano, para el mantenimiento de alarmas y disparos, de manera oportuna.

¿Se recomienda un SIS?	SI (ya existe)
Justificación de la recomendación:	Se requiere un sistema de protección de respuesta rápida que evite la escalacion de los problemas subsecuentes por lo que se recomienda un sistema instrumentado de seguridad.

DETERMINACION DEL SIL	Aplica
Justificación:	Aplica un SIL, puesto que se requiere un sistema instrumentado de seguridad, y el valor de Sadd = 2.0 corresponde a un valor de **SIL = 1**.

INTERRUPTOR AUTOMÁTICO (INTERLOCK) UY-503/534:

- PSL-535/534 manda señal al solenoide UY-503/534.
- UY-503/534 manda cerrar las válvulas UV-503/534.

5.1.3 Sistemas con detectores de fuego, con válvulas de aislamiento de activación remota (VAAR).

ESTUDIO # 8.	
Escenario s/n.	
Causa:	Fugas en los sellos y/o bridas, de las bombas BA-514 A/RT
Efecto:	Incendio, paro de planta, sobrepresionamiento de FA-513.

NOMBRE DE LA PLANTA:	Planta reformadora de Naftas 2 (U-500).
NODO: 1. Tanque de balance de carga FA-513, bombas GA-514 A/RT.	
Circuito:	Circuito de carga.
Producto:	Nafta pesada.
Localizado en Diagrama(s):	U-500-001

DESVIACIÓN:	Fuga en bridas o sellos de las bombas GA-514 A/RT.		
EVENTO RIESGOSO:	Incendio, paro de planta, sobrepresionamiento de FA-513.		
Clase de Gravedad de Consecuencia:	Mayor	Posibilidad de uno o más heridos graves, daño mayor a una o varias áreas de proceso con un costo estimado mayor a 1 millón de dólares con algo de pérdidas de producción	
Frecuencia al Umbral (F_t):	4	Máxima aceptable, 1/3000 eventos por año.	
EVENTO INICIAL:	Fuga en los sellos de las bombas y/o bridas.		
Frecuencia del Evento inicial (F_i):	6	Posible (no se tienen registros pero puede ocurrir. Evento observado entre 30 y 100 años).	
CAPAS DE PROTECCION:		PFD	S_{PFD}
	Ninguno		0.0
Efectividad de las Capas (E_s): $\sum S_{PFD}$	0.0		
Frecuencia Reducida (F_r): $F_i - E_s$	6.0 - 0.0 = 6.0		
Protecciones adicionales (S_{add}): $F_r - F_t$	6.0 - 4.0 = 2.0		

CONCLUSIÓN: El valor de S_{add} es positivo, por lo que se requiere una capa de protección adicional.	
ALTERNATIVAS DE SOLUCIÓN:	Instalación de VAAR activada por un sistema de detección y alarma para fuego, instalada de acuerdo al No. de documento NRF-011-PEMEX-2001, cercana a la fuente de liberación más probable (bridas y sellos de las bombas) en la dirección contraria a los vientos dominantes. Otra buena recomendación sería instalar un sistema de doble sello (Sistema Retrofit) en las bombas GA-514 A/RT.

¿Se recomienda un SIS?	SI
Justificación de la recomendación:	Sistema detector de fuego conectado a un PLC y éste a su vez a la VAAR, al disparo de las bombas y a un sistema automático de extinción de fuego.

DETERMINACION DEL SIL	Aplica
Justificación:	Sadd = 2.0 por lo cual SIL = 1

ESTUDIO # 9.	
Escenario 90.	
Causa:	Fugas en los sellos y/o bridas, de las bombas GA-504/R
Efecto:	Incendio en el interior del calentador BA-502.

NOMBRE DE LA PLANTA:	Planta reformadora de Naftas 2 (U-500).
NODO: 7. Zona de agotamiento de la torre DA-501, bomba GA-504 A/R, calentador BA-502 y retorno al fondo de la torre DA-501.	
Circuito:	Circuito de estabilización.
Producto:	Reformado estabilizado.
Localizado en Diagrama(s):	U500-006

DESVIACIÓN:	Bajo flujo de recirculación al calentador BA-502.		
EVENTO RIESGOSO:	Cavitación de la bomba de recirculación GA-504 /R, posible daño del sello, ruptura, fuga e incendio. Ruptura, fuga, e incendio en el interior del calentador BA-502.		
Clase de Gravedad de Consecuencia:	Mayor	Posibilidad de uno o más heridos graves, daño mayor a una o varias áreas de proceso con un costo estimado mayor a 1 millón de dólares o algo de pérdida de producción	
Frecuencia al Umbral (F_t):	4	Máxima aceptable, 1/3000 eventos por año.	
EVENTO INICIAL:	Pichanchas obstruidas de la bomba de recirculación, GA-504 /R		
Frecuencia del Evento inicial (F_i):	7.5	Ocasional (Ha ocurrido varias veces durante la vida de la planta. Evento observado entre 1 y 3 años).	
CAPAS DE PROTECCION:		PFD	S_{PFD}
	Alarma por bajo flujo al calentador BA-502 con procedimiento operativo.	1.98E-2	2.0
Efectividad de las Capas (E_s): $\sum S_{PFD}$	2.0		
Frecuencia Reducida (F_r): $F_i - E_s$	7.5 - 2.0 = 5.5		
Protecciones adicionales (S_{add}): $F_r - F_t$	5.5 - 4.0 = 1.5		

CONCLUSIÓN: El valor de S_{add} es positivo, por lo que se requiere una capa de protección adicional.	
ALTERNATIVAS DE SOLUCIÓN:	Instalación de VAAR en la salida del fondo de la torre DA-501 activada por un sistema de detección y alarma para fuego, instalada de acuerdo a el No. de documento NFR-011-PEMEX-2001, cercana a la fuente de liberación más probable (bridas y sellos de las bombas) en la dirección contraria a los vientos dominantes, integrado al interruptor automático (interlock) de disparo del calentador BA-502. Otra buena recomendación sería instalar un sistema de doble sello (Sistema Retrofit) en las bombas GA-504 A/R.

¿Se recomienda un SIS?	SI
Justificación de la recomendación:	Sistema detector de fuego conectado a un PLC y éste a su vez a la VAAR, al disparo de las bombas GA-504 A/R, integrado al interruptor automático (interlock) de disparo del calentador BA-502 y a un sistema automático de extinción de fuego.

DETERMINACIÓN DEL SIL	Aplica.
Justificación:	Sadd = 1.5 por lo cual SIL = 1

5.1.4 Sistema automático de alarma para detección de fuego y/o por atmósferas riesgosas.

ESTUDIO # 10.	
Escenario 108.	
Causa:	Ruptura de sellos del 1er y 2do paso de los compresores reciprocantes GB-502 A/B.
Efecto:	Incendio, posible paro de planta.

NOMBRE DE LA PLANTA:	Planta reformadora de Naftas 2 (U-500).
NODO: 9.Salida domo FA-502, guardas de cloro FA-503, compresor GB-502 A/B 1er y 2do paso y salidas a plantas U-400, CCR Y U-100.	
Circuito:	Circuito de compresión.
Producto:	Hidrógeno.
Localizado en Diagrama(s):	U500-004

DESVIACIÓN:	Daños en las estructuras de los compresores.		
EVENTO RIESGOSO:	Fuga de hidrogeno e hidrocarburos con incendio, paro del equipo, bajo flujo de hidrógeno a las unidades U-400/100 con su posible paro.		
Clase de Gravedad de Consecuencia:	Crítico	Pérdidas mínimas en la producción	
Frecuencia al Umbral (F_t):	5	Máxima aceptable, 1/300 eventos por año.	
EVENTO INICIAL:	Ruptura de sellos del 1er y 2do paso de los compresores reciprocantes GB-502 A/B.		
Frecuencia del Evento inicial (F_i):	8	Frecuente (Ha ocurrido más de una vez al año. Evento observado entre 0.3 y 1 año).	
CAPAS DE PROTECCION:		PFD	S_{PFD}
	Ninguno	0.0	0.0
Efectividad de las Capas (E_s): $\sum S_{PFD}$	0.0		
Frecuencia Reducida (F_r): $F_i - E_s$	8.0-0.0=8.0		
Protecciones adicionales (S_{add}): $F_r - F_t$	8.0-5.0=3.0		
CONCLUSIÓN: El valor de S_{add} es positivo por lo que se requiere de protecciones adicionales para cumplir con los criterios de aceptabilidad de riesgos.			
ALTERNATIVAS DE SOLUCIÓN:	Para mitigar la probabilidad de fugas e incendio en la descarga del compresor GB-502 A/B, 1er Y 2do paso y de acuerdo con los requerimientos de protecciones adicionales.		

	Se requiere tener en forma permanente, un juego de anillos, bandas de émbolo y un juego de sellos del compresor GB-502 A/B originales. Verificar y probar el metalizado de los émbolos nuevos a instalar. Realizar estudio técnico-económico para reemplazar el compresor GB-502 A por uno nuevo, por ser equipo obsoleto. Si se cumplen las peticiones anteriores, es importante estar analizando el comportamiento del escenario para verificar que disminuya la frecuencia del evento inicial, y complementarlo con una capa de protección adicional, como un sistema de detección y alarma para atmósferas contaminadas con productos inflamables. Interconectado con un sistema fijo automático para extinción de fuego para mitigar el evento no deseado a niveles permisibles.

¿Se recomienda un SIS?	SI
Justificación de la recomendación:	Es necesario instalar un sistema independiente de detección y alarma para atmósferas contaminadas con productos inflamables, con PLC complementado con sistema fijo automático para extinción de fuego.

DETERMINACIÓN DEL SIL	Aplica.
Justificación:	Aplica un SIL, puesto que se requieren un sistemas instrumentado de seguridad, con valores de S_{add} = 2.0, por lo cual les correspondería un valor de SIL = 1.

CAPÍTULO 6

DISCUSIÓN

Y

RECOMENDACIONES

6.1 DISCUSIÓN DE RESULTADOS

De acuerdo a los análisis efectuados con la metodología cuantitativa simplificada a los eventos de alto riesgo, escenarios con interruptores automáticos (interlocks) existentes, sistema con detectores de fuego, con válvulas de aislamiento de activación remota, eventos con propuesta de instalación de un sistema automático de alarma por detección de fuego y/o por atmósferas riesgosas sistema se obtuvieron los siguientes resultados.

EVENTOS DE ALTO RIESGO (CLASIFICACIÓN A Y B).

En el estudio #1. El escenario de riesgo está referido a problemas de operación del proceso, por lo que éste se mitiga reduciendo la frecuencia del evento inicial, se requiere de un sistema que elimine los residuos de azufre de la carga.

Se recomienda la instalación de guardas de azufre y analizador continuo de azufre en la línea de recibo de carga liquida.

En el estudio #2. El escenario de riesgo no requiere de capas de protección adicional, esto significa que para reducir la frecuencia del evento inicial y mantener los niveles de hidrógeno de manera estable es necesario modernizar los equipos de proceso.

Se recomienda mejorar el mantenimiento preventivo de filtros coalescedores y soloaire y/o en su caso remplazar el compresor booster.

En el estudio #3. El escenario de riesgo no requiere de capas de protección adicional, al dispararse el compresor GB-501 para evitar consecuencias posteriores, se dispara el calentador BA-501 A/D y el corte de carga liquida, activándose los sistemas de desfogues.
Se recomienda un buen programa de mantenimiento preventivo del compresor.

En el estudio #4. El escenario de riesgo está referido a problemas en los servicios auxiliares, sólo se requiere tener un programa de medidas preventivas en caso de que se tenga baja presión de vapor en la alimentación de la turbina y estar en comunicación permanente con el área de fuerza.

Se recomienda alarma en el cabezal de baja presión seguido de un procedimiento por falla de vapor en la planta U-500, en el caso del compresor y para evitar daños posteriores se requiere disparo del calentador BA-501 A/B y procedimiento para paro de planta.

ESCENARIOS CON INTERRUPTORES AUTOMÁTICOS (INTERLOCKS) EXISTENTES,

En el estudio #5. El método cuantitativo simplificado permite evaluar la confiabilidad de los sistemas instrumentados de seguridad ya existente, en este caso además de tener las medidas adecuadas de mantenimiento preventivo de los instrumentas es importante protegerse de consecuencias posteriores al incidente, por lo que se requiere proteger el calentador por alta temperatura a la salida y bajo flujo de la carga.

En el estudio #6. El escenario tiene las capas de protección adecuadas, el análisis es importante para evaluar el interruptor automático (interlock) ya existente, cuya función es, disparo de la bomba de carga GA-514, en el cual el PSL-509 actúa al cerrar la válvula automática FV-509 por bajo flujo y que también actúe mandando cortar el suministro de gas combustible, disparando el calentador BA-501 A/D.

En el estudio #7. El escenario al igual que el anterior tiene las capas de protección adecuadas, el análisis es importante para evaluar el interruptor automático (interlock) ya existente, cuya función es bloquear suministro de gas combustible y apagar quemadores del calentador.

*NOTA: Es necesario modificar los interruptores automáticos (interlocks) existentes de los estudios 5, 6,7 de tal manera que la configuración quede de acuerdo a la arquitectura propuesta a un SIL 1.

SISTEMAS CON DETECTORES DE FUEGO, CON VÁLVULAS DE AISLAMIENTO DE ACTIVACIÓN REMOTA (VAAR).

En el estudio #8. De acuerdo al Diagrama de Tubería e Instrumentación (figura 1), para un Sistema Instrumentado de Seguridad (SIS), la secuencia es la siguiente: disparo de la bomba GA-514/R, cierre de la válvula de corte rápido VAAR-FA-513, disparo del calentador BA-501 A/B/C/D, y aviso a plantas contiguas del paro de planta.

Estudio #9. De acuerdo al Diagrama de Tubería e Instrumentación (figura 1), para un Sistema Instrumentado de Seguridad (SIS), la secuencia es la siguiente: disparo de la bomba GA-504/R, cierre de la válvula de corte rápido VAAR- DA-501, disparo del calentador BA-501 A/B/C/D, y aviso a plantas contiguas del paro de planta.

EVENTOS CON PROPUESTA DE INSTALACIÓN DE UN SISTEMA AUTOMÁTICO DE ALARMA POR DETECCIÓN DE FUEGO Y/O POR ATMÓSFERAS RIESGOSAS.

Estudio #10. Las fugas de las corrientes de hidrógeno en las descargas de compresores provoca que su flujo disminuya y que por lo tanto, se disparen los quemadores del calentador y dañe otras unidades de producción para evitar problemas mayores.

El hidrógeno es un gas flamable, por lo que se tiene que tener cuidado en su manejo.

Para mitigar la frecuencia del evento es importante contar con un programa permanente de mantenimiento preventivo para tener en buen estado los sellos de los compresores, además, para prever consecuencias con el hidrógeno en la atmósfera es importante contar con un sistema de detección y alarma para atmósferas contaminadas con productos inflamables, PLC, complementado con sistema fijo automático para extinción de fuego generado por el hidrógeno.

6.2 RECOMENDACIONES.

De acuerdo a los resultados generados en los análisis de los escenarios potenciales donde se aplica la metodología semí cuantitativa, se proponen las siguientes recomendaciones para la planta reformadora de naftas de la refinería de Minatitlan Ver.

Paro de Emergencia por Detección de Fuego y/o por Atmósferas Riesgosas.

En caso de riesgo por fuego y/o atmósferas riesgosas, se deberá instalar un sistema de detección y alarma de explosividad, cerca de las bombas y en dirección contraria a los vientos dominantes (de acuerdo a los criterios establecidos en la norma sobre sistemas automáticos para la detección y alarma por fuego o por atmósferas riesgosas, DG-GPASI-SI-2720), conectado a un Controlador Lógico Programable, PLC, y éste, a su vez, conectado a la Válvula

de Aislamiento de Activación Remota, VAAR (acorde a los criterios y requerimientos mínimos establecidos en la norma DG-GPASI-SI-2740).

El sistema propuesto, incluye la instalación de alarmas por alta explosividad, e interruptores activados en campo o en tablero de control. Además, se requiere que los sensores a instalar sean de doble canal, para tener mayor confiabilidad en la lectura y determinar posibles fallas en el sensor.

Para prever consecuencias posteriores, se muestra los casos en que de acuerdo al proceso, se detalla la secuencia en la que deben dispararse los equipos.

Configuración SIL1, caso A

RECIPIENTE-BOMBAS: Se requiere la instalación de interruptores conectados al PLC de la VAAR, que manden disparar a los motores de las bombas. Pero si las bombas son activadas por turbinas entonces, se requiere la instalación de válvulas solenoides, conectadas al PLC de la VAAR, que activen a las válvulas de corte rápido, que se propone sean instaladas a la entrada de la línea de vapor de las turbinas. Mostrado en Figura 6.1

Configuración SIL1, caso B

RECIPIENTE-BOMBAS-CALENTADOR: Se requiere la instalación de interruptores conectados al PLC de la VAAR, que manden disparar a los motores de las bombas. Pero, si las bombas son activadas por turbinas, entonces, se requiere la instalación de válvulas solenoides, conectadas al PLC de la VAAR, que activen a las válvulas de corte rápido, que se propone sean instaladas a la entrada de la línea de vapor de las turbinas. Y al mismo tiempo, el PLC, mande bloquear la válvula de corte rápido del suministro de gas combustible del calentador. Mostrado en Figura 6.2

Figura 6.0 Diagrama de Flujo Genérico para el Sistema Instrumentado de Seguridad SIS).

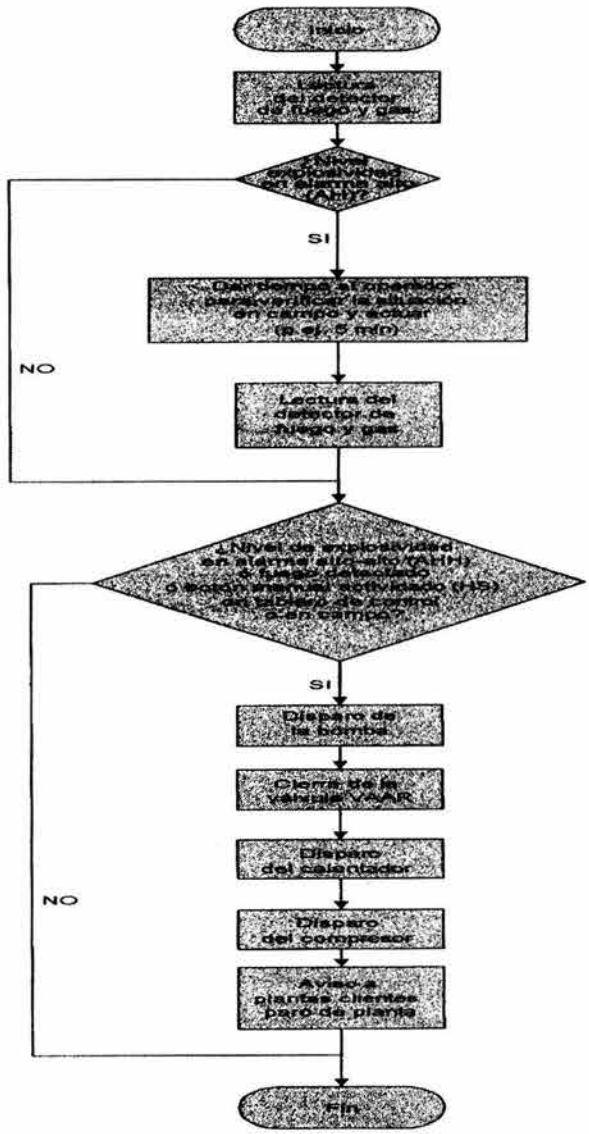


Figura 6.1 propuesta de Configuración para SIL1. Caso A

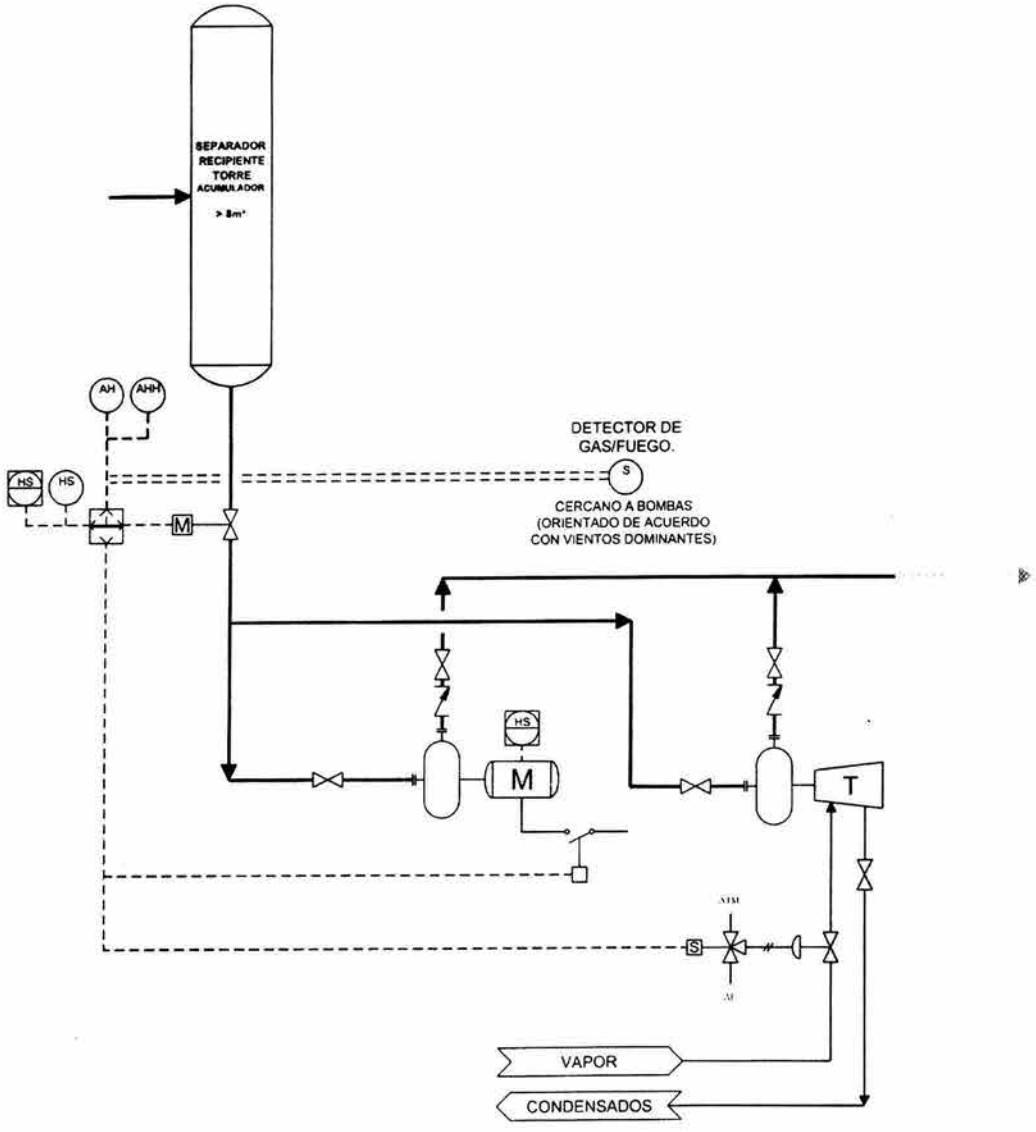
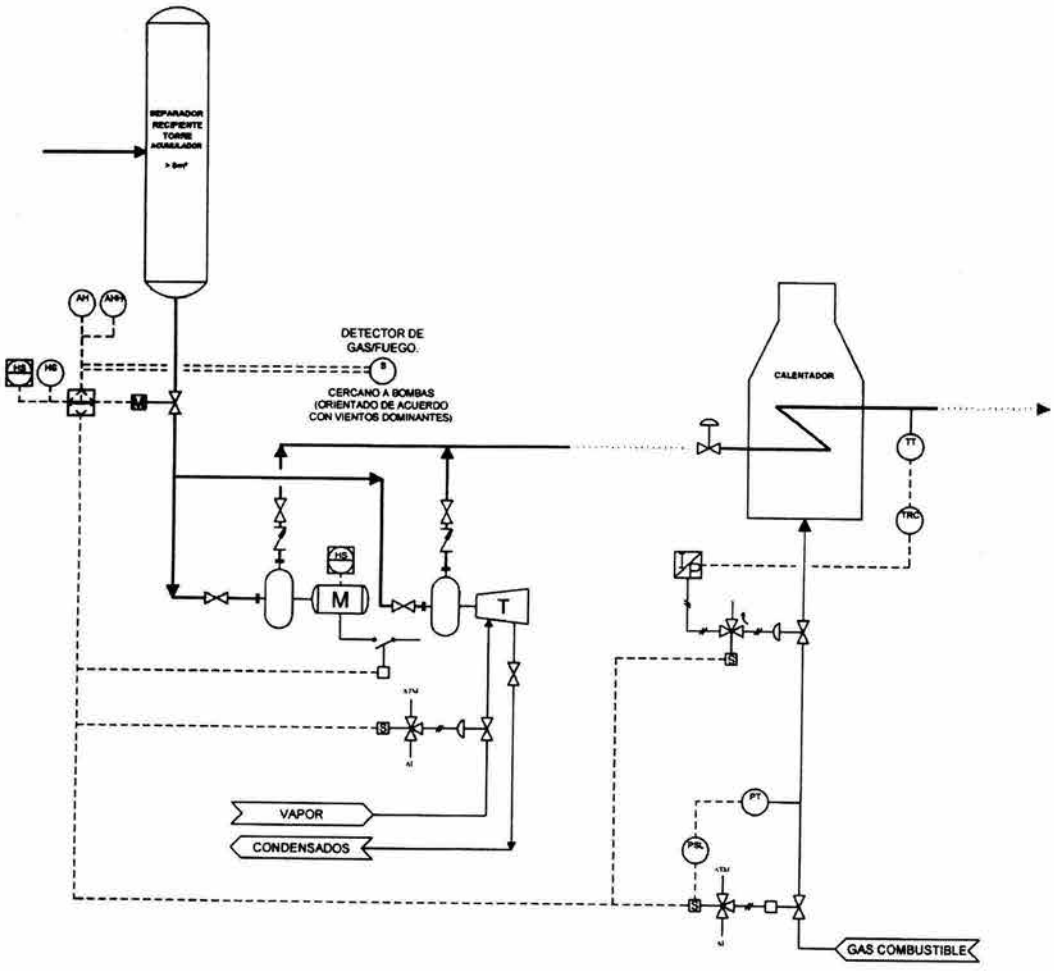


Figura 6.2 propuesta de Configuración para SIL1. Caso B



Recomendaciones para mejorar los niveles de integridad de la seguridad de diseño de los sistemas de seguridad existente [9].

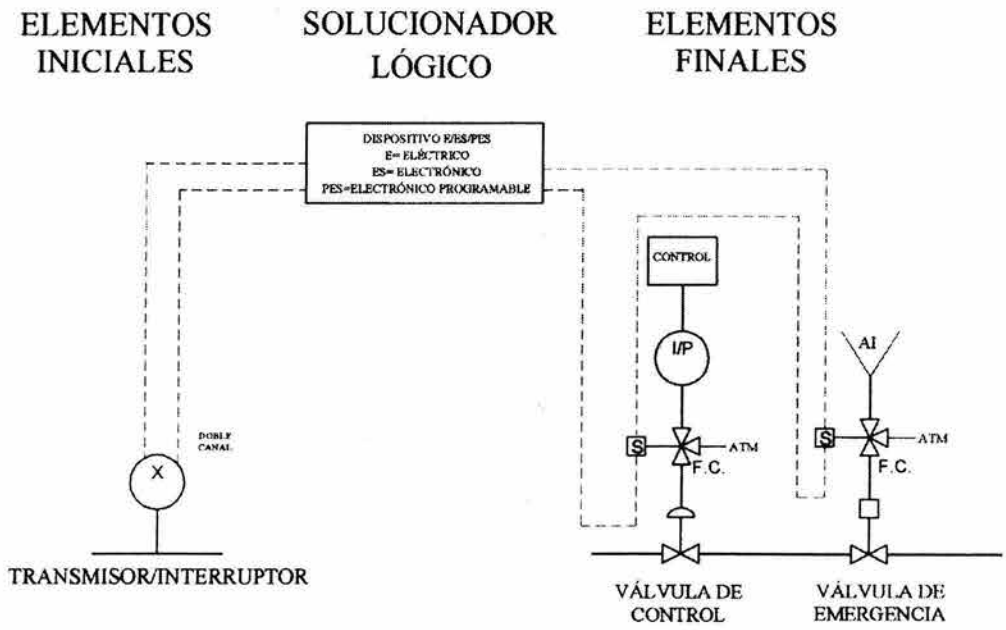
Varias observaciones pueden ser hechas en el diseño de una arquitectura genérica basadas en el diseño hipotético, (ejemplo. Sistema de canales simples, sistema de redundancias parciales,

Sistemas de redundancias completas, sistema de diversidad parcial y sistema de diversidad completa) usando diferentes combinaciones de sensores, solucionadores lógicos y elementos finales. El método cuantitativo de árbol de fallas fue aplicado para cada sistema, usando valores de tasa de falla, basada en datos históricos, donde los resultados arrojaron la siguiente información.

- El solucionador lógico, para los sistemas eléctricos/electrónicos (E/ES) y electrónicos programables (PES), está dado en órdenes de magnitud más confiables que los elementos de campo. Sin embargo, los elementos de campo determinan la confiabilidad del sistema y no la tecnología del solucionador lógico.
- Los interruptores de valores ocultos de proceso y los transmisores de flujo son menos confiables que el nivel, temperatura y transmisores de presión. Por lo tanto, los interruptores de valores ocultos de proceso no pueden ser usados en sistemas con SIL 3 y SIL 4.
- Las válvulas tienen la más baja confiabilidad. Una sola válvula simple no puede ser usada como elemento final en un sistema de paro de emergencia. (ESS).
- Un sistema de canal simple no tiene suficiente integridad para ser usado en un ESS.
- Al incrementar el sistema redundante, incrementa la integridad del sistema, pero además las causas comunes de fallas (CCFs) reducen significativamente la probabilidad de falla más alla del SIL 2.
- La incorporación de diversidades reduce las causas comunes de falla y permite mayor confiabilidad del sistema que si es lograda con redundancias idénticas.

Tomando en cuenta las observaciones de los párrafos anteriores se pueden hacer las propuestas siguientes: Arquitectura que pueden mejorar la integridad de diseño de los sistemas instrumentados de seguridad existentes de la planta reformadora de naftas.

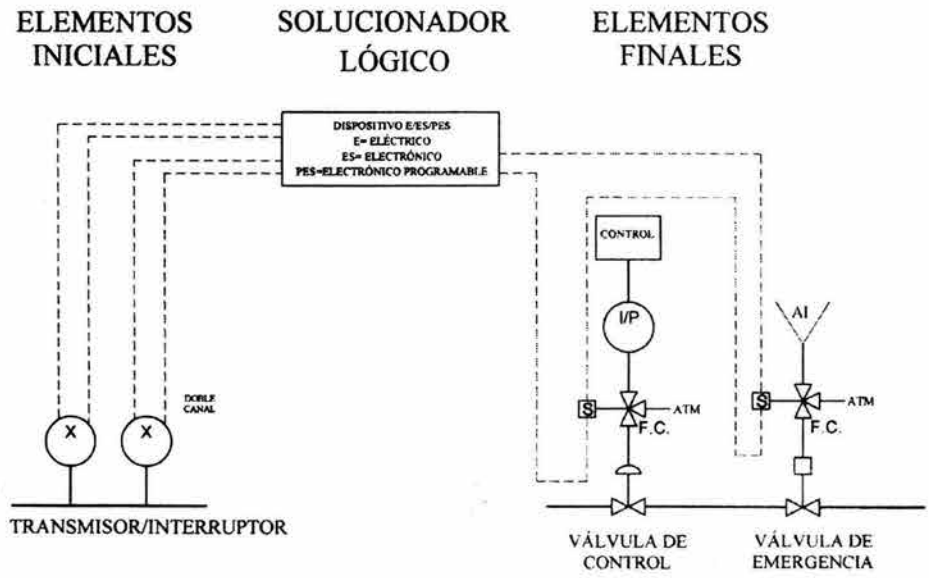
Figura 6.3 Propuesta de Arquitectura Genérica para una Configuración SIL1.



PFD's para la Configuración.

ELEMENTO FINAL	ELEMENTO INICIAL	E/ES	PES
		PFD	PFD
Válvula ESS (Sistema de Paro de Emergencia) y Válvula de Control.	Interruptor de Nivel	1.02×10^{-2}	1.02×10^{-2}
	Interruptor de Temperatura	3.03×10^{-2}	3.03×10^{-2}
	Interruptor de Presión	2.82×10^{-2}	2.82×10^{-2}
	Interruptor de Flujo	1.82×10^{-2}	1.82×10^{-2}
	Transmisor de Flujo	2.41×10^{-2}	2.37×10^{-2}

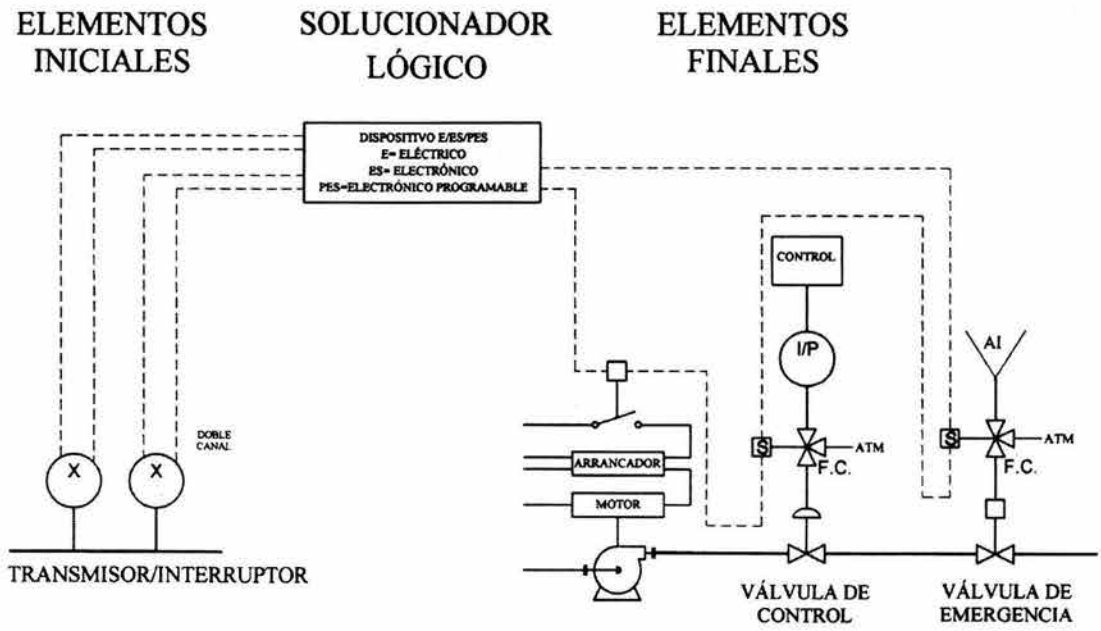
Figura 6.4 Propuesta de Arquitectura Genérica para una Configuración SIL 2.



PFD's para la Configuración.

ELEMENTOS FINALES	ELEMENTOS INICIALES	E/ES	PES
		PFD	PFD
Válvula ESS (Sistema de Paro de Emergencia). Válvula de Control.	Transmisor de Nivel	$8.33x10^{-3}$	$7.95x10^{-3}$
	Transmisor de Temperatura	$2.95x10^{-3}$	$2.56x10^{-3}$
	Transmisor de Presión	$2.95x10^{-3}$	$2.56x10^{-3}$
	2 Interruptores de Nivel	$5.64x10^{-3}$	$5.69x10^{-3}$
	2 Transmisores de Nivel	$5.44x10^{-3}$	$5.42x10^{-3}$
	2 Interruptores de Temperatura	$5.13x10^{-3}$	$5.19x10^{-3}$
	2 Transmisores de Temperatura	$1.57x10^{-3}$	$1.55x10^{-3}$
	2 Interruptores de Presión	$7.95x10^{-3}$	$8.01x10^{-3}$
	2 Transmisores de Presión	$1.57x10^{-3}$	$1.55x10^{-3}$
	2 Interruptores de Flujo	$6.58x10^{-3}$	$6.63x10^{-3}$
	2 Transmisores de Flujo	$4.20x10^{-3}$	$4.17x10^{-3}$
Válvula ESS (Sistema de Paro de Emergencia). Válvula de Control. Motor de la bomba.	2 Interruptores de Temperatura	$3.72x10^{-3}$	$3.78x10^{-3}$
	2 Interruptores de Presión	$2.86x10^{-3}$	$2.91x10^{-3}$
	2 Interruptores de Flujo	$1.48x10^{-3}$	$1.36x10^{-3}$
	2 Transmisores de Flujo	$2.78x10^{-3}$	$2.76x10^{-3}$

Figura 6.5 Propuesta de Arquitectura Genérica para una Configuración SIL 3.



PFD's para la Configuración.

ELEMENTOS FINALES	ELEMENTOS INICIALES	E/ES	PES
		PFD	PFD
Válvula ESS (Sistema de Paro de Emergencia). Válvula de Control. Motor de la bomba.	2 Interruptores de Nivel	$5.38x10^{-4}$	$5.81x10^{-4}$
	2 Transmisores de Nivel	$3.35x10^{-4}$	$3.17x10^{-4}$
	2 Transmisores de Temperatura	$1.56x10^{-4}$	$1.39x10^{-4}$
	2 Transmisores de Presión	$1.56x10^{-4}$	$1.39x10^{-4}$
Válvula ESS (Sistema de Paro de Emergencia). Válvula de Control. Motor de la bomba.	Interruptor y Transmisor de Flujo	$2.99x10^{-4}$	$3.00x10^{-4}$
	Transmisor de Flujo y Nivel	$1.13x10^{-4}$	-
	Interruptor de Temperatura y Presión	$6.71x10^{-4}$	$6.78x10^{-4}$

CAPÍTULO 7.

CONCLUSIONES

CONCLUSIONES

6.1 CONCLUSIONES

Un factor importante para la aplicación de esta metodología fue haberse apoyado en una herramienta de análisis cualitativo (HAZOP), elemento primordial que permitió identificar los escenarios potenciales de una manera más precisa.

- La metodología desarrollada en este estudio, permite identificar las capas de protección que se tienen en un escenario de riesgo y probar a su vez que es una herramienta sencilla de manejar y con resultados representativos para la evaluación del SIL de un SIS instalados en la planta reformadora de Nafta, además esta metodología requiere de menos tiempo en su aplicación que una técnica de análisis cuantitativa.
- Otra de las aplicaciones de esta metodología, es que se puede calcular la eficiencia de las capas de protección y establecer los criterios para decidir si se requieren o no de capas de protección adicional, o bien, si se tiene la necesidad de instalar un SIS; ya que se observó que en muchos de los escenarios estudiados no se tiene la condición de agregar capas de protección adicional, debido a que sólo se encontró una sobre estimación del riesgo. Además se demuestra que el nivel de riesgo disminuye en algunos escenarios mejorando las condiciones de operación, instrumentación básica y equipo del proceso.

Este tipo de análisis permite tener mejores argumentos, para decidir en que punto es estrictamente necesario instalar un SIS así como evaluar el SIL objetivo de los SIS existentes en la planta, así como justificar la instalación de válvulas de activación remota (VAAR´S) y evaluar los sistema ya existentes como es el caso de los interruptores automáticos (interlocks) de los equipos críticos. Elementos importantes para poder confrontarlos con lo propuesto por los proveedores de los sistemas instrumentados de seguridad. La utilidad de estos resultados permitirá optimizar recursos económicos destinados a la seguridad industrial.

La identificación de las capas de protección necesarias y la instalación de los SIS, permite disminuir las fallas e incidencias de accidentes en escenarios de alto riesgo potencial, (identificados previamente por los análisis HAZOP); lo cual es uno de los propósitos principales al realizar este tipo de proyectos. Con esto se valida la hipótesis propuesta en el inicio del trabajo.

Además el método puede ser empleado en otras plantas de procesos si se determinan los criterios específicos para esa industria en cuestión.

De acuerdo a datos estadísticos mencionados por PEMEX; el índice de incidentes ha aumentado en los últimos dos años; por lo tanto, es importante que estas propuestas, para reducir los riesgos, sean implementadas en las plantas, como una contribución de mejora de los niveles de confiabilidad de no accidentes en la industria petrolera.

GLOSARIO

GLOSARIO

Accidente: Cualquier acontecimiento no planeado que implica una desviación intolerable sobre las condiciones de diseño de un sistema causando daños a las personas, y/o al medio ambiente y/o a la propiedad.

Accidente menor: Es un acontecimiento no deseado que provoca daños leves a las personas, siendo necesaria la aplicación de primeros auxilios para que se incorporen en sus actividades normales.

Accidentes mayores: Es cualquier suceso que es consecuencia de un desarrollo

Incontrolable de una actividad industrial y que puede provocar una situación de gran riesgo, catástrofe o calamidad publica , inmediata o diferida para las personas, para el medio ambiente y para los bienes materiales, ya sea en el interior o exterior de las instalaciones.

Administración: Proceso consistente en planear, coordinar, ejecutar y controlar esfuerzos, organizada y sistemáticamente para lograr un objetivo.

Administración de Riesgos: Conjunto de procesos que incluye el análisis de los riesgos, la evaluación de su aceptabilidad, el establecimiento de medidas de prevención y control así como el seguimiento (auditoria) de los mismos.

Alarma: Situación indicativa de condición riesgosa, que puede desencadenar en un siniestro si no es corregida.

Análisis de Procesos: Identificación, separación y estudio realizados a cada una de las operaciones que comprenden un proceso, generalmente para evaluar la eficiencia del mismo buscando su optimización.

Análisis de riesgo: Método de evaluación de los riesgos potenciales de un proceso industrial o instalación, por identificación de los eventos indeseables que podrían conducir a la materialización de un riesgo, que incluye el mecanismo del análisis por el cual pueden ocurrir

estos eventos y usualmente, la estimación de las consecuencias. El análisis de riesgo debe formar parte desde la ingeniería del proyecto y sus resultados deben incluir el nivel de integridad de seguridad del sistema a utilizar.

Arquitectura: Es el arreglo físico y de configuración de los componentes y subsistemas de un sistema, cuando éste es digital.

Atmósfera Riesgosa: Mezcla de aire, gas (es) o vapor(es) tóxico(s) o inflamable(s), que pueden causar daño o riesgos a la salud y al medio ambiente inherente al proceso.

Causa: Son las razones por las que la falla ocurre. Una vez que se ha determinado que la falla puede tener causas plausibles, debe considerarse a ésta como algo de suma importancia. Mientras mayor número de causas puedan encontrarse, debe considerarse una mayor posibilidad de ocurrencia de la falla y se debe dar mayor atención a ésta causa.

Capas protectoras: Sistemas de protección o capas que involucran diseños de proceso especiales, equipo de proceso, procedimientos administrativos, Sistemas de Controlador Básicos del Proceso, y/ó programas para responder a inminentes riesgos. Estas respuestas pueden ser automáticas ó iniciadas por la acción humana.

Ciclo de vida de seguridad: secuencia de actividades involucradas en la implantación de sistemas instrumentados de seguridad desde el diseño conceptual hasta el desmantelamiento del mismo.

Control: Fase del proceso de Administración, que consiste en evaluar si lo programado está ocurriendo como se planeó y en su caso tomar las acciones correctivas pertinentes.

Confiabilidad: Probabilidad de que un sistema pueda desempeñar una función definida bajo condiciones especificas para un periodo de tiempo dado.

Comisionamiento: Es la verificación y confirmación de que el SIS cumple con las características especificadas en la documentación del diseño detallado y se encuentra listo para las pruebas de prearranque.

Detector: Dispositivo capaz de reconocer, mediante un elemento sensible, la presencia de alguna condición anormal preestablecida como fuego o atmósfera riesgosa, generando una señal que enviará a la unidad de control.

Demanda: Condición que requiere el sistema instrumentado de seguridad para tomar la acción de prevenir un riesgo o mitigar las consecuencias de un riesgo.

Desviación: Son las palabras guías que indican una modificación cualitativa o cuantitativa de los parámetros a analizar.

Desmantelamiento: La remoción completa de un SIS de su servicio activo.

Disparo en falso: Activación de cualquier función instrumentada de seguridad (SIF) perteneciente al SIS, sin existir una demanda real en campo.

Disponibilidad de seguridad: Fracción de tiempo en que un sistema de seguridad es capaz de desempeñar un servicio de seguridad designado cuando el proceso esta en operación, un SIS no esta disponible si se encuentra en un estado de falla (seguro o peligroso), o esta fuera para mantenimiento.

Diversidad: Uso de dispositivos y equipo con diferentes tecnologías o métodos de diseño que desempeñan una función de seguridad común, de manera que se minimicen las fallas de causa común.

Estado seguro: Estados que debe tener el equipo o proceso bajo control después de la operación apropiada del SIS.

Elemento final de control: Recibe la señal del controlador y modifica el caudal del fuido o agente de control. La válvula de control es el elemento final típico.

Emergencia: Situación derivada de un incidente/accidente que puede resultar en efectos adversos a los trabajadores, la comunidad, el ambiente y/o las instalaciones y que por su

naturaleza de riesgo, activa una serie de acciones para controlar o mitigar la magnitud de sus efectos.

Equipo intrínsecamente seguro: Instrumento que por su construcción y diseño, es incapaz de comportarse como una fuente de ignición por sus bajos valores de energía.

Escenario de Emergencia: Son los equipos o instalaciones y sus áreas y circunstancias donde puede ocurrir un accidente y que son analizados por medio de un estudio de riesgo y que se utilizan como base para determinar operaciones y recursos que deben realizar y emplear los grupos de emergencia con la finalidad de obtener el control de la situación lo más inmediato posible.

Escenario de Riesgo: Determinación de un evento hipotético en el cual se toma en consideración la ocurrencia de un accidente bajo condiciones determinadas, definiendo mediante la aplicación de modelos matemáticos y criterios acordes a las características de los procesos y/o materiales, las zonas potencialmente afectadas.

Evaluación de Riesgos: Estudios que se desarrollan para determinar y prevenir los tipos de riesgo a la salud del personal, las instalaciones y/o los ecosistemas, que se ocasionan como consecuencia de posibles incidentes y accidentes.

Explosión: Combustión súbita y violenta de una mezcla de aire u oxígeno con un gas combustible, generando gases de alta velocidad con liberación de energía que causa un incremento de presión u onda de choque.

Falla: Es la desviación de la intención original del componente, la cual se encuentra aplicando las palabras guía.

Falla de causa común: Falla, resultado de uno o más eventos, causando fallas coincidentes de dos ó más componentes separados conduciendo a la falla del SIS.

Fallas no reveladas: Fallas que pueden ser clasificadas como ocultas, encubiertas, no detectadas, latentes, entre otras.

Falla segura: Es una falla la cual no tiene potencial para poner el SIS referido a seguridad en un estado dañino o en un estado de falla para funcionar.

Falla revelada: Fallas que son clasificadas como anunciadas, detectadas, reveladas, entre otras.

Fallas sistemáticas: Fallas debido a errores (incluyendo equivocaciones y opiniones) en las actividades del ciclo de vida de seguridad, las cuales causan que el SIS falle bajo alguna combinación particular de entradas o bajo ciertas condiciones ambientales.

Frecuencia: Es el número de veces que se espera se repita u ocurra una falla .esta frecuencia será equivalente a la frecuencia mayor de cualquiera de las causas de una falla y generalmente se fija como incidencias por año.

Función de seguridad: Es una función a ser implementada por un sistema de seguridad.

Función instrumentada de seguridad (SIF): Capa de protección instrumentada independiente, cuyo propósito es llevar al proceso a un estado seguro cuando se violan condiciones predeterminadas.

Impacto: Efecto probable o cierto, positivo o negativo, directo o indirecto, reversible o irreversible, de naturaleza social, económica y ambiental que deriva de una o varias acciones con origen en las actividades industriales.

Intervalo de prueba: Intervalo de tiempo entre pruebas funcionales.

Indicador: Dato empírico o medida que revela la presencia o la intensidad de un fenómeno o variable.

Incidente: Evento no deseado, inesperado e instantáneo, que puede o no traer consecuencias al personal, a terceros ya sea en sus bienes o en sus personas, al medio ambiente, a las instalaciones y/o alteración a la actividad normal del proceso.

Indicador de alarma: Emisión audible y/o visual que informa al personal sobre la presencia de condiciones anómalas. También se entiende como el equipo físico que al activarse produce una señal sonora y/o luminosa, como puede ser: sirena, bocina, campana, teléfono, semáforo o foco de luz fija, destellante o giratoria.

Interlock (interruptor automático): Dispositivo de seguridad que es activado de manera automática por un sensor a fin de prevenir una condición riesgosa durante un proceso. En algunas situaciones también se le denomina "trinquete" o "cierre automático".

Líquido Inflamable: Líquido cuya temperatura de inflamación es menor a 37.8°C (100°F), que tiene una presión de vapor menor o igual a 2.81 kg/cm2 (2.068 mm de Hg) a 37.8°C (clase I NFPA).

Mitigación: Conjunto de acciones para disminuir las consecuencias por la ocurrencia de un accidente.

Nivel de integridad de la seguridad (SIL): Es un nivel discreto para la especificación de los requerimientos de integridad de las funciones de seguridad a ser asignados a sistemas instrumentados de seguridad. Cada nivel discreto se refiere a cierta probabilidad de que un sistema referido a seguridad realice satisfactoriamente las funciones de seguridad requeridas bajo todas las condiciones establecidas en un periodo de tiempo dado.

Peligro: Es cualquier condición química o física que tiene el potencial para causar daños a la gente, propiedades, o el medio ambiente, "propiedad inherente de un agente químico, biológico o físico".

Probabilidad de falla en demanda (PFD): Valor que indica la probabilidad de que un SIS falle para responder a una demanda.

Prueba: Verificación operativa por simulación del funcionamiento de equipos o sistema completo, para confirmar que su operación real corresponderá con lo previsto.

Redundancia: Uso de múltiples elementos o sistemas para desarrollar la misma función, ésta puede ser implementada por elementos idénticos o por elementos diversos.

Redundancia diversa: La redundancia diversa, aplica diferentes tecnologías, diseños, manufactura, programas de cómputo (software), etc. Con la finalidad de reducir la influencia de fallas de causa común. La redundancia diversa debe emplearse únicamente para alcanzar el (SIL) requerido, este tipo de redundancia no debe emplearse cuando su aplicación resulte en el uso de componentes de baja confiabilidad.

Relé: Relevador, Tecnología usada en sistemas instrumentados de seguridad basada en señales lógicas discretas (encendido/apagado).

PLC: Instrumento capaz de ser configurado para llevar a cabo el control de las funciones del sistema, por interrelación de las señales de detección, así como para establecer la comunicación con sistemas complementarios y el diagnostico del mismo. Este instrumento debe cumplir con parámetros internacionales (IEC-61508) ó equivalente, que garantice su confiabilidad y disponibilidad en operación.

Riesgo: Una medida de la perdida económica o daños humanos en términos de la probabilidad de incidentes y la magnitud de la perdida o daño. Un peligro puede ser la causa o contribuir a un riego, pero no es un riesgo per se. La palabra perdida significa un derroche de recursos innecesarios.

Riesgo potencial: Es el riesgo de un escenario, sin considerar las capas de protección existentes, evaluadas cualitativamente, mediante una matriz de riesgo.

Riesgo Mayor: Probabilidad de ocurrencia de un accidente, que significaría el mayor daño por sus consecuencias, por el número de personas afectadas, por la magnitud de los daños materiales, afectación al ambiente, o por la combinación de éstos.

Sensor: Es un dispositivo físico que al igual que los sentidos humanos, detecta el valor de las variables del proceso siguiendo principios físicos o químicos conocidos en la terminología de instrumentación a estos dispositivos se les llama elementos primarios de medición como es el caso de transmisores, interruptores de proceso, interruptores de posición, entre otros.

Sistemas automáticos de alarma por detección de fuego y/o por atmósferas riesgosas (SAAFAR): Sistema automático integrado por diferentes elementos eléctricos, electrónicos, mecánicos y electrónicos programables, que permite monitorear, señalizar y ubicar la existencia de condiciones anormales de riesgo no tolerable, a través de la activación de indicadores de alarma, ya sea por medios visuales /audibles y/o de presentación digital, siendo capaz de historizar los eventos.

SIS (Safety Instrumented Systems): Es un sistema compuesto por sensores, solucionadotes lógicos y elementos finales de control que tiene el propósito de llevar al proceso a un estado seguro cuando se han violado condiciones predeterminadas. Otros términos comúnmente usados son sistemas de paro de emergencia sistema de paro de seguridad.

Sistemas de Controlador Básico del Proceso (BPCS): Es el sistema que responde a señales de entrada del equipo bajo control y/ó de un operario, y señales de salida generando, que el equipo bajo control opere de la manera deseada.

Solucionador lógico: Dispositivo del sistema instrumentado de seguridad constituido por un sistema eléctrico programable/ eléctrico/electrónico, que ejecutan las aplicaciones lógicas del sistema, estos sistemas incluyen módulos de entrada y salida.

Sistema de supresión de fuego: Sistema de extinción de fuego a base de agente limpio o de aspersión de agua o espuma, conformado por tablero de supresión, cabezal de control, cabezal de descarga, tubería, boquillas, cilindros, agente limpio, detectores, alarma y letreros de señalización.

Tasa de demanda: La frecuencia con el cual un SIS es requerido para realizar su función.

Tasa de falla: Es la tasa promedio a la cual se espera que ocurra fallas de los componentes del SIS.

Tablero de Control Contraincendio: Equipo formado por dispositivos, circuitos, interruptores y otros elementos eléctricos, electrónicos y electromecánicos, que interaccionan las señales de entrada provenientes de los detectores y estaciones manuales de alarma, generando señales que activan las alarmas. Pueden hacer funcionar los sistemas automáticos para el combate de incidentes no tolerables, además de estar en posibilidad de transmitir la información recabada a los sistemas que controlan el proceso de una instalación industrial y a otros sistemas relacionados con la seguridad.

Temperatura de ignición: Es la temperatura menor a la que una sustancia sólida, líquida o gaseosa, entra en combustión y puede mantenerla.

Transmisores: Proporciona señales que indican el estado actual de la variable que se ésta mediendo.

Tiempo medio de reparación: Es la tasa promedio a la cual se espera que ocurra fallas de los componentes del SIS.

Tiempo medio de disparo en falso: Tiempo medio para que se presente una falla del SIS que resulte en un paro en falso del proceso ó del equipo bajo control.

APÉNDICE

APÉNDICE A

Tablas de Probabilidad de Falla en Demanda, PFD.

"Análisis y Reducción de Riesgos en la Industria Química". Fundación Mapfre J. M. Santamaría Ramiro. P. A. Braña.

Probabilidad	Acción del operador
0.04	No observa el indicador, o lo observa pero no emprende ninguna acción, aunque debería hacerlo.
0.03	No percibe la alarma, o la percibe pero no emprende ninguna acción, aunque debería hacerlo.
0.001	No bloquea una tubería, como estaba previsto en una parada de emergencia.
0.005	No bloquea una tubería, como estaba previsto en una parada de emergencia.
0.0025	Se equivoca al accionar las válvulas cuando se intercambia un conjunto de dos bombas (se para la que está funcionando, se arranca la que estaba en espera).
0.01	Para manual de una bomba sin tomar acciones para bloquear la tubería.
0.003	Error general de comisión (por ejemplo, leer equivocadamente un rotulo y como consecuencia seleccionar el interruptor equivocado).
0.03	Errores de operación aritméticas simples, realizadas manualmente y comprobadas rutinariamente, sin repetir el calcúlo en otro papel.
$\cong 1.0$	El operador no toma la decisión correcta, durante los primeros sesenta segundos en una situación de muy alto estrés.
0.9	El operador no toma la decisión correcta, durante los primeros cinco minutos en una situación de muy alto estrés.
0.1	El operador no toma la decisión correcta, durante los primeros treinta minutos en una situación de muy alto estrés.

Referencia "LOPA (layers of protection analysis): simplified process risk assessment", CCPS, AIChE, 2001

Independent Protection Layer	Minimum PFOD
Basic Process Control Systems	
Automatic control loop (If independent of the initiating event)	10^{-1}
Human Intervention	
Manual response in field with more than 10 minutes available for response (If sensor/alarm is independent of the initiating event and other IPLs, and operator training included required response)	10^{-1}
Manual response in field with more than 40 minutes available for response (If sensor/alarm is an independent SIF and operator training included required response)	10^{-2}
Manual response to abnormal readings collected regularly on a checklist, and the checklist is used in practice (operator training requires use of checklist; use of checklist audited > 2/year)	10^{-1}
Passive Devices	
Secondary containment such as a dike or underground drainage system (If good administrative control over drain valves exists)	10^{-2}
Relief Devices	
Spring-loaded relief valve or rupture disks in clean service	10^{-3}
Safety Interlocks (per ISA S84.01 Standard)	
SIL (class) 3 interlock (Provided independent of other interlocks)	10^{-3}
SIL (class) 2 interlock (Provided independent of other interlocks)	10^{-2}
SIL (class) 1 interlock (Provided independent of other interlocks)	10^{-1}

EQUIPOS/INSTRUMENTOS/ SISTEMAS	TASA DE FALLAS (FRECUENCIAS) FRECUEN. BAJA	FRECUEN. TIPICA	FRECUEN. ALTA	PROBALIDAD DE FALLA EN DEMANDA PROBABIL. BAJA	PROBABIL. TIPICA	PROBABIL. ALTA
Motor AC	2.00E-04	1.50E-01	4.00E-01	2.00E-04	1.39E-01	3.30E-01
Inversor	1.00E-02	2.50E-01	1.00E+00	9.95E-03	2.21E-01	6.32E-01
Transformador de potencia	1.00E-03	2.00E-02	7.00E-02	1.00E-03	1.98E-02	6.76E-02
Generador de diesel de	1.50E+00	2.00E+01	6.00E+01	7.77E-01	1.00E+00	1.00E+00
Analizador (AR)	6.00E-01		4.00E+01	4.51E-01		1.00E+00
Transmisor de flujo neumático	1.80E-02	1.00E+00	4.00E+00	1.78E-02	6.32E-01	9.82E-01
Transmisor de nivel neumático	2.00E-02	8.00E-01	3.00E+00	1.98E-02	5.51E-01	9.50E-01
Transmisor de presión	1.80E-03	8.00E-01	3.50E+00	1.80E-03	5.51E-01	9.70E-01
Transmisor de temperatura	1.40E-02	8.00E-01	3.50E+00	1.39E-02	5.51E-01	9.70E-01
PDT en la industria en general	8.00E-03	5.50E-01	2.00E+00	7.97E-03	4.23E-01	8.65E-01
PDT en condiciones	3.00E-02	1.80E+00	8.00E+00	2.96E-02	8.35E-01	1.00E+00
Switch de flujo eléctrico	9.00E-03	3.20E-01	1.50E+00	8.96E-03	2.74E-01	7.77E-01
Válvula de seguridad (PSV)	2.00E-03	1.20E-02	4.00E-02	2.00E-03	1.19E-02	3.92E-02
Switch de nivel eléctrico	8.50E-03	1.00E-02	2.00E-02	8.46E-03	9.95E-03	1.98E-02
Switch de presión eléctrico	4.00E-03	4.50E-01	1.80E+00	3.99E-03	3.62E-01	8.35E-01
Sistema de polvo contra	2.00E-04	1.00E-02	5.00E-02	2.00E-04	9.95E-03	4.88E-02
Switch de temperatura eléctrico	8.00E-04	2.00E-02	9.00E-02	8.00E-04	1.98E-02	8.61E-02
Sistema de agua contra	1.00E-03	8.00E-02	3.50E-01	1.00E-03	7.69E-02	2.95E-01
Detector de flama	3.00E-04	4.00E+00	1.80E+01	3.00E-04	9.82E-01	1.00E+00
Detector de fuego	1.00E-04	8.50E-03	3.00E-02	1.00E-04	8.46E-03	2.96E-02
Convertidor I/P	9.00E-03	5.50E-01	2.50E+00	8.96E-03	4.23E-01	9.18E-01
Válvula actuada por solenoide	6.00E-03	4.00E-01	1.90E+00	5.98E-03	3.30E-01	8.50E-01
Controlador de proceso	2.00E-02	6.00E-02	2.50E+00	1.98E-02	5.82E-02	9.18E-01
Controlador electrónico	3.00E-02	1.60E+00	7.00E+00	2.96E-02	7.98E-01	9.99E-01

Referencia: F. J. Master.

EQUIPOS/INSTRUMENTOS/ SISTEMAS	TASA DE FALLAS (FRECUENCIAS) FRECUEN. BAJA	FRECUEN. TIPICA	FRECUEN. ALTA	PROBALIDAD DE FALLA EN DEMANDA PROBABIL. BAJA	PROBABIL. TIPICA	PROBABIL. ALTA
Recipiente atmosférico	1.00E-03	8.00E-03	3.00E-02	1.00E-03	7.97E-03	2.96E-02
Controlador neumático	6.00E-03	3.80E-01	1.80E+00	5.98E-03	3.16E-01	8.35E-01
Recipiente presurizado	1.00E-06	8.00E-05	4.00E-04	1.00E-06	8.00E-05	4.00E-04
Anunciador (alarmas)	2.00E-04	6.00E-04	2.00E-02	2.00E-04	6.00E-04	1.98E-02
Válvula de control	2.50E-03	3.00E-02	1.00E-01	2.50E-03	2.96E-02	9.52E-02
Registrador	4.00E-03	2.00E-01	9.00E-01	3.99E-03	1.81E-01	5.93E-01
Válvula motorizada	2.00E-03	1.00E-02	3.00E-02	2.00E-03	9.95E-03	2.96E-02
Intercambiador de calor de tubos y coraza	1.00E-04	3.00E-01	1.60E+00	1.00E-04	2.59E-01	7.98E-01
Válvula manuale	1.00E-04	1.00E-03	4.00E-03	1.00E-04	1.00E-03	3.99E-03
Compresor con motor eléctrico	2.50E-01	2.30E+01	9.00E+01	2.21E-01	1.00E+00	1.00E+00
Tramo de un tramo de tubo	6.00E-06	2.00E-04	1.00E-03	6.00E-06	2.00E-04	1.00E-03
Conexión de tubería	9.50E-05	4.00E-04	2.00E-02	9.50E-05	4.00E-04	1.98E-02
Bomba centrífuga accionada	4.00E-01	2.50E+00	9.00E+00	3.30E-01	9.18E-01	1.00E+00
Bomba centrífuga accionada por motor (funcionamiento contínuo)	6.50E-03	9.00E-01	4.00E+00	6.48E-03	5.93E-01	9.82E-01
Bomba centrífuga accionada por turbina	8.00E-02	8.00E-01	2.50E+00	7.69E-02	5.51E-01	9.18E-01
Válvula check	4.00E-04	3.00E-02	1.00E-01	4.00E-04	2.96E-02	9.52E-02

	TASA DE FALLAS (FRECUENCIAS)			PROBALIDAD DE FALLA EN DEM.		
EQUIPOS/INSTRUMENTOS/	FRECUEN.	FRECUEN.	FRECUEN.	PROBABIL.	PROBABIL.	PROBABIL.
SISTEMAS	BAJA	TIPICA	ALTA	BAJA	TIPICA	ALTA
Acoplamientos	5.69E-02		5.26E-01	5.53E-02		4.09E-01
Acoplamientos de engrane	7.45E-03		5.26E-01	7.42E-03		4.09E-01
Cilindros hidráulicos	5.69E-05		2.19E-03	5.69E-05		2.19E-03
Juntas hidráulicas	4.38E-03		2.19E-02	4.37E-03		2.17E-02
Filtro de aceite	7.45E-02		5.26E-01	7.18E-02		4.09E-01
Engranes	2.63E-02		3.50E-01	2.60E-02		2.95E-01
Impulsores de bombas	6.13E-03		6.57E-02	6.11E-03		6.36E-02
Juntas mecánicas	8.76E-04		6.57E-03	8.76E-04		6.55E-03
Liner, recip. comp. cyl.	4.38E-02		5.26E-01	4.29E-02		4.09E-01
Packings, recip. comp. rod.	4.38E-01		3.50E+00	3.55E-01		9.70E-01
Máquinas de pistones	6.13E-02		4.82E-01	5.95E-02		3.82E-01
Sellos mecánicos	7.45E-02		6.13E-01	7.18E-02		4.58E-01
Flechas de bombas	4.38E-01		3.94E+00	3.55E-01		9.81E-01
Soportes para vibración	4.38E-02		3.07E-01	4.29E-02		2.64E-01
Valves, recip. comp.	6.13E-02		5.69E-01	5.95E-02		4.34E-01
Lubricadores de bombas	2.63E+00		1.31E+01	9.28E-01		1.00E+00
Corta circuitos	6.13E-03		2.19E-01	6.11E-03		1.97E-01
Bombas centrífugas	5.25E-02		7.44E+00	5.11E-02		9.99E-01
Bombas centrífugas	5.25E-02		7.44E-01	5.11E-02		5.25E-01
Transformadores	4.82E-04		6.13E-01	4.82E-04		4.58E-01
Controladores neumáticos	8.76E-03		6.57E+00	8.72E-03		9.99E-01
Controladores de estado	5.25E-02		4.82E-01	5.11E-02		3.82E-01
Válvulas de control	3.50E-02		6.57E-01	3.44E-02		4.82E-01
Válvulas motorizadas	8.76E-03		5.25E-01	8.72E-03		4.08E-01
Válvulas selenoide	8.76E-03		2.63E-01	8.72E-03		2.31E-01

EQUIPOS/INSTRUMENTOS/ SISTEMAS	TASA DE FALLAS (FRECUENCIAS) FRECUEN. BAJA	FRECUEN. TIPICA	FRECUEN. ALTA	PROBALIDAD DE FALLA EN DEM. PROBABIL. BAJA	PROBABIL. TIPICA	PROBABIL. ALTA
Transductores	1.75E-01		7.88E-01	1.61E-01		5.45E-01
Transmisores	6.54E-03		8.76E-02	6.52E-03		8.39E-02
Indicadores de temperatura	3.94E-03		5.69E-02	3.93E-03		5.53E-02
Indicadores de presión	8.76E-03		7.88E-02	8.72E-03		7.58E-02
Instrumentación de flujo	8.76E-04		8.76E-02	8.76E-04		8.39E-02
Instrumentación de nivel	3.50E-02		6.57E-01	3.44E-02		4.82E-01
Partes electromecánicas	8.76E-03		8.76E-01	8.72E-03		5.84E-01
Hervidores y condensadores	3.50E-03		7.88E-01	3.49E-03		5.45E-01
Recipientes a presión	2.63E-04		7.01E-03	2.63E-04		6.99E-03
Filtros y strainers	5.69E-05		2.63E-03	5.69E-05		2.63E-03
Válvulas check	7.45E-03		8.76E-02	7.42E-03		8.39E-02
Válvulas de relevo	8.76E-03		8.76E-02	8.72E-03		8.39E-02
Líquido refrigerante	4.38E-01		8.76E-01	3.55E-01		5.84E-01
Refrigerante-lubricante de compresores de tornillo	3.94E-01		8.76E-01	3.26E-01		5.84E-01
Aceites lubricantes y minerales	5.69E-01		3.94E+00	4.34E-01		9.81E-01
Grasas	3.94E-01		2.19E+00	3.26E-01		8.88E-01

Referencia." process Equipment Reliability Data", CCPS, AIChE, 1989.

Referencia."Process Equipment Reliability Data", CCPS, AIChE, 1989.

		Fallas por cada millon de horas			Frecuencia (fallas/año)			Tiempo promedio entre fallas (años)			Orden de magnitud			Frecuencia de evento Inicial (FI)		
Equipo	modo de falla	Mínimo	Promedio	Máximo	Mínimo	Promedio	Máximo	Mínimo	Promedio	Máximo	Mínimo	Promedio	Máximo	Mínimo	Promedio	Máximo
Motor electrico AC con protecciones	catastrofico:sin especificar	0,0222	15,8	46,7	0,000194	0,138152	0,409092	5155	7	2	-4,0	-1,0	-0,5	3,0	6,0	6,5
Motor electrico AC con protecciones(fallas por 10^3 demandas)	catastrofico:sin especificar	0,00448	0,0247	0,0685	0,000039	0,000216	0,0006	25641	4630	1667	-4,5	-4,0	-3,5	2,5	3,0	3,5
Motor eléctrico AC Inducción	catastrofico:sin especificar	0,311	3,2	10,5	0,002724	0,028032	0,09198	367	36	11	-3,0	-2,0	-1,5	4,0	5,0	5,5
Motor eléctrico AC Inducción(fallas por 10^3 demandas)	catastrofico:sin especificar	0,00448	0,0247	0,0685	0,000039	0,000216	0,0006	25641	4630	1667	-4,5	-4,0	-3,5	2,5	3,0	3,5
Motor eléctrico DC	catastrofico: sin especificar	7,91	22,6	47,6	0,068292	0,19873	0,416976	14	5	2	-1,5	-1,0	-0,5	5,5	6,0	6,5
Batería - Acido/plomo	catastrofico:sin potencia	0,379	2,65	6,42	0,00332	0,01974	0,056239	301	51	18	-2,5	-2,0	-1,5	4,5	5,0	5,5
Batería - Niquel/cadmio	catastrofico:sin especificar	0,22	0,261	0,285	0,001927	0,002199	0,002497	519	456	400	-3,0	-3,0	-3,0	4,0	4,0	4,0
Cargador de baterías	catastrofico:sin potencia electrica	0,284	7,0	28,5	0,002486	0,060536	0,24966	402	16	4	-3,0	-1,5	-1,0	4,0	5,5	6,0
Interruptores AC	catastrofico:falsa operación	0,162	1,73	5,79	0,001419	0,015151	0,05072	705	66	20	-3,0	-2,0	-1,5	4,0	5,0	5,5
Interruptores DC	catastrofico:falsa operación	0,0348	3,8	14,4	0,000305	0,033288	0,126144	3279	30	8	-4,0	-1,5	-1,0	3,0	5,5	6,0
Inversores	catastrofico:sin potencia	1,04	28,7	116	0,00911	0,251412	1	110	4	1	-2,5	-1,0	0,0	4,5	6,0	7,0
Fusibles	catastrofico:sin especificar	0,0265	0,624	2,36	0,000232	0,005554	0,020674	4310	180	48	-4,0	-2,5	-2,0	3,0	5,5	5,0
Relés de protección	catastrofico:sin especificar	1,79	1,91	2,04	0,01568	0,016732	0,01787	64	60	56	-2,0	-2,0	-2,0	5,0	5,0	5,0
Transformadores de potencia	catastrofico:sin especificar	0,125	2,53	9,26	0,001095	0,022169	0,081118	913	45	12	-3,0	-2,0	-1,5	4,0	5,5	5,5
Rectificadores	catastrofico:sin potencia	0,357	1,07	2,31	0,003127	0,009371	0,020236	320	107	49	-3,0	-2,0	-2,0	4,0	4,5	5,0
Generador diesel de emergencia(MO=Standby)	catastrofico:falla al funcionar	172	2250	7710	2	20	68	0,5	0,05	0,01	0,0	1,0	1,5	7,0	8,0	8,5
Analizadores	catastrofico:sin especificar	6,87	2300	4800	0,060181	20	42	17	0,05	0,02	-1,5	1,0	1,5	5,5	7,0	8,5
Transmisor electronico de nivel - capacitancia	catastrofico:sin especificar	0,438	11,1	97,1	0,003819	0,096879	0,850598	262	10	1	-2,5	-1,0	-0,5	4,5	6,0	6,5
Transmisor de flujo neumático	catastrofico:sin especificar	1,93	107	439	0,016907	0,95484	4	59	1	0,25	-2,0	0,0	0,5	5,0	6,5	7,5
Transmisor de flujo neumático - presión diferencial	catastrofico(incluye control equivocado):sin especificacion	2,03	116	486	0,017783	1	4	56	1	0,25	-2,0	0,0	0,5	5,0	7,0	7,5
Transmisor de flujo neumático - area variable	catastrofico:sin especificar	1,59	84,3	373	0,013928	0,738359	3	72	1	0,33	-2,0	-0,5	0,0	5,0	6,5	7,0
Transmisor de nivel neumático	catastrofico:sin especificar	2,32	141	573	0,020323	1	5	49	1	0,2	-2,0	0,0	0,5	5,0	7,0	7,5
Transmisor de nivel neumático - presión diferencial	catastrofico:sin especificar	2,18	99,4	417	0,019097	0,870744	4	52	1	0,25	-2,0	-0,5	0,5	5,0	6,5	7,5
Transmisor de nivel neumático - flotador	catastrofico:sin especificar	3,25	187	723	0,02847	2	6	35	0,5	0,17	-2,0	0,0	0,5	5,0	7,0	7,5
Transmisor de presión neumático	catastrofico:sin especificar	0,159	91,9	381	0,001393	0,799788	3	718	1	0,33	-3,0	-0,5	0,0	4,0	6,5	7,0
Transmisor de temperatura	catastrofico:sin especificar	1,68	97	375	0,014717	0,84972	3	68	1	0,33	-2,0	-0,5	0,0	5,0	6,5	7,0
Transmisor de presión diferencial - industrial	catastrofico:sin especificar	1,01	58,8	254	0,008848	0,514888	2	113	2	0,5	-2,5	-0,5	0,0	4,5	6,0	7,0
Transmisor de presión diferencial - condiciones de operación severas	catastrofico:sin especificar	3,79	718	843	0,0332	2	7	30	0,5	0,14	-1,5	0,0	0,5	5,5	7,0	7,5
Switches - Flujo eléctrico-condiciones de operación severas	catastrofico:sin especificar	0,917	29,6	101	0,008033	0,259766	0,88476	124	4	1	-2,5	-1,0	-0,5	4,5	6,0	6,5
Switches- Flujo electrico-condiciones de operación severa	catastrofico:funcionando sin señal	0,378	0,89	1,61	0,003311	0,007634	0,014104		133	71		-2,5	-2,0		4,5	5,0
Switches- Flujo electrico-condiciones de operación severa	catastrofico:falla al funcionar con señal	0,165	4,2	15,7	0,001445	0,036792	0,137532		27	7		-1,5	-1,0		5,5	6,0
Switches - Nivel eléctrico	catastrofico:sin especificar	0,737	3,74	3,33	0,006456	0,015242	0,029171	155	66	34	-2,5	-2,0	-2,0	4,5	6,0	6,0
Switches - Nivel eléctrico	catastrofico:funcionando sin señal	0,152	0,728	2,65	0,001332	0,008103	0,023214		123	43		-2,5	-2,0		4,5	5,0
Switches - Nivel eléctrico	catastrofico:falla al funcionar con señal	0,0702	0,17	0,33	0,000615	0,001489	0,002891		672	346		-3,0	-3,0		5,0	4,0
Switches - Nivel eléctrico	degradado:sin especificar	0,375	1,7	4,4	0,003285	0,014892	0,038544		67	26		-2,0	-1,5		5,0	5,5
Switches - Presión eléctrica	catastrofico:sin especificar	0,525	46,9	192	0,004599	0,434496	2	217	2	0,5	-2,5	-0,5	0,0	4,5	6,5	7,0
Switches - Presión eléctrica	catastrofico:funcionando sin señal	0,00122	0,07	0,271	0,000011	0,000619	0,002374		1631	421		-4,0	-3,0		6,5	4,0
Switches - Presión eléctrica	catastrofico:falla al funcionar con señal	0,00809	0,4	1,55	0,000071	0,003504	0,013578		285	74		-2,5	-2,0		4,5	5,0
Switches - Temperatura eléctrica	catastrofico:sin especificar	0,102	2,26	10,1	0,000894	0,019873	0,088476	1119	50	11	-3,5	-2,0	-1,5	3,5	5,0	5,5
Switches - Temperatura eléctrica	catastrofico:funcionando sin señal	0,107	0,53	4,69	0,000937	0,019182	0,041084		52	24		-2,0	-1,5		5,0	5,5
Switches - Temperatura eléctrica	catastrofico:falla al funcionar con señal															
Switches - Velocidad eléctrica	catastrofico:sin especificar	0,285	0,48	0,742	0,002497	0,004205	0,0065	400	238	154	-3,0	-2,5	-2,5	4,0	4,5	4,5
Switches - Velocidad eléctrica	catastrofico:funcionando sin señal	0,02	0,15	0,455	0,000175	0,001314	0,003986		761	251		-3,0	-2,5		4,5	4,5
Switches - Velocidad eléctrica	catastrofico:falla al funcionar con señal	0,541	0,57	0,6	0,004739	0,004993	0,005256		200	190		-2,5	-2,5		4,5	4,5
Switches - Flujo neumático	catastrofico:sin especificar	1,64	4,1	7,8	0,014366	0,03594	0,068328	70	28	15	-2,0	-1,5	-1,5	5,0	5,5	5,5
Switches - Flujo neumatico	catastrofico:funcionando sin señal	0,027	0,86	2,46	0,000237	0,007582	0,02155		132	46		-2,5	-2,0		4,5	5,0
Switches - Flujo neumático	degradado:funcionando a un nivel de señal irregular	0,15	1,5	4,1	0,001314	0,013388	0,035918		68	28		-2,0	-1,5		5,0	5,5
Switches - Nivel neumático	catastrofico:sin especificar	0,0972	0,62	1,8	0,000851	0,005431	0,015768	1175	184	63	-3,5	-2,5	-2,0	3,5	5,5	5,0
Switches - Nivel neumático	catastrofico:falla al funcionar con señal	0,0484	0,54	1,8	0,000424	0,00473	0,015768		211	63		-2,5	-2,0		5,5	5,0
Switches - Nivel neumático	degradado funcionando a un nivel de señal irregular	0,375	1,7	4,4	0,003285	0,014892	0,038544		67	26		-2,0	-1,5		5,0	5,5

Switches - Presión neumática	catastrofico:funcionando sin señal	0,0515	1,7	6	0,000451	0,014892	0,05256		97	19		2,0	-1,5		5,0	5,5
Switches - Presión neumática	catastrofico:falla al funcionar con señal	0,11	1,7	6	0,000964	0,014892	0,05256		97	19		2,0	-1,5		5,0	5,5
Switches - Presión neumática	degradado:funcionando con un nivel de señal irregular	11,8	18	26	0,103368	0,15768	0,22776		6	4		1,0	-1,0		5,0	6,0
Switches - Temperatura neumática	catastrofico:sin especificar	1,09	5	13	0,009548	0,04438	0,11388	105	22	9	-2,5	1,5	-1,0	4,5	7,0	6,0
Switches - Temperatura neumática	degradado:sin especificar	0,61	3	8	0,005344	0,02628	0,07008		38	14		2,0	-1,5		5,0	5,5
Detectores de flama	catastrofico:sin especificar	0,053	432	1760	0,000464	4	15	2155	0,02	0,07	-3,5	0,5	1,0	3,5	5,5	8,0
Indicadores de temperatura - Pirómetro de radiación	catastrofico:sin especificar	4,31	245	959	0,037756	2	6	26	0,5	0,13	-1,5	0,0	0,5	5,5	7,0	7,5
Transductores - Corriente a neumático	catastrofico:sin especificar	1,08	62,8	243	0,009461	0,550129	2	106	4	0,5	-2,5	0,5	0,0	4,5	6,5	7,0
Controladores	catastrofico:sin especificar	2,43	66,8	260	0,021287	0,602655	2	47	2	0,5	-2,0	0,5	0,0	5,0	6,5	7,0
Controladores electronic en tablero (un lazo)	catastrofico:sin especificar	3,56	205	793	0,031188	2	7	32	0,5	0,14	-2,0	0,5	0,5	6,0	7,0	7,5
Controladores neumático en tablero (un lazo)	catastrofico:sin especificar	0,754	43,4	168	0,006605	0,380154	1	151	3	1	-2,5	0,5	0,0	4,5	6,5	7,0
Anunciadores	catastrofico:sin especificar	0,0272	0,77	2,9	0,000238	0,006745	0,025404	4202	119	39	-4,0	2,5	-2,0	3,0	5,5	5,0
Registradores	catastrofico:sin especificar	0,436	25,1	97,1	0,003819	0,219876	0,850596	262	8	1	-2,5	1,0	-0,5	4,5	6,5	6,5
Módulos neumáticos computacionales	catastrofico:sin especificar	0,337	19,4	75	0,002952	0,169944	0,657	339	10	2	-3,0	1,0	-0,5	4,0	6,0	6,5
Heat transfer devices - Non Fired indirect contact - Tubed Baffled	catastrofico:sin especificar	0,0173	31,1	131	0,000152	0,272456	1	6579	1	1	-4,0	1,0	0,0	3,0	6,0	7,0
Heat transfer devices - Non Fired indirect contact - Tubed Baffled	catastrofico:leakage>1/4"	1,62	15,8	91,3	0,014191	0,229908	0,799788	70	2	1	-2,0	1,0	-0,5	5,0	6,0	6,5
Piping systems - metal straight selections	catastrofico:sin especificar	0,000485	0,0268	0,104	0,000004	0,000235	0,000911	250000	7692	1098	-5,5	2,0	-3,5	1,5	3,5	3,5
Piping systems - metal connections	catastrofico:>10% area de flujo	0,0099	0,57	2,2	0,000087	0,004913	0,019272	11494	354	52	-4,5	1,5	-2,0	2,5	5,0	5,0
Piping systems - Lined pipe - straight sections	catastrofico:sin especificacion	0,00743	0,412	1,71	0,000065	0,003672	0,01498	15385	474	67	-4,5	1,5	-2,0	2,5	5,0	5,0
Piping systems - Rigid Plastic - Straight sections	catastrofico:ruptura	0,0154	0,855	3,42	0,000135	0,007563	0,029959	7407	228	33	-4,0	1,5	-2,0	3,0	5,0	5,0
Hoses	catastrofico:ruptura	0,0099	0,57	2,2	0,000087	0,004923	0,019272	11494	354	52	-4,5	1,5	-2,0	2,5	5,0	5,0
Rotating Equipment - Compressors	catastrofico:sin especificar	3,09	143	565	0,027088	1,53	49	37	0,02	0,02	-2,0	1,0	1,5	5,0	7,0	8,5
Rotating Equipment - Compressors- Electrical Motor Driven	catastrofico:sin especificar	27,9	2470	9690	0,244404	22	85	4	0,00	0,01	-1,0	1,0	1,5	6,0	8,0	8,5
Rotating Equipment - Compressors - Turbine driven (fallas por 10^3 demandas)	catastrofico:falla de arranque ante demanda	96,5	127	163	0,84534	1	1	1	1	1	-0,5	0,0	0,0	6,5	7,0	7,0
Rotating Equipment - Motor - Driven Fans	catastrofico:falla en funcionamiento	1,75	9,09	24,7	0,01533	0,085828	0,216372	65	2,13	5	-2,0	1,5	-1,0	5,0	6,5	6,0
Rotating Equipment - Motor - Driven Fans (fallas por 10^3 demandas)	catastrofico:falla de paro ante demanda	0,00944	0,309	0,769	0,000083	0,001722	0,006736	12048	344	148	-4,5	3,0	-2,5	2,5	5,0	4,5
Rotating Equipment - Pumps motor driven - pressure centrifugal (MO= Alternating)	catastrofico:falla en funcionamiento	43,3	292	862	0,379308	3	8	3	0,09	0,13	-0,5	0,0	0,5	6,5	7,0	7,5
Rotating Equipment - Pumps motor driven - pressure centrifugal (MO= Alternating), (fallas por 10^3 demandas)	catastrofico:falla de arranque ante demanda	0,36	10,8	43	0,003154	0,094608	0,37668	317	9	3	-3,0	1,0	-0,5	4,0	6,5	6,5
Rotating Equipment - Pumps motor driven - pressure centrifugal (MO= Alternating)	degradado:falla de funcionamiento a la velocidad tasada	15,8	820	3560	0,138408	8	31	7	0,19	0,03	-1,0	0,5	1,0	6,0	7,5	8,0
Rotating Equipment - Pumps motor driven - pressure centrifugal (MO= Running)	catastrofico:falla en funcionamiento	0,812	104	450	0,007113	0,91104	4	141	4	0,25	-2,5	1,0	0,5	4,5	6,5	7,5
Rotating Equipment - Pumps motor driven - pressure centrifugal (MO= Running)	degradado:falla en funcionamiento a la velocidad tasada	0,417	24	92,8	0,003653	0,21024	0,812928	274	8	1	-2,5	1,0	-0,5	4,5	6,5	6,5
Rotating Equipment - Pumps motor driven - pressure centrifugal (MO=Standby), (fallas por 10^3 demandas	catastrofico:falla de paro ante demanda.	1,94	15,6	59,9	0,016994	0,162936	0,524724	59	2	2	-2,0	1,0	-0,5	5,0	6,0	6,5
Rotating Equipment - Pumps turbine driven	catastrofico:falla en funcionamiento	10,9	69,1	277	0,095484	0,780816	2	10	0,5	0,5	-1,5	0,5	0,0	5,5	6,5	7,0
Rotating Equipment - Pumps turbine driven (falla por 10^3 demandas)	catastrofico:falla de paro ante demanda	4,16	26,2	75,8	0,036617	0,229812	0,664008	27	0,8	2	-1,5	1,0	-0,5	5,5	6,5	6,5
Solids Handling - conveyors screw	catastrofico:sin especificar	16,4	912	3640	0,143664	9	32	7	0,10	0,03	-1,0	0,5	1,5	6,0	7,5	8,5
Solids Handling - conveyors screw	degradado:sin especificar	1,72	95,2	384	0,015067	0,955992	3	66	2	0,33	-2,0	0,5	0,0	5,0	6,5	7,0
Valves operated - stop check (falla por 10^3 demandas)	catastrofico:falla en check	0,0307	1,81	6,68	0,000269	0,014104	0,058517	3717	103	17	-4,0	2,0	-1,5	3,0	5,5	5,5
Valves non operated check	catastrofico:sin especificar	0,0552	3,18	12,3	0,000484	0,027057	0,107748	2066	57	9	-3,5	2,0	-1,0	3,5	5,5	6,0
Valves non operated check (falla por 10^3 demandas)	catastrofico:falla en check	0,265	2,5	6,73	0,002497	0,019272	0,058955	400	22	17	-3,0	2,0	-1,5	4,0	5,5	5,5
Valves non operated check (falla por 10^3 demandas)	catastrofico:falla para abrir	0,0347	1,948	0,364	0,000304	0,06127	0,003189	3289	707	314	-4,0	3,0	-2,5	3,0	4,5	4,5
Valves Manual	catastrofico:sin especificar	0,0141	0,184	0,501	0,000124	0,001332	0,004389	8065	731	228	-4,0	3,0	-2,5	3,0	4,5	4,5
Valves Manual(falla por 10^3 demandas)	catastrofico:sin especificar	0,0141	0,291	1,06	0,000124	0,002549	0,009286	8065	1382	108	-4,0	3,0	-2,5	3,0	4,5	4,5
Valves operated - Motor	catastrofico:operación falsa	0,239	1,36	3,8	0,002094	0,011914	0,033288	478	14	30	-3,0	2,0	-1,5	4,0	5,5	5,5
Valves operated - Motor (falla por 10^3 demandas)	catastrofico:no cambia de posicion en demanda	0,504	3,56	18,6	0,004415	0,048991	0,162936	227	20	6	-2,5	1,5	-1,0	4,5	6,0	6,0
Valves operated - Pneumatic	catastrofico:operación falsa	0,274	1,56	12,3	0,0024	0,031448	0,107748	417	36	9	-3,0	2,0	-1,0	4,0	6,0	6,0
Valves operated - Pneumatic (falla por 10^3 demandas)	catastrofico:no cambia de posicion en demanda	0,306	2,3	6,82	0,002681	0,019272	0,057991	373	32	17	-3,0	2,0	-1,5	4,0	5,5	5,5
Valves operated - Solenoid	catastrofico:sin especificar	0,679	48,7	189	0,005948	0,426612	2	168	5	0,5	-2,5	1,5	0,0	4,5	7,0	7,0
Valves operated - Solenoid	catastrofico:operación falsa	0,108	0,408	0,985	0,000946	0,003583	0,008629	1057	273	116	-3,5	1,5	-2,5	3,5	5,5	4,5
Valves operated - Solenoid (falla por 10^3 demandas)	catastrofico:no cambia de posicion en demanda	0,336	2,83	10	0,002943	0,024791	0,0876	340	44	11	-3,0	2,0	-1,5	4,0	5,5	5,5
Vessels Atmospheric Metallic	catastrofico:sin especificar	0,127	0,995	3,02	0,001113	0,008629	0,028455	898	116	38	-3,0	2,0	-2,0	4,0	5,5	5,0
Vessels Atmospheric non Metallic	catastrofico:sin especificar	0,021	1,21	4,68	0,000184	0,0105	0,040997	5435	94	24	-4,0	2,0	-1,5	3,0	5,0	5,5
Vessels Pressurized Metallic	catastrofico:sin especificar	0,000142	0,0109	0,0424	0,000001	0,000095	0,000371	1000000	10526	2695	-6,5	4,5	-3,5	0,5	5,0	3,5
Vessels Pressurized Metallic	degradado:sin especificar	0,000951	0,0636	0,247	0,000008	0,000557	0,002164	125000	1795	462	-5,5	3,5	-3,0	1,5	3,5	4,0

Protection Systems Fire - Fire Detection	catastrofico:sin especificar	0,0198	1,14	4,41	0,000173	0,009966	0,038632	5780	100	26	-4,0	-2,5	-1,5	3,0	5,5	5,5
Protection Systems Fire - Fire Suppression Systems Water	catastrofico:sin especificar	0,168	9,66	37,4	0,001472	0,084822	0,327624	679	12	3	-3,0	-1,5	-0,5	4,0	5,5	6,5
Protection Systems Fire - Fire Suppression Dry Powder	catastrofico:sin especificar	0,0245	1,41	5,45	0,000215	0,012352	0,047742	4651	81	21	-4,0	-2,0	-1,5	3,0	5,5	5,5
Protection Systems Fire - Fire Water Pumps - Diesel (MO=Standby),(falla por 10^3 demandas)	catastrofico:falla en funcionamiento	0,769	18,7	69,8	0,006736	0,163512	0,611448	148	9	2	-2,5	-1,0	-0,5	4,5	6,5	6,5
Protection Systems Fire - Fire Water Pumps - Electric (falla por 10^3 demandas)	catastrofico: falla en arranque	3,62	42,6	143	0,031711	0,3723	1	32	3	1	-1,5	-0,5	0,0	5,5	6,5	7,0
Pressure-Safety Relief-Valves-Pilot Operated (falla por 10^3 demandas)	catastrofico:falla para cerrar una vez abierto	0,188	5	18,8	0,001647	0,0438	0,164688	607	23	6	-3	-1,5	-1	4	5,5	6
Pressure-Safety Relief-Valves-Pilot Operated (falla por 10^3 demandas)	catastrofico:falla para abrir en demanda	0,00932	4,15	18,2	0,000082	0,036354	0,159432	12195	28	6	-4,5	-1,5	-1	2,5	5,5	6

APÉNDICE B

ESTUDIO DE ANÁLISIS DE RIESGO Y OPERABILIDAD (HAZOP) DE LA PLANTA REFORMADORA DE NAFTAS U-500.

Planta: Planta Reformadora de Nafta Pesada 2 (U-500) **Circuito:** Circuito de calentamiento y reacción **Fecha:** 12 de Diciembre de 2002 al

Nodo: 2. Tanque de balance de carga FA-513, bombas GA-514 A/R, intercambiador EA-501, Calentador de carga BA-501A/B/C/D, Reactor DC-501A/B/C/D hasta entrada a soloaire EC-501.

Diagramas: U500-001 y 002 **Producto:** Nafta pesada

Desviación: 7. Baja Conversión de Reformado en los reactores DC-501A/B/C/D. **LOI:** **LOS:** **LSI:** 90 No. Octan **LSS:** 98 No. Octa

	Causa	Consecuencias	Protecciones	Recomendaciones	F	G	R	Clase
31	2.Contaminación de la carga con azufre.	1. Disminución de la producción de hidrógeno. 2. Incumplimiento con el programa de producción. 3. Producto fuera de especificación (bajo octano). 4. Daños irreversibles al catalizador.	1. Análisis rutinario de azufre en la carga líquida. 2. Análisis rutinario con acetato de plomo en la carga 3. Análisis 3. Procedimiento para el reajuste de condiciones de operación cuando se detecta carga contaminada. 4. Programa de simulacros operacionales.	1. Solicitar e instalar analizador continuo de azufre, en la línea de recibo de carga líquida, con la finalidad de desviar la carga y no contaminar la planta. 2. Realizar estudio técnico-económico para la instalación de guardas de azufre en la línea de recibo de carga líquida. 3. Solicitar e instalar analizador de octano en línea, en la salida de producto final a tanque de almacenamiento.	1 (1)	2 (3)	3 (4)	B
37	2.Arrastre de hidrocarburos en el gas de recirculación (gas de levantamiento y de enfriamiento de catalizador a la zona de reducción) por: a) Operación deficiente de filtros coalescedores.	1. Disminución de la producción de hidrógeno. 2. Posibles daños a los internos de reactor. 3. No flujo de catalizador a la unidad de regeneración continua de catalizador	1. Toma de lectura de campo y de bunker de la temperatura y presión del gas hidrógeno de levantamiento y enfriamiento. 2. Programa de mantenimiento de filtros coalescedores. 3. Sistema de enfriamiento y	1. Contar con el refaccionamiento oportuno para el mantenimiento de filtros coalescedores y soloaires. 2. Tener disponibilidad de un compresor booster de hidrógeno. 3. Adquirir un compresor booster nuevo para reemplazar al GB-502B.	1 (1)	2 (3)	3 (4)	B

Planta: Planta Reformadora de Nafta Pesada 2 (U-500) **Circuito:** Circuito de separación y compresión de gas de recirculación **Fecha:** 13 de enero de 2003

Nodo: 3. Solcaire EC-501, condensador EA-507 A/B, separador de baja presión FA-501 hasta la succión del compresor de recirculación GB-501.

Diagramas: U500-003 **Producto:** Reformado, Hidrógeno e hidrocarburos gaseosos condensables y no condensables

Desviación: 4. Alta Presión en el separador de Baja Presión FA-501 **LOI:** **LOS:** **LSI:** **LSS:**

	Causa	Consecuencias	Protecciones	Recomendaciones	F	G	R	Clase
	b) Falla en el calentamiento del gas de arrastre.	4. Incumplimiento con el programa de producción. 5. Producto fuera de especificación (bajo octano). 6. Alta formación de ligeros. 7. Posible paro de planta con cambio y/o cribado de catalizador.	condensación del efluente del reactor. 4. Alarma por alta temperatura en la zona de reducción. 5. Manual de operación del módulo CCR. 6. Disparo de la unidad CCR por No Flujo de gas hidrógeno proveniente del compresor booster. 7. Programa de simulacros operacionales. 8. Cursos de capacitación continua, de formación y actualización. 9. Procedimiento de paro de planta.					
48	2.Disparo del compresor GB-501.	1. Carbonización del catalizador en el reactor DC-501 A/D. 2. Carbonización en el interior de los serpentines de calentador BA-501 A/D. 3. Paro de planta.	1. Interlock de disparo del calentador BA-501A/D y de corte de carga líquida. 2. Procedimiento a falla del compresor GB-501 de la planta U500, SGO-41131-PR-009. 3. PIC-524, actuando la PV-524B enviando a desfogue o gas combustible. 4. Válvula de alivio del FA-501, PSV-502 y su línea de directo. 5. Alarma por bajo flujo de hidrógeno de recirculación, FAL-510 A/B. 6. Programa de simulacros operacionales. 7. Programa de mantenimiento preventivo de instrumentación y mecánico, del compresor GB-501. 8. Procedimiento de paro de planta.	1. Contar con el refaccionamiento oportuno y de calidad para el mantenimiento del compresor.	1 (1)	2 (3)	3 (4)	B

Planta: Planta Reformadora de Nafta Pesada 2 (U-500) **Circuito:** Circuito de compresión de gas de recirculación **Fecha:** 21 de enero de 2003

Nodo: 4. Compresor GB-501.

Diagramas: U500-003 **Producto:** Reformado, Hidrógeno e hidrocarburos gaseosos condensables y no condensables

Desviación: 2. Baja Presión de descarga del compresor GB-501 **LOI:** **LOS:** **LSI:** **LSS:**

	Causa	Consecuencias	Protecciones	Recomendaciones	F	G	R	Clase
58	2.Baja Presión del vapor de alimentación a la turbina.	1. Bajo rendimiento del compresor. 2. Inestabilidad (Surge) del compresor GB-501. 3. Mayor carbonización y formación de ligeros, en el reactor DC-501 A/D. 4. Posibles daños al compresor, con posibilidad de fuga de gas de recirculación en el sello. 5. Envío de hidrógeno de baja pureza al compresor booster. 6. Pérdida de producción. 7. Posible paro de planta.	1. Indicador de presión del vapor a la turbina, en tablero de control del compresor. 2. Indicador de presión en pantalla del SCD, del cabezal general de suministro de vapor a la planta. 3. Indicador de velocidad, en tablero de control del compresor. 4. Registro y seguimiento de las condiciones de operación. 5. Reajuste de carga. 6. Procedimiento para falla de vapor de la planta U500, SGO-41131-PR-007. 7. Procedimiento a falla del compresor GB-501 en la planta U500, SGO-41131-PR-009. 8. Alarma y disparo (calentador BA-501 A/Dj por bajo flujo de gas de recirculación, FAL-510A/B y FSL-510A/B. 9. Comunicación permanente con el Área de Fuerza.	1. Configurar alarma por baja presión en el cabezal de suministro de vapor a la planta.	1 (1)	2 (3)	3 (4)	B

Planta: Planta Reformadora de Nafta Pesada 2 (U-500) **Circuito:** Circuito de calentamiento y reacción **Fecha:** 12 de Diciembre de 2002 al

Nodo: 2. Tanque de balance de carga FA-513, bombas GA-514 A/R, intercambiador EA-501, Calentador de carga BA-501A/B/C/D, Reactor DC-501A/B/C/D hasta entrada a soloaire EC-501.

Diagramas: U500-001 y 002 **Producto:** Nafta pesada

Desviación: 2. Menos Flujo de carga líquida en la descarga de las bombas GA-514/R los reactores DC-501A/B/C/D. **LOI:** **LOS:** **LSI:** **LSS:**

	Causa	Consecuencias	Protecciones	Recomendaciones	F	G	R	Clase
12	1.Falla en FIC-509 con válvula automática cerrada.	1. Alta temperatura en la salida del calentador de carga. 2. Carbonización en el interior de los serpentines. 3. Depósito de carbón en el catalizador. 4. Producto final fuera de especificación. 5. Incumplimiento con el programa de producción en el proceso de gasolina. 6. Paro de planta.	1. Alarma y disparo del calentador por bajo flujo FAL/FSL-509. 2. Alarma y disparo del calentador de carga por alta temperatura en la salida (accionamiento del interlock). 3. Indicadores de temperatura en la salida de los calentadores, y en el hogar inferior, superior y chimenea. 4. Recirculación de hidrógeno en el calentador de carga. 5. Pasar el control de la válvula automática a manual. 6. Bloqueo de la automática y uso de la línea de directo, con indicador de flujo en el SCD. 7. Procedimiento de paro de emergencia. 8. Programa de simulacros operacionales. 9. Capacitación continua al	1. Contar con el refaccionamiento para la instrumentación adecuado y oportuno.	2 (2)	2 (3)	4 (6)	C
29	3.Bajo flujo de hidrógeno de recirculación al calentador.	1. Alta formación de carbón en el catalizador. 2. Carbonización en el interior de los serpentines del calentador. 3. Daños en los serpentines del calentador. 4. Disminución de la vida útil de los serpentines. 5. Incumplimiento del programa de producción. 6. Paro de planta.	1. Alarma por bajo flujo de gas de recirculación, FAL-510. 2. Interlock de disparo del calentador BA-501A/B/C/D (corte del suministro de gas combustible) y cierre de automática de carga líquida FV-509, FSL-510. 3. Procedimiento de paro de emergencia de la planta. 4. Alarmas por alta temperatura en cada una de las salidas del calentador, TAH-502/505/508/512. 5. Alarmas por alta temperatura en el hogar del	1. Contar con refaccionamiento estratégico de la instrumentación. 2. Contar con el refaccionamiento estratégico de equipos de enfriamiento con aire (soloaires) y condensación.	2 (2)	2 (3)	4 (6)	C

Planta: Planta Reformadora de Nafta Pesada 2 (U-500) **Circuito:** Circuito de calentamiento y reacción **Fecha:** 12 de Diciembre de 2002 al

Nodo: 2. Tanque de balance de carga FA-513, bombas GA-514 A/R, intercambiador EA-501, Calentador de carga BA-501A/B/C/D, Reactor DC-501A/B/C/D hasta entrada a soloaire EC-501.

Diagramas: U500-001 y 002 **Producto:** Nafta pesada

Desviación: 2. Menos Flujo de carga líquida en la descarga de las bombas GA-514/R los reactores DC-501A/B/C/D. **LOI:** **LOS:** **LSI:** **LSS:**

Causa	Consecuencias	Protecciones	Recomendaciones	F	G	R	Clase
		calentador, TAH-513 al 518. 6. Programa de simulacros operacionales. 7. Toma y registro de lecturas en campo. 8. Cursos de actualización y de formación. 9. Pláticas al inicio de jornada (Técnicas japonesas).					

Planta: Planta Reformadora de Nafta Pesada 2 (U-500) **Circuito:** Circuito de estabilización **Fecha:** 6 de febrero de 2003

Nodo: 7. Zona de agotamiento de la torre DA-501, bomba GA-504/R, calentador BA-502 y retorno al fondo de la torre DA-501.

Diagramas: U500-006 **Producto:** Reformado estabilizado

Desviación: 2. Baja Temperatura en el fondo de la torre DA-501. **LOI:** **LOS:** **LSI:** **LSS:**

Causa	Consecuencias	Protecciones	Recomendaciones	F	G	R	Clase
83 4. Baja presión de la red de gas combustible	1. Reformado fuera de especificación. 2. Menor producción de destilado en la torre DA-501. 3. Pérdida de producción, por disminución de carga. 4. Posible aumento de nivel en el fondo de la torre DA-501. 5. Mayor consumo de gas. 6. Incumplimiento con el programa de producción.	1. Alarma por baja presión de gas combustible al calentador, PAL-536. 2. Disparo del calentador BA-502 por baja presión de gas combustible accionando válvula de corte rápido, PSL-535. 3. Verificación de la presión en manómetros de campo. 4. Indicadores de temperatura en la salida del calentador. 5. Compensación al suministro de gas combustible con gas de campo. 6. Procedimiento de paro de emergencia de la planta.	1. Contar con el refaccionamiento para el mantenimiento de alarmas y disparos, de manera oportuna. 2. Contar con el refaccionamiento de la válvula de corte rápido para su mantenimiento a efectuarse en cada reparación general.	2 (3)	2 (3)	4 (7)	D

Planta: Planta Reformadora de Nafta Pesada 2 (U-500) **Circuito:** Circuito de estabilización **Fecha:** 6 de febrero de 2003

Nodo: 7. Zona de agotamiento de la torre DA-501, bomba GA-504/R, calentador BA-502 y retorno al fondo de la torre DA-501.

Diagramas: U500-006 **Producto:** Reformado estabilizado

Desviación: 2. Baja Temperatura en el fondo de la torre DA-501. **LOI:** **LOS:** **LSI:** **LSS:**

	Causa	Consecuencias	Protecciones	Recomendaciones	F	G	R	Clase
90	2.Pichanchas obstruidas de la bomba de recirculación, GA-504/R.	1. Cavitación de la bomba de recirculación GA-504/R. 2. Posibles daños del sello, ruptura, fuga e incendio. 3. Posible carbonización en el interior de los serpentines. 4. Posibles daños de los serpentines por falta de carga (falta de enfriamiento interno). 5. Ruptura, fuga, e incendio en el interior del calentador BA-502. 6. Paro de planta.	1. Indicador de presión en la descarga de la bomba GA-504/R. 2. Alarma por bajo flujo al calentador BA-5023, FAL-521 A/B. 3. Equipo de relevo disponible y procedimiento para ponerlo en operación. 4. Controlador de temperatura de salida del calentador BA-502, TIC-526. 5. Recorridos operacionales para toma de datos y registro de los mismos en la hoja de condiciones de operación. 6. Programa de simulacros operacionales. 7. Programa de rotación de equipo mecánico y eléctrico (REME).	1. Instalar arranque automático desde bunker, de bomba de relevo GA-504/R. 2. Tener el refaccionamiento original de bombas, oportuno y a la mano.	2 (2)	3 (4)	6 (7)	D

Planta: Planta Reformadora de Nafta Pesada 2 (U-500) **Circuito:** Circuito de compresión **Fecha:** 28 de febrero de 2003

Nodo: 9. Salida domo FA-502, Guardas de cloro FA-503, Compresor GB-502 A/B 1er y 2do paso y salidas a plantas U400, CCR y U100.

Diagramas: U500-004 **Producto:** Hidrógeno

Desviación: 4. Daños en la estructura de los compresores **LOI:** **LOS:** **LSI:** **LSS:**

	Causa	Consecuencias	Protecciones	Recomendaciones	F	G	R	Clase
108	1.Ruptura de sellos del 1er y 2do paso de los compresores reciprocantes GA-502 A/B.	1. Fuga de hidrógeno e hidrocarburo, e incendio. 2. Paro del equipo. 3. Bajo flujo de hidrógeno a la Unidad Hidrodesulfuradora de Nafta (U-400). 4. Bajo flujo de hidrógeno a la Unidad Hidrodesulfuradora de Destilados Intermedios (U-100). 5. Posible paro de plantas U-100 y U-400.	1. Recorrido e inspección visual en campo, aplicando la técnica VOTO. 2. Procedimiento para fuga excesiva de hidrogeno en los compresores GB-502 A/B de la Planta Reformadora de Nafta No. 2 (U-500), SGO-41131-PR-035. 3. Uso de equipo de relevo. 4. Procedimiento de paro de planta.	1. Contar con el refaccionamiento crítico, oportuno y de calidad para el mantenimiento de compresores. 2. Tener en almacenamiento en forma permanente, un juego de anillos y bandas del émbolo y un juego de sellos del compresor GB-502 A/B, originales. 3. Realizar estudio para instalar sistema de detección de mezclas explosivas. 4. Realizar estudio técnico-económico para reemplazar el compresor GB-502A por uno nuevo, por ser equipo obsoleto. 5. Realizar estudio técnico-económico para modernizar el compresor GB-502B, para tener el equipo confiable. 6. Verificar y probar el metalizado de los émbolos nuevos a instalar.	1 (1)	3 (3)	4 (4)	B

BIBLIOGRAFÍA

BIBLIOGRAFÍA.

1. ANSI/ISA-S84.01-1996. "Application of Safety Instrumented Systems for the Process Industries". Instrumentation, Systems and Automation Society, 1996.

2. Browning R.L," Chem. Prog-loss prevent", U.S.A, vol. 12, 1979.

3. Center of Chemical Process Safety (CCPS), Center of Chemical American Institute of Chemical Engineers (AIChE). "Layers Of Protection Analysis (LOPA): Simplified Process Risk Assessment". New York, 2001.

4. Center of chemical Process Safety (CCPS), Center of Chemical American Institute of Chemical Engineers (AIChE).technical management of chemical process, New York, NY. 1989.

5. Center of Chemical Process Safety (CCPS), American Institute of Chemical Engineers (AIChE). "Guidelines for Hazard Evaluation Procedures". Second Edition. New York, 1992.

6. Center of Chemical Process Safety (CCPS), American Institute of Chemical Engineers (AIChE). "Guidelines for Chemical Process Quantitative Analysis". Second Edition. New York, 2000.

7. Center of Chemical Process Safety (CCPS), American Institute of Chemical Engineers (AIChE). "Guidelines for Process Equipment Reliability Data tables", New York 1989.

8. Center of Chemical Process Safety (CCPS), American Institute of Chemical Engineers (AIChE)."Center for Chemical Process Safety, American Insttitute of Chemical Engineers, Guidelines For Investigating Process Incidents", 1era Edicion, 1992.

9. Dallas L. Green Arthur M. Dowell. "How To Design, Verify, And Validate Emergency Shutdown Systems". "Control Technology Supervisor Technical Fellow, Risk Analysis" Rohm and Haas Company Rohm and Haas Texas Inc, 1998.

10. Angela E. Summers, "Understanding Safety Integrity Levels", Control Engineering online, página de internet: http://www.controleng.com/archives/2200/ctl0201.00/0002we3.htm.

11. Angela E. Summers, "Draft IEC 61508 Target Safety Integrity Levels", Institute of Instrumentation and Control Australia Inc., página de internet: http://www.controleng.com/archives/2200/ctl0201.00/0002we3.htm.

12. Donald M. Little, "Catalytic Reforming Pennwell Books", Pennwell Publishing Company Tulsa, Oklahoma 1985.

13. J.B.F,"Facility Risk Review a Technical Approach", Associates, Inc. 1992.

14. Huff M. Andrew and Randal L. Montgomery. "Analysis of Safety Instrumented Systems to Meet Plant Objectives". ABS Consulting, página de Internet: http://www.jbfa.com/qrasis.html.

15. Gary, Handwerk. Refino de Petróleo, Editorial Reverte, 1980.

16. Klett, Trevor, "What went wrong? Case Histories of Process Disasters". 4th edition. Gulf Publishing Company, Texas, 1998.

17. Khan I. Faisal, and Amyotte," Evaluation of Available Indices for Inherently Safer Design Options", Process Safety Progress, vol. 22. No.2, June 2003.

18. Manual de Operación," Unidad Reformadora De Naftas Pesada 2", Minatitlan, Veracruz, PEMEX, 1985.

19. Mark Moderski, Sankar Mahalingam, Safety Integrity Levels in Desing,Stone and Webster Engineering Corporation 1430 Enclave Parkway Houston, Texas 77077-2023.

20. Offshore Reliability Data Hanbook, OREDA, 3rd Edition, 1997.

21. OSHA 1910.119, Process Safety Management of Highly Hazardous Chemical. U.S, Department of Laboral, Regulations, STANDARS- 29 CFR, 1991.

22. Oficina internacional del trabajo, Control de riesgos de accidentes mayores, editorial alfa omega,1990.

23. Rao V. Kolluru, Steven M. Bartell, Robin M. Pitblado, R. Scott Stricoff. "Manual de Evaluación y Administración de Riesgos", Ed. Mc. Graw-Hill, 1ª edición. 1998.

24. Santamaría Ramiro, J.M. "Análisis y Reducción de Riesgos en la Industria Química". Fundación MAPFRE, España, 1994.

25. Cruz Campa Héctor Javier, Rodríguez Jiménez Julio César, Díaz Torres Daniel, Cruz Gómez M. Javier. "Determinación del Nivel de Integridad de la Seguridad (SIL) mediante el análisis cuantitativo simplificado de los escenarios de alto riesgo potencial, obtenidos por la técnica HAZOP". Laboratorio E-212, Departamento de Ingeniería Química, Facultad de química. UNAM.

26. Hauptmanns, U." Análisis de Árbol de Fallas", Ediciones Bellaterra. Barcelona,1986.