

28



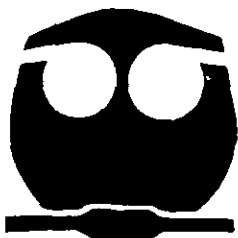
UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE QUIMICA

DETERMINACION DEL NIVEL DE INTEGRIDAD DE SEGURIDAD EN EL SISTEMA DE DETECCION, ALARMA Y PARO DE EMERGENCIA PARA LA PLATAFORMA IXTOC-A

T E S I S

QUE PARA OBTENER EL TITULO DE: INGENIERO QUIMICO PRESENTA: MANUEL CASTAÑEDA PEÑA



EXAMENADO Y APROBADO FACULTAD DE QUIMICA

MEXICO, D. F.

286647

2000



Universidad Nacional
Autónoma de México

Dirección General de Bibliotecas de la UNAM

Biblioteca Central



UNAM – Dirección General de Bibliotecas
Tesis Digitales
Restricciones de uso

DERECHOS RESERVADOS ©
PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

Jurado asignado:

Presidente	Prof. José Antonio Ortiz Ramírez
Vocal	Prof. José Agustín Texta Mena
Secretario	Prof. Rodolfo Torres Barrera
1er. Suplente	Prof. Jesús Arturo Butrón Silva
2o. Suplente	Prof. Alfonso Durán Moreno

Sitio donde se desarrollo el tema:

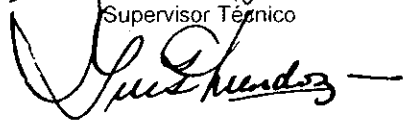
INSTITUTO MEXICANO DEL PETRÓLEO

Asesor del tema



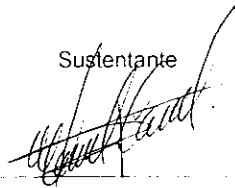
Ing. José Agustín Texta Mena

Supervisor Técnico



Ing. José Luis Gordillo Mendoza

Sustentante



Manuel Castañeda Peña

AGRADECIMIENTOS:

Gracias a Jehová Dios Todo Poderoso y a nuestro Señor Jesucristo por brindarme la oportunidad de vivir y de estar a lado de las personas que amo.

Gracias a mis padres, Manuel y Ma. de los Angeles, por el gran amor que me tienen y por todos los cuidados y atenciones que siempre han tenido conmigo.

Gracias a mis hermanos, Paty, Guille, Pablo, Erika, Karla y Brenda, por su apreciable cariño.

Gracias a mis amigos las "Vacas Flacas" que de no contar con su amistad, mi vida no estaria completa.

Gracias Alma por brindarme tu amor y compañía, y por compartir conmigo muchos momentos felices.

Gracias a todos los maestros y compañeros de la Facultad de Química por todo el apoyo que me brindaron a lo largo de la carrera.

*Gracias al Instituto Mexicano del Petróleo por todas las facilidades que dieron para la realización de este trabajo, en especial a:
Ing. José Luis Gordillo Mendoza,
Ing. Benjamín Alfonso Castillo López
Rossy Tames Cerezo*

Gracias Popis por darme tu amistad durante el tiempo que estuviste con nosotros. luego te alcanzamos.

CONTENIDO

	Página
Lista de figuras	i
Lista de tablas	ii
Prefacio	iii
Introducción	iv
I. METODOLOGÍAS DE ANÁLISIS DE RIESGO	1
1.1 Lista de verificación (Checklist)	1
1.2 ¿Que pasa si...? (What if...)	2
1.3 Estudio de Riesgos de Operabilidad en Procesos (HAZOP)	2
1.4 Arbol de Fallas (Failure Tree)	3
1.5 Índice Mond de Fuego, Explosión y Toxicidad	4
1.6 Evaluación de Riesgos	5
II. FILOSOFÍA OPERATIVA DEL SISTEMA DE DETECCIÓN, ALARMA Y PARO DE EMERGENCIA DE LA PLATAFORMA IXTOC-A	7
II.1 Objetivo del Sistema de Paro de Emergencia	7
II.2 Alcance del Sistema de Paro de Emergencia	7
II.3 Descripción general del proceso	10
II.4 Paro de emergencia por condiciones de proceso	12
II.5 Paro de emergencia por acción manual	13
II.6 Paro de emergencia por condiciones de seguridad	14
II.7 Normatividad aplicada	16
III. NIVELES DE INTEGRIDAD DE SEGURIDAD	17
III.1 Conceptualización de los niveles de seguridad	17
III.2 Métodos para determinar el SIL	21
III.2.1 HAZOP modificado	22
III.2.2 Consecuencia solamente	22
III.2.3 ALARP	23
III.2.4 Matriz del riesgo	24
III.2.5 Gráfico del riesgo	26
III.2.6 Análisis cuantitativo	28
III.2.7 SIL asignado por mandato corporativo	29

IV. DETERMINACIÓN DEL NIVEL DE INTEGRIDAD DE SEGURIDAD EN EL SISTEMA DE DETECCIÓN, ALARMA Y PARO DE EMERGENCIA PARA LA PLATAFORMA IXTOC-A	30
IV.1 Etapas del Ciclo de Vida de Seguridad	30
IV.2 Análisis de Peligros del Proceso	31
IV.3 Definición del Nivel de Seguridad	34
IV.4 Análisis con árbol de fallas	37
IV.5 Determinación del Nivel de Integridad de Seguridad	40
IV.5.1 Pozos de Producción No. 16 y 18	40
IV.5.2 Separador de Prueba FA-1101	48
IV.5.3 Línea de Salida 8" P-1108	54
IV.5.4 Sistema global de producción	60
V. ANÁLISIS DE RESULTADOS	63
V.1 Pozos de Producción No. 16 y 18	63
V.2 Separador de Prueba FA-1101	66
V.3 Línea de Salida 8" P-1108	69
V.4 Sistema global de producción	73
VI. CONCLUSIONES Y RECOMENDACIONES	75
VII. BIBLIOGRAFÍA	77

Lista de figuras

Figura No.	Descripción	página
Figura II.1	Esquema de funcionalidad del paro de emergencia de Ixtoc-A	9
Figura II.2	Diagrama general de proceso de la plataforma de perforación Ixtoc-A	11
Figura III.1	Diagrama de ALARP para la tolerancia del riesgo	24
Figura III.2	Lazo entre la reducción del riesgo y el coste del ciclo de vida	24
Figura III.3	Matriz dimensional del riesgo	25
Figura III.4	Matriz tridimensional del riesgo	26
Figura III.5	Ejemplo de gráfico del riesgo	27
Figura III.6	Ejemplo de árbol de fallas	28
Figura IV.1	Etapas del ciclo de vida de seguridad	31
Figura IV.2	Matriz de riesgo y acciones generadas para la plataforma Ixtoc-A	33
Figura IV.3	Gráfico para la definición del SIL	34
Figura IV.4	Ejemplos de símbolos utilizados en la construcción de Árboles de Falla	38
Figura IV.5	Árbol de fallas para sobrepresión en pozos de producción	41
Figura IV.6	Árbol de fallas para fuego externo en pozos de producción	42
Figura IV.7	Árbol de fallas para fuga de gas combustible en pozos de producción	43
Figura IV.8	Árbol de fallas para fuga de gas tóxico en pozos de producción	44
Figura IV.9	Árbol de fallas para ruptura en pozos de producción	45
Figura IV.10	Árbol de fallas para disparo en falso en pozos de producción	47
Figura IV.11	Árbol de fallas para sobrepresión en separador de prueba	49
Figura IV.12	Árbol de fallas para fuego externo en separador de prueba	50
Figura IV.13	Árbol de fallas para fuga de gas combustible en separador de prueba	51
Figura IV.14	Árbol de fallas para fuga de gas tóxico en separador de prueba	52
Figura IV.15	Árbol de fallas para disparo en falso en separador de prueba	53
Figura IV.16	Árbol de fallas para sobrepresión en línea de salida	55
Figura IV.17	Árbol de fallas para ruptura en línea de salida	56
Figura IV.18	Árbol de fallas para fuga de gas tóxico en línea de salida	57
Figura IV.19	Árbol de fallas para fuga de gas combustible en línea de salida	58
Figura IV.20	Árbol de fallas para disparo en falso en línea de salida	59
Figura IV.21	Árbol de fallas para sobrepresión y ruptura del sistema global	61
Figura IV.22	Árbol de fallas para disparo en falso del sistema global	62

Lista de tablas

Tabla No.	Descripción	página
Tabla III.1	Correlación del SIL con la disponibilidad y probabilidad de falla (PFD)	17
Tabla III.2	Categorías de la probabilidad	18
Tabla III.3	Vista cualitativa del SIL	20
Tabla III.4	Tabla de decisión de la consecuencia solamente	23
Tabla IV.1	Ponderación de la severidad de la consecuencia	32
Tabla IV.2	Ponderación de la frecuencia	32
Tabla IV.3	Ponderación resultante del HAZOP para la plataforma Ixtoc-A	33
Tabla IV.4	Parámetros de severidad de la consecuencia	35
Tabla IV.5	Parámetros de la frecuencia	36
Tabla IV.6	Definición del SIL utilizando gráfico del riesgo	37
Tabla IV.7	Datos de tasa de falla para los dispositivos involucrados en el SPE	39
Tabla V.1	Resultados ante el evento de sobrepresión en pozos de producción	64
Tabla V.2	Resultados ante el evento de fuego externo en pozos de producción	65
Tabla V.3	Resultados ante el evento de fuga de gas combustible en pozos	65
Tabla V.4	Resultados ante el evento de fuga de gas tóxico en pozos de producción	65
Tabla V.5	Resultados ante el evento de ruptura en pozos de producción	66
Tabla V.6	Resultados ante el evento de paro en falso en pozos de producción	66
Tabla V.7	Resultados ante el evento de sobrepresión en separador de prueba	67
Tabla V.8	Resultados ante el evento de fuego externo en separador de prueba	68
Tabla V.9	Resultados ante la fuga de gas combustible en separador de prueba	68
Tabla V.10	Resultados ante el evento de fuga de gas tóxico en separador de prueba	68
Tabla V.11	Resultados ante el evento de ruptura en separador de prueba	69
Tabla V.12	Resultados ante el evento de paro en falso en separador de prueba	69
Tabla V.13	Resultados ante el evento de sobrepresión en línea de salida	71
Tabla V.14	Resultados ante la fuga de gas combustible en línea de salida	71
Tabla V.15	Resultados ante el evento de fuga de gas tóxico en línea de salida	72
Tabla V.16	Resultados ante el evento de ruptura en línea de salida	72
Tabla V.17	Resultados ante el evento de paro en falso en línea de salida	72
Tabla V.18	Resultados ante sobrepresión y ruptura del sistema global	73
Tabla V.19	Resultados ante paro en falso del sistema global	74

PREFACIO.

El Instituto Mexicano del Petróleo (IMP) desarrolló la Ingeniería para el proyecto "Sistema de detección, alarma y paro de emergencia para la plataforma Ixtoc-A", dentro del cual se integró como parte fundamental, la determinación del nivel de integridad de seguridad (SIL).

Se tienen como antecedentes: los reportes de anomalías emitidos por la entidad operativa, que concluyen en la necesidad de disponer de un sistema de seguridad integral en Ixtoc-A, que incluya un sistema de paro de emergencia que permita: identificación de problemas, determinación de situaciones (qué está pasando exactamente y qué se está afectando), sistema de respuesta inmediata (para minimizar consecuencias) y acciones a seguir para *ayudar a restaurar las operaciones a situación normal*; y el Estudio de Riesgos y Operabilidad del proceso (HAZOP) efectuado junto con personal operativo de la plataforma, en el proyecto denominado "Análisis de riesgo para las Instalaciones del Activo Ek-Balam", de donde se identificaron los eventos no deseados, así como su frecuencia de ocurrencia y la severidad de sus consecuencias.

La determinación del nivel de integridad de seguridad tiene como objetivo que la plataforma Ixtoc-A cumpla con un nivel que garantice al proceso un estado seguro ante eventos no deseados por la acción de un paro por emergencia. Lo cual implica que la Ingeniería para el Sistema de Paro de Emergencia (SPE) contemple la adición de sensores como elementos primarios y válvulas de corte como elementos finales configurados al Sistema Instrumentado de Seguridad (SIS).

La determinación cuantitativa se elaboró empleando el Análisis de Arbol de Falla usando modelos rigurosos de confiabilidad mediante el software CARA-Fault-Tree versión 4.02 de la compañía DNV en cada interlock o sistema en estudio, y obedeciendo sólo las etapas aplicables del ciclo de vida de la seguridad estipuladas en el estándar ANSI/ISA S-84.01. Los resultados se obtuvieron en función de la Probabilidad de Falla en Demanda (PFD) del SPE en cada sistema y ante la presencia de los eventos no deseados.

INTRODUCCIÓN

La reducción eficaz de los riesgos es esencial para proporcionar la seguridad de empleados y la preservación del medio ambiente, reduciendo pérdidas de capital, interrupciones del proceso que se acortan y conservar la imagen corporativa de la empresa. Esto implica el análisis del riesgo y la metodología de la reducción de riesgos para las industrias, incluyendo: la refinación de petróleo, petroquímica, elaboración de productos químicos, la producción de aceite y gas, producción de pulpa y papel, y en todas aquellas en las que la seguridad y confiabilidad de los procesos sean primordiales.

Para ello, es necesario identificar peligros involucrados mediante el uso de técnicas de detección tales como: Lista de Verificación (Checklist), ¿Qué pasa si...? (What if...), Estudio de Riesgos de Operabilidad de Procesos (HazOp), Arbol de Fallas (Failure Tree), Índice Mond de Fuego, Explosión y Toxicidad y Evaluación de Riesgos entre otros. En el Capítulo I se describen brevemente estas metodologías de análisis de riesgo.

Si un sistema no puede ser diseñado de modo que sea intrínsecamente seguro, necesitan ser puestas en ejecución otras salvaguardias tales como Sistemas Instrumentados, controles mecánicos o procedimientos de funcionamiento. En el Capítulo II se resume de manera concisa el funcionamiento y en que consiste el sistema de detección y paro de emergencia de Ixtoc-A.

Si un sistema instrumentado está utilizado para atenuar el peligro, entonces se debe dar una cierta consideración hacia la integridad de este sistema, basado sobre el riesgo presentado por el peligro. En función de estándares IEC 61508 e ISA S84.01, el nivel de la integridad de este sistema instrumentado debe ser especificado para poder alcanzar la probabilidad correspondiente del incidente en demanda. En estos estándares se establecen los requerimientos para que las compañías asignen un nivel de integridad de seguridad (SIL) para todas las aplicaciones de los sistemas instrumentados de seguridad (SIS). Se asigna un SIL para cualquier proceso en el cual el análisis de peligros del proceso (PHA) haya determinado que la integridad mecánica del proceso y/o el control del mismo, sean escasos para atenuar el peligro potencial. La asignación se basa en la cantidad de reducción del riesgo que sea necesaria para atenuar el riesgo asociado al proceso a un nivel aceptable. Todos los diseños, de SIS, operación y opciones de mantenimiento, se deben entonces verificar contra el SIL. En el Capítulo III se explica el concepto de niveles de integridad de seguridad y se examinan las

siete técnicas más utilizadas actualmente para determinar el SIL: HAZOP modificado, consecuencia solamente, ALARP, matriz del riesgo, gráfico del riesgo, gravamen cuantitativo y SIL asignado por mandato corporativo.

El Capítulo IV contiene la determinación del SIL para el Sistema de Detección, Alarma y Paro de Emergencia para la Plataforma Ixtoc-A.

La parte final del documento contiene las Conclusiones derivadas de la determinación del SIL, así como las recomendaciones que se proponen.

I. METODOLOGÍAS DE ANÁLISIS DE RIESGO (15)

Nos encontramos en una era donde los grandes avances tecnológicos están presentes en cada uno de los procesos industriales, debido principalmente a la complejidad de los mismos. Esto nos conlleva a que también los sistemas de paro de emergencia en cada proceso sufran diversas modificaciones, como resultado de los accidentes catastróficos surgidos en el pasado, los cuales tuvieron diferentes magnitudes de acuerdo a sus consecuencias, dañando al personal, al medio ambiente, a los equipos, a la producción y la propia imagen corporativa de la empresa. Los factores anteriormente mencionados, obligan a desarrollar y establecer diversas técnicas de análisis de riesgo ambiental, así como políticas del uso del suelo que eviten la coexistencia entre zonas urbanas o ecológicamente sensibles y áreas industriales de alto riesgo. Es importante señalar aquí algunas de las técnicas más utilizadas para el análisis de riesgo.

1.1 Lista de Verificación (Checklist).

Una lista de verificación es una lista de preguntas acerca de la organización de la planta, operación, mantenimiento y otras áreas de interés. Históricamente, el propósito general de utilizar listas de verificación ha sido el mejorar la confiabilidad y desempeño humano durante varias etapas del proyecto, o bien, asegurar la concordancia con las regulaciones o estándares nacionales e internacionales.

Esta metodología puede ser utilizada durante el diseño preliminar de algún proyecto, durante la construcción y operación de una planta o durante la realización de paros y arranques de la misma.

Las ventajas que representa esta metodología son las siguientes:

- ✓ Especifica los requerimientos mínimos.
- ✓ Útil para gente de poca experiencia.
- ✓ Uniformidad en la información.
- ✓ Bajo costo en su desarrollo y aplicación.

Las desventajas que representa esta metodología son las siguientes:

- × Limitada a la experiencia de la persona que desarrollo la lista.
- × Necesita actualización constante.
- × No es efectivo para riesgos complejos en nuevas instalaciones o procesos.

1.2 ¿Que pasa si ...? (What if...).

Esta técnica no requiere métodos cuantitativos especiales o una planeación extensiva. El método utiliza información específica de un proceso para generar una especie de preguntas de lista de verificación. Un equipo especial prepara una lista de preguntas, llamadas preguntas ¿Que pasa Si?, las cuales son entonces contestadas colectivamente por el grupo de trabajo y resumidas en forma tabular.

Esta técnica es ampliamente utilizada durante las etapas de diseño del proceso, así como durante el tiempo de vida o de operación de una instalación, asimismo cuando se introducen cambios al proceso o a los procedimientos de operación.

Las ventajas que representa esta metodología son las siguientes:

- ✓ Fácil de utilizar.
- ✓ Aplicable al proceso completo o secciones del mismo.
- ✓ Método creativo con una visión de trabajo en equipo.
- ✓ Flexible.
- ✓ Puede usarse en procesos por lote (batch).

Las desventajas que representa esta metodología son las siguientes:

Fácilmente pasa por alto los riesgos potenciales ya que:

- × Carece de estructura.
- × Su efectividad depende de la experiencia del coordinador.
- × Requiere de un entendimiento básico de las operaciones de proceso y de los procedimientos.
- × Requiere de los diagramas de tubería e instrumentación (DTI's).
- × Se basa en una revisión conceptual.

1.3 Estudio de Riesgos de Operabilidad en Procesos (HAZOP).

Un estudio de riesgo en el proceso, es simplemente una metodología estructurada para la identificación de riesgos. Es un programa que permite al usuario emplear el pensamiento creativo en la identificación de problemas operacionales y de peligro.

Un HAZOP involucra una examinación metódica y sistemática de los documentos de diseño que describen las instalaciones. El estudio se lleva a cabo por un grupo multidisciplinario que identifica los problemas de riesgo en el proceso que pueden causar un accidente. Las desviaciones del valor de diseño o los parámetros clave, son estudiados usando palabras guía

para controlar la evaluación de la examinación. Esto supone que los valores de diseño de los flujos, temperaturas, presiones, concentraciones y otros procesos variables son inherentemente seguros y operables.

La aplicación de esta técnica es utilizada durante el diseño de un proyecto, durante la instalación de una instalación industrial, operación de instalaciones existentes o cuando se realizan cambios mayores en los procesos.

Las ventajas que representa esta metodología son las siguientes:

- ✓ Incluye múltiples puntos de vista.
- ✓ En forma estructurada se identifican mayor número de problemas con una visión de grupo.
- ✓ Toma en cuenta el error humano.
- ✓ Analiza a detalle el sistema.
- ✓ En general, permite identificar entre el 90 y el 99% los riesgos existentes, pero sin ser todos reales.

Las desventajas que representa esta metodología son las siguientes:

- × El éxito o fracaso depende de la exactitud y actualización de la información, diagramas y habilidad del grupo.
- × Es un método muy cansado, se requiere en teoría para un nuevo proyecto de 6 meses con sesiones de 40 horas semanales.
- × No indica las interacciones entre nodos o secciones del sistema.

1.4 Arbol de Fallas (Failure Tree).

Es una herramienta de análisis que utiliza el razonamiento deductivo y diagramas gráficos, mostrando la lógica del proceso de razonamiento deductivo para determinar como puede ocurrir un evento particular no deseado.

Es un método estructural y sistemático que puede ser utilizado en un sistema sencillo.

Es una de las pocas herramientas que puede tratar adecuadamente el asunto de fallas comunes, y es una técnica que puede producir resultados tanto cualitativos como cuantitativos.

Las etapas donde se utiliza esta metodología son durante el diseño para detectar fallas escondidas, o durante la operación para evaluar accidentes potenciales en el sistema y detectar fallas en procedimientos o en el operador.

Las ventajas que representa esta metodología son las siguientes:

- ✓ Uno de los mejores métodos para encontrar las causas de un evento, siguiendo interrelaciones complejas.

- ✓ Incorpora el error humano.
- ✓ Muestra los efectos aditivos al accidente.

Las desventajas que representa esta metodología son las siguientes:

- × Requiere de un conocimiento muy completo del caso de estudio.
- × Requiere de entrenamiento para usarlo.
- × El árbol puede ser difícil de interpretar, ya que diferentes representaciones dan diferentes resultados.
- × Es costoso ya que requiere de mucho tiempo.
- × Esta metodología puede dar resultados cuantitativos si se incluye una asignación de rangos en cuanto a fallas.

1.5 Índice Mond de Fuego, Explosión y Toxicidad.

Este método se basa en la peligrosidad de los productos y en el carácter crítico de los procesos en función de sus antecedentes de operación en instalaciones similares. Este índice fue desarrollado por ICI (empresa química de origen británico), y permite obtener índices numéricos de riesgos para cada sección de las instalaciones industriales, en función de las características de las sustancias manejadas, cantidad, tipo de proceso, y de las condiciones específicas de operación.

Esta técnica es utilizada durante las etapas de diseño de instalaciones, así como durante el tiempo de vida o de operación de una instalación y realización de cambios mayores al proceso.

Las ventajas que representa esta metodología son las siguientes:

- ✓ Amplía gama de matrices a considerar.
- ✓ Amplio rango de procesos.
- ✓ Rápido y fácil de usar.
- ✓ Estima el valor de las pérdidas en el área de estudio.
- ✓ Identifica las secciones de mayor riesgo y por tanto, busca medidas de seguridad.

Las desventajas que representa esta metodología son las siguientes:

- × Se debe seccionar basándose en los materiales presentes, cantidad, condiciones de operación y tipo de proceso.
- × La toxicidad es considerada sólo como un factor de complicación.

1.6 Evaluación de Riesgos.

Con base en los riesgos detectados, utilizando procedimientos tales como los antes indicados, es conveniente evaluar el nivel del riesgo detectado a fin de poder integrar las opciones para su reducción mediante un análisis costo-beneficio, que permita el desarrollo industrial sin descuidar la protección a la población.

Entre los procedimientos para la evaluación del riesgo, se tienen los siguientes:

En forma sucinta podemos mencionar el denominado análisis de riesgo, en el cual se considera a los accidentes como resultado de un encadenamiento de eventos simples para los cuales se puede evaluar el nivel de probabilidad de su ocurrencia. El encadenamiento de los distintos eventos simples sigue en su comportamiento matemático las leyes del álgebra booleana obteniendo el nivel de probabilidad mediante simples operaciones matemáticas entre los niveles de probabilidad de los eventos simples.

Es importante mencionar que una vez determinado el nivel de riesgo, este se puede modificar estableciendo medidas de seguridad más estrictas, por lo que es necesario establecer un valor probabilístico para el accidente que se está evaluando, lo que se puede hacer mediante el análisis del costo que la implementación de las medidas implica, en relación con lo que se previene.

Juegan un papel importante entre los criterios a observar en la evaluación de riesgos, el establecimiento de parámetros de medición, mediante los cuales se fijan valores tope que permitan salvaguardar la salud de quienes se encuentran en los alrededores de instalaciones de alto riesgo, así como proteger sus bienes.

En este sentido se ha considerado como un parámetro de protección de la salud en cuanto a afectación por toxicidad, el IDLH (peligro inmediato a la salud o a la vida), que se define como un valor máximo en ppm ó mg/m^3 en concentración de un contaminante tóxico al cual una persona puede escapar sin daños irreversibles a su salud en un período de hasta 30 minutos de exposición.

Este valor se utiliza para definir la zona de alto riesgo, lo cual se hace mediante la utilización de modelos de dispersión que permiten determinar que distancia se requiere en los casos en los que ocurran accidentes en actividades industriales con fugas o derrames.

El TLV (valor límite umbral), es el valor promedio de concentración máxima permisible para exposición, dado en ppm ó mg/m^3 de un contaminante tóxico que se considera no tener ningún efecto en una persona expuesto al mismo en una exposición de 15 minutos

Este valor se utiliza para definir la zona de amortiguamiento siguiendo un procedimiento semejante al que se realiza para determinar la zona de alto riesgo.

En lo relativo a afectación por riesgo en los casos de actividades en las cuales se utilizan sustancias con características explosivas, para la determinación de la zona de alto riesgo, se establece como parámetro de afectación 0.5 lb/pulg^2 , tomando como zona de afectación el área de un círculo con un radio que considera la distancia desde donde se encuentra el punto donde se puede formar la nube explosiva y cuyo extremo representa la distancia a la cual se tiene una onda de sobrepresión de 0.5 lb/pulg^2 .

II. FILOSOFÍA OPERATIVA DEL SISTEMA DE DETECCIÓN, ALARMA Y PARO DE EMERGENCIA DE LA PLATAFORMA IXTOC-A

A los sistemas que conforman la operabilidad (el manejo, control, operación y seguridad) del complejo Ixtoc-A, compuesto por las plataformas de Perforación, Habitacional-Telecomunicaciones y de Almacenamiento de Combustible se les implementará un sistema de seguridad que deberá aplicar acciones necesarias para lograr una secuencia de paro en situaciones de riesgo de incidentes o emergencias, el cual se le denominará "Sistema de Paro de Emergencia" (SPE) que estará centralizado en la plataforma Ixtoc-A Habitacional-Telecomunicaciones segundo nivel, en una unidad de procesamiento que se denominará UPR de Paro de Emergencia, con sus propias fuentes de energía, respaldo, hardware, software y control, localizadas en forma independiente siendo estas adicionales a los dispositivos de control utilizados para la operación normal del proceso, destinado a las funciones de la plataforma.

II.1 Objetivo del Sistema de Paro de Emergencia

El SPE de la plataforma tiene como principal propósito una filosofía de operación con acciones destinadas a la protección del personal e instalaciones y a la prevención de posibles incidentes, accidentes y emergencias causadas por un comportamiento anormal en el sistema de proceso de la operación de explotación, detección de falla de suministro de energía eléctrica del CCM, situaciones de detección de altas concentraciones de gas tóxico, gas combustible y/o flama, detección de alta temperatura en áreas de operación por medio del Sistema de Seguridad de alarmas visibles y audibles y activación del Sistema Automatizado de Agua Contra incendio para áreas de perforación, separador, tableros y áreas de equipos de servicio general en la plataforma de Perforación Ixtoc-A.

II.2 Alcance del Sistema de Paro de Emergencia

El sistema de seguridad en la plataforma se compone de dos subsistemas

- El SPE compuesto por las variables de proceso, y
- El Sistema de Detección de gas y fuego

Siendo absolutamente independientes uno del otro en hardware y software.

El sistema se integra en tres partes básicas de control basándose en la normatividad API-RP-14C, ISA-S84.01, ISA-S84 02 e ISA-S91:

a.- Dispositivos de Detección (sensores)

b.- Sistema Electrónico Programable

c.- Elementos de Acción de Respuesta

a. Dispositivos de Detección (sensores).- 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).

b. Sistema Electrónico Programable.- El equipo (hardware) que ejecutará las funciones de la lógica de la matriz de paro en detección, monitoreo, registro, proceso de análisis y acción.

c. Elementos de acción de respuesta.- Son todos los elementos finales que se encuentran instalados para las funciones de respuesta, producto del procesamiento de la filosofía de operación-respuesta del SPE, tales como: actuadores automáticos de válvula de corte, válvulas solenoides, válvulas de seguridad y desfogue, interruptores de arranque y paro de bombas, equipo de servicios, alumbrado, válvulas de cierre de pozos, etc.

La **Funcionalidad del SPE** considera las siguientes acciones principales

I.- Paro de emergencia por condiciones del proceso

II.- Paro de emergencia por acción manual

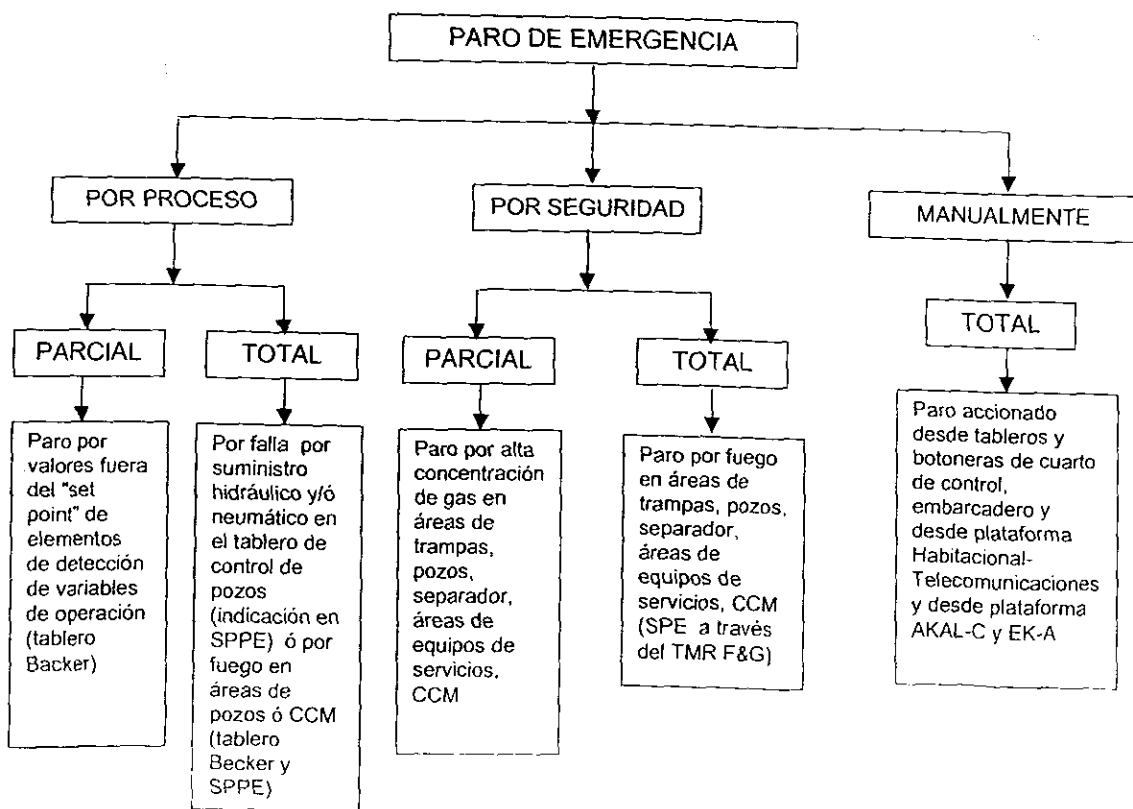
III.- Paro de emergencia por condiciones de seguridad

La UPR del SPE monitorea las condiciones de: posición y presión en válvula de corte (actuador automatizado), presión en bajantes por SCADA y en el ducto de envío, presión de los equipos y bajantes de producción de campo, niveles de toxicidad y explosividad de gases (tóxico y combustible) y flama para procesar, analizar y dar respuesta de acuerdo a la lógica que

considera condiciones anormales de operación involucradas en la matriz de paro para el disparo manual o automático secuencial, parcial o total desde la consola que monitorea y controla las funciones de paro en la plataforma ó desde botoneras localizadas en helipuerto, acceso de puente, atracaderos y en el cuarto de control en la Plataforma Habitacional-Telecomunicaciones IXTOC-A y/ó remotamente desde las plataformas AKAL-C y EK-A.

Por lo tanto un evento detectado como condición anormal acciona el SPE, aplicando comandos en todas las actividades de producción de la plataforma cerrando de manera total ó secuencial los pozos relacionando señales con el tablero de control de pozos (la Consola Baker) y con los demás sistemas de seguridad (Sistema de Detección y Alarmas Audiovisuales y Sistema Automatizado de la Red de Agua Contra incendio) que están actuando de manera independiente y a la vez ligados a la matriz.

Figura II.1 Esquema de funcionalidad del paro de emergencia de Ixtoc-A (16)



II.3 Descripción general del proceso

La Figura II.2 muestra en forma general el proceso que se lleva a cabo en la Plataforma de Perforación Ixtoc-A. Esta Plataforma cuenta con dos pozos, número 16 y 18, los cuales se encuentran fluyendo de manera natural, con una producción promedio total de aceite ligero de 9340 BPD y una Relación Gas-Aceite (RGA) de $180 \frac{m^3 \cdot gas \cdot std}{m^3 \cdot aceite}$. Esta producción es enviada por el raiser de salida de 8"x14" de diámetro desde la plataforma de telecomunicaciones hacia la batería de separación de la Plataforma de Producción PB-AC1, previo paso por la plataforma Akal-F, para su procesamiento y distribución.

Cada uno de los pozos en producción cuenta con un modulo Baker que esta instalado en la consola del mismo nombre y un tablero de interfase. Estos módulos Baker sirven como sistema de seguridad de los pozos por muy alta o muy baja presión del yacimiento o situaciones externas de emergencia, gracias al cierre de la válvula de tormenta (SCSSV) instalada aproximadamente 150 metros bajo el nivel del mar, y del sistema de seguridad superficial (SSV). Además el cierre en forma remota es a través del tablero de Interfase desde los botones de paro localizados en helipuerto, muelle y puente a telecomunicaciones, así como desde las plataformas EK-A y PB-AC-1.

La producción es manejada normalmente por las bajantes hacia el cabezal de producción, las cuales cuenta con una válvula de bola y check que no permiten el retroceso de flujo hacia los pozos. El cabezal de producción sufre una reducción súbita de 24"x8" en donde corriente abajo se encuentra instalada una válvula de corte SDV-1170.

Por otra parte se tiene un sistema de aforo de pozos mediante el que se efectúa la medición de la cantidad de gas y aceite que tiene la mezcla de cada uno de los pozos, según el programa general de aforo de pozos del Activo. Este sistema consta de un cabezal de grupo de prueba como conducto de alimentación al separador de prueba, el cual separa las fases presentes en la mezcla, y por medio de dos medidores de flujo localizados, uno en la salida de gas y el otro en la salida de aceite, la mezcla nuevamente se vuelve a unir para entrar al cabezal de producción. Aquí se encuentra una línea de derivación alineada al quemador Boom, en caso de requerirse.

Además, la plataforma cuenta con las instalaciones necesarias para la recepción y/o generación de los servicios auxiliares necesarios que se requieren para la recolección de crudo, tales como, el sistema de aire para los instrumentos y el sistema de desfogue.

El aire para los instrumentos es suministrado por medio de dos compresores, siendo uno de ellos relevo del otro y un paquete de secado de aire, donde sus usuarios principales son la consola Baker y los instrumentos de control del proceso. El sistema de desfogue de la plataforma está formado por cabezales de desfogue con la función de alinear flujo al quemador Boom en operación de aforo de los pozos.

Por último, es importante mencionar que en esta plataforma también se encuentra un paquete de potabilización de agua de mar mediante ósmosis inversa, tres tanques de almacenamiento de agua potable con sus respectivas bombas de distribución, para dar servicio a la plataforma habitacional-telecomunicaciones.

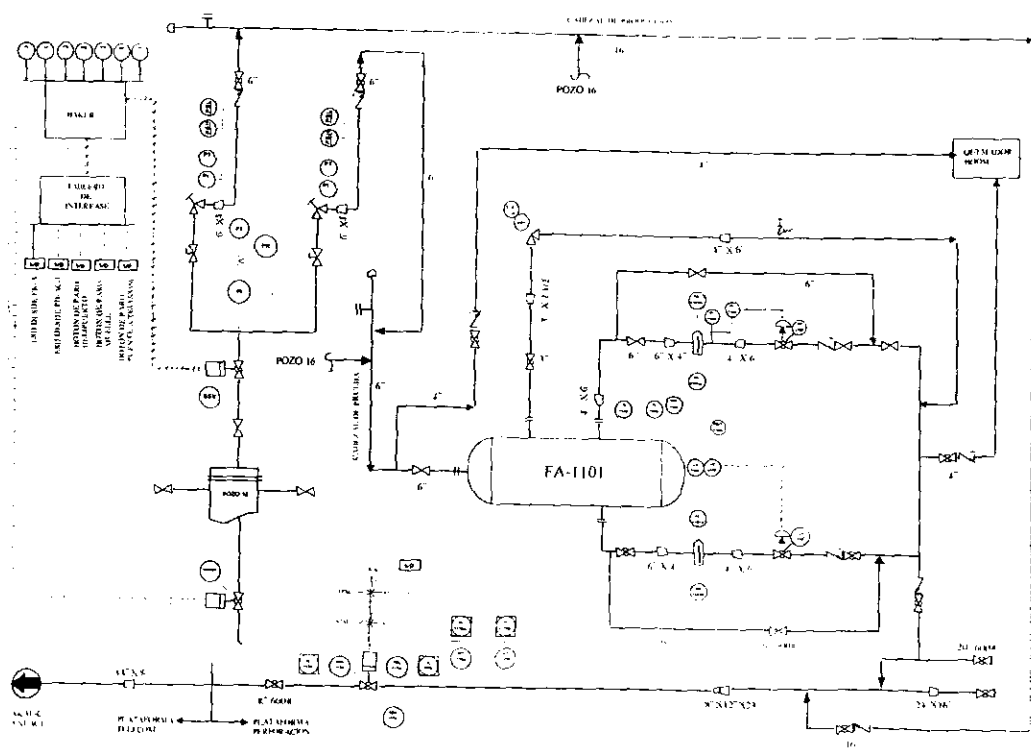


Figura 11.2 Diagrama general de Proceso de la Plataforma de Perforación Ixtoc-A (17)

II.4 Paro de emergencia por condiciones de proceso (16)

El Paro de Emergencia por proceso incluye las condiciones de operación anormal del proceso que signifiquen algún riesgo y que de mantenerse o aumentar puedan ocasionar algún daño al personal, instalaciones y medio ambiente.

Se contempla el paro total de la plataforma, tanto por proceso como en forma manual debido a disparos por alta o baja presión en el cabezal de envío de mezcla, por detección de fuego a través del sistema de F & G o por los botones eléctricos ubicados en diferentes puntos de la plataforma, esto ocasionaría el cierre de la válvula de corte SDV-1170 y el cierre total de pozos. En lo que respecta al paro parcial, es decir el cierre de un solo pozo se efectúa mediante dispositivos ubicados en campo, tales como los interruptores de presión en las bajantes de producción, los cuales actuarán por alta o baja presión directamente sobre el pozo que presente la condición anormal.

El Paro de Emergencia por proceso se aplica de manera parcial, manual y automático por la UPR de proceso, de acuerdo al análisis de señales de operación que están contenidas en el software configurado con la lógica de la Matriz, en donde el estado de una presión anormal del cabezal de producción harán disparar la válvula de corte, comunicando y alarmando de su estado (anormal) para ser evaluado.

En caso de encontrarse alineado el separador de prueba con uno o varios pozos, la secuencia interna de la lógica de la Matriz de la UPR de paro mandará a cerrar las válvulas SCSSV y SSV por medio del tablero de control de pozos (la consola Baker) y posteriormente la SDV, permitiendo con esta operación desplazar el gas y el crudo contenido en la línea del cabezal de producción hacia la salida de la válvula de desfogue del separador y/o la salida al quemador.

La lógica de Paro de Emergencia por proceso está ligada a los sensores y detectores de las variables de operación y a la condición de emergencia de paro parcial ó total mediante la función de la matriz, emitiendo información de acciones de diferentes tipos de condición de prevención y emergencia de tipo operativo y del proceso de producción según lo detectado en las consolas de mano de producción en los cuartos de control de IXTOC-A y AKAL-C.

La única consideración de paro total de proceso fuera de las variables de operación es por detección de fuego en la zona de pozos, situación que se encuentra integrada en la matriz de paro de la plataforma.

II.5 Paro de emergencia por acción manual (16)

El paro de emergencia puede hacerse en forma manual por el personal (capacitado y autorizado) que se encuentre abordo de la plataforma de perforación, desde las estaciones manuales o interruptores remotos dentro de la misma plataforma o en las plataformas habitacional-telecomunicaciones y/o servicios de almacenamiento y carga de combustible, aplicando también para este caso la plataforma AKAL-C.

Debido a la complejidad e importancia de esta filosofía de paro de Emergencia, todo el personal de operación y mantenimiento debe estar debidamente capacitado para poder llevar a cabo estas funciones, dándose por un hecho que las actividades a realizarse como emergencia deben estar integradas como parte del plan de contingencias de la plataforma Ixtoc-A.

El paro de emergencia manual podrá ser parcial ó total. En forma parcial desde el tablero Baker que incluye cierre de pozos en forma independiente (Pozo No. 16 ó Pozo No. 18). Las condiciones de la eventualidad del riesgo y análisis de la situación de un evento de condición anormal serán decisión del personal operativo al mando de la operación del proceso de producción en el momento del incidente detectado.

El Paro de Emergencia manual total que incluye el paro general de pozos (cierre de válvulas SCSSV y SSV), aplica desde la consola del cuarto de control mandando señal de mando al tablero de control de pozos (la Consola Baker), o remotamente de las botoneras de paro total ubicadas en: plataforma de perforación, plataforma habitacional-telecomunicaciones, plataforma de servicios de almacenamiento y carga de combustible, consola central de mando de la plataforma AKAL-C y consola central de mando en la plataforma EK-A.

En caso de que en el momento de eventualidad se encuentre alineado algún pozo al separador de prueba (por aforo ó mantenimiento) la lógica de funcionamiento de paro (incluida en la matriz) debe realizar la secuencia para efectuar el desfogue respectivo con la ayuda de la válvula de venteo del separador y accionando el encendido del Quemador de la plataforma.

La funcionalidad del Paro de Emergencia manual con respecto al sistema de alarmas visibles y audibles esta contemplado en la matriz de paro para accionar las alarmas audiovisuales de manera que según sea la condición del estado de una operación anormal y que se haya accionado manualmente un disparo de emergencia, el sistema de alarma funcionará de acuerdo al tipo de botón accionado, informando visual y auditivamente el tipo de situación prevaleciente con las respectivas instrucciones de acciones a tomar.

Una vez que se haya pulsado el botón de paro de emergencia desde cualquiera de las botoneras existentes, el sistema retarda la acción de cierre de válvulas a un máximo de 45 segundos para permitir que sea inhibida la secuencia de paro de emergencia desde la consola de control.

La condición de paro total se considera necesaria cuando:

- a. Existe fuego en los pozos o falla de suministro hidráulico/neumático para el tablero de control de pozos (la Consola Baker).
- b. Cuando se presente alguna situación crítica del proceso en la Plataforma Akal-C1 (la cual maneja la producción de la Plataforma de Perforación de Ixtoc-A).
- c. Cuando se presente la detección del fenómeno de contrapresión fuera de control en el flujo del crudo de la Plataforma Ixtoc-A en su trayectoria entre Akal-F, Akal-C y Akal-C1.
- d. Cuando se presente la detección de fuga en el ducto de la producción entre las plataformas Ixtoc-A, Akal-C, Akal-F y Akal-C1.

II.6 Paro de emergencia por condiciones de seguridad (16)

De manera independiente al proceso (desde el punto de vista hardware y software) las acciones de monitoreo, análisis y respuestas por condiciones detectadas como normales en el estado de las instalaciones y con respecto a los límites permisibles de operatividad en todas las zonas de riesgo de las instalaciones de la plataforma Ixtoc-A son procesadas por la UPR de Paro de Emergencia.

Las señales incluidas en el monitoreo de condiciones de operatividad de las instalaciones desde el punto de vista seguridad del personal incluyen las de los sensores de detección de gas (tóxico y combustible) y fuego, en caso de que algunas de las áreas o varias de ellas simultáneamente sobrepasen los límites permisibles de concentración predeterminados (explosividad, toxicidad y flama). Para el caso de los detectores de gas y que en otro caso sea detectada flama, la UPR de paro de emergencia analizará e informará la condición anormal y se comunicará a la UPR del proceso (relación de liga incluida en la matriz de paro de emergencia) para ejecutar entre ambas la secuencia de paro a seguir dependiendo de la gravedad y zona del evento detectada como situación de riesgo controlando, previniendo y eliminando riesgos y peligros eminentes.

El Paro de Emergencia por condiciones de seguridad puede ser total o parcial de manera secuencial o de una sola acción de disparo dependiendo de las situaciones incluidas en la matriz de paro:

- a. Cuando se ha detectado fuego o alta concentración de gas (tóxico o combustible) y que por sus dimensiones represente riesgo para el personal que se encuentre en las instalaciones de la plataforma, así como para el CCM y los equipos de operación y servicios de la misma.
- b. La condición de paro total (con posibilidad de accionamiento manual) se considera necesaria cuando existe fuego en la zona de pozos o por falla de suministro hidráulico/neumático para el tablero de control de pozos (la consola Baker).
- c. El paro ocasionado por detección de alta concentración de gas tóxico ó gas combustible se incluye en la lógica como alarma audiovisual de detección para tomar acciones correctivas en la secuencia de paro correspondiente, la cual no podrá ser total y solo se accionara como parcial, para localizar la falla, controlar, aislar, evitar la continuación de la falla, evitar la *propagación del gas detectado* y corregir la posible fuga. Si la secuencia de paro se activa por este motivo (detección de gas) el lógico de la matriz debe eliminar la fuga deteniendo la producción si así lo considera necesario dependiendo del área donde se localice la falla (área de pozos, área de equipos y área del CCM).
- d. Si el sistema detecta fuego en cualquier zona se debe cerrar en forma automática la válvula de corte SDV-1104 y se deben cerrar los pozos (cierre de válvulas SCSSV y SSV), adicionalmente el sistema deberá detectar su localización para tomar las medidas de aislamiento de la zona para evitar la propagación del fuego accionando los mecanismos del sistema contraincendio incluidos también en la matriz de paro de emergencia. En el caso de que el fuego se propague, dentro de la lógica de la matriz de paro se considerará que este evento represente un riesgo de posibles consecuencias mayores de manera que la lógica de la matriz interpretará la acción como paro total de toda la plataforma.
- e. Para la condición de que en el momento de la detección de fuego se encuentre algún pozo alineado al separador de prueba, la secuencia de paro debe incluir el venteo del gas con la válvula de descarga del separador y el desfogue del fluido líquido via quemador.

La lógica de paro de emergencia por seguridad esta ligada a los sensores y detectores de valores, previos a la condición de emergencia y mediante la función en la matriz, que a su vez esta ligada a alarmas audibles y visibles que emiten información de acciones de diferentes tipos de condición de prevención y emergencia desde la detección de altas concentraciones de gases (tóxicos y combustibles), hasta el desembarcar o abandonar las instalaciones.

El Sistema de Detección y Alarmas, Sistema Automatizado de la Red de Agua Contraincendio y el CCM, como principales integrantes de señales de la matriz de paro de emergencia, tienen la función de informar, prevenir y alertar a nivel plataforma de las condiciones anormales de operación y equipos que la contienen.

Dentro de la lógica de paro de emergencia se incluye la función de informar, prevenir y alertar, cuando el personal de la plataforma y que por condiciones operativas de seguridad active una condición de paro parcial o total, el Sistema de Detección y Alarmas emita un tono sonoro de identificación particular del evento, así como la emisión de una alarma visible con un destello luminoso de un color y secuencia característico correspondiente al tipo de evento que sirve para alertar al personal de la plataforma y además alertando a personal de embarcaciones e instalaciones próximas sobre la situación de emergencia que prevalece en la plataforma, para los efectos de prestar ayuda hacia el personal de la plataforma IXTOC-A en peligro.

II.7 Normatividad aplicada

ISA-S91.0	Sistema de paro de emergencia
ISA-S84.01	Aplicación de Sistemas Instrumentados de Seguridad
ISA-S84.02	Técnicas de evaluación de niveles Instrumentados de Seguridad
OSHA-29 CFR 1910.119	Administración de la seguridad en procesos químicos altamente peligrosos
OSHA-29 CFR 1926.64	Guías de cumplimiento y recomendaciones para administración de la seguridad de procesos
OSHA-40 CFR 48	Programas de administración de riesgo para prevención de accidentes
API RP 14C	Prácticas recomendadas para el análisis, diseño, instalación y pruebas de sistemas de seguridad a bordo de plataformas marinas de producción

III. NIVELES DE INTEGRIDAD DE SEGURIDAD

Los estándares ISA S84.01 e IEC 61508 requieren que un nivel de integridad de seguridad (SIL) esté asignado para cualquier nuevo o adaptado sistema instrumentado de seguridad (SIS). El SIS consiste en la instrumentación o los controles que están instalados con el fin de atenuar el peligro o de traer al proceso a un estado seguro en el acontecimiento de un trastorno del proceso. Un SIS se utiliza para cualquier proceso en el cual el análisis de peligros del proceso (PHA) haya determinado que la integridad mecánica del equipo de proceso, del control de proceso, y de otro equipo protector es escasa para atenuar el peligro potencial.

Las designaciones del nivel de seguridad se pueden correlacionar a la probabilidad para fallar y a los requisitos de la disponibilidad del SIS. Según lo mostrado en la Tabla III.1, el IEC 61508 reconoce SIL 4 que el estándar ISA S84.01 no contempla.

SIL		DISPONIBILIDAD DE LA SEGURIDAD	PROBABILIDAD DE FALLA EN DEMANDA (PFD)	1/PFD
IEC 61508	ISA S84.01			
4		> 99.99%	1 E-005 a 1 E-004	100,000 a 10,000
3	3	99.90 – 99.99%	1 E-004 a 1 E-003	10,000 a 1,000
2	2	99.00 – 99.90%	1 E-003 a 1 E-002	1,000 a 100
1	1	90.00 – 99.00%	1 E-002 a 1 E-001	100 a 10

Tabla III.1 Correlación del SIL con la disponibilidad y la probabilidad de falla (PFD)

III.1 Conceptualización de los niveles de seguridad (18)

El concepto del nivel de seguridad (SIL), con respecto a ISA S84.01-1996 e IEC 61508, existe actualmente en alguna parte entre la ciencia-ficción y la comercialización. La versión de la ciencia-ficción es limitada por una creencia que SIL describe el funcionamiento absoluto del SIS en términos de incidentes potenciales. Los vendedores y proveedores del servicio, que hacen demandas referentes al funcionamiento del producto, controlan la opinión de la comercialización. Ninguna de las dos opiniones es correcta.

SIL es una medida del funcionamiento del SIS relacionado solamente con los dispositivos que abarcan el SIS. Esta medida se limita a la integridad del dispositivo, configuración, pruebas,

diagnóstico y los incidentes comunes inherentes al diseño específico del SIS. No se relaciona explícitamente con una matriz de causa y efecto, sino que se relaciona con los dispositivos usados para prevenir un incidente específico. Además, SIL no es una característica de un dispositivo específico. Es una característica del sistema; dispositivos de entrada de información a través del resolutor de la lógica a los dispositivos de salida. Finalmente, SIL no es una medida de frecuencia del incidente. Se define como la probabilidad (del SIS) para fallar en demanda (PFD). Una demanda ocurre siempre que el proceso alcance la condición de disparo y hace que el SIS tome la acción correctiva.

Debe ser entendido que SIL y la disponibilidad son representaciones simplemente estadísticas de la integridad del SIS cuando ocurre una 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 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 alcanzara el punto de alto nivel, habría un incidente predicho del SIS y el desbordamiento subsecuente del tanque. ¿Está esto dentro del riesgo aceptable?

Una explicación simple del lazo entre la frecuencia del incidente y SIL es considerar una rueda de la suerte. Esta consiste en una rueda horizontal que contiene ranuras numeradas. Se hace girar la rueda y una bola se sacude sobre la rueda. En un establecimiento del juego, las apuestas se ponen en una ranura específica numerada. Si la bola aterriza en la ranura seleccionada por el jugador, la casa paga a este.

En un juego de la ruleta de SIL, la bola representa SIL # y la ocasión, o probabilidad de que la bola de SIL aterrice en una ranura específica en la rueda que ha sido definida por estándares internacionales.

SIL	CATEGORIAS DE LA PROBABILIDAD
1	1 en 10 a 1 en 100
2	1 en 100 a 1 en 1,000
3	1 en 1000 a 1 en 10,000
4	1 en 10,000 a 1 en 100,000

Tabla III.2 Categorías de la probabilidad

En un juego de la ruleta de " SIL 1 ", se asume que hay diez ranuras (mínimo requerido para SIL 1). Una ranura se pinta de rojo; las otras nueve se pintan de negro. La rueda comienza a girar y la bola se sacude sobre la ruleta cuando ocurre una demanda de proceso, es decir, se incrementa el nivel de líquido dentro de un tanque. Si la bola aterriza en cualesquiera de las nueve ranuras negras, la función de seguridad trabaja, es decir, la válvula de vaciado abre y baja el nivel. Si la bola aterriza en la ranura roja, la función de seguridad no trabaja y la acción para la cual fue diseñada la función de seguridad para prevenir, ocurre, es decir, el desbordamiento del tanque. Como los desbordamientos del tanque son a menudo un producto del número de vueltas (demanda del proceso) y de la relación de transformación de ranuras rojas a ranuras negras (PFD o SIL), en este juego, el jugador puede controlar la probabilidad del éxito controlando el número de ranuras (SIL) y minimizar la frecuencia del incidente reduciendo el número de vueltas (demandas del proceso).

¿Cuántas ranuras se requieren y qué acciones se deben tomar para reducir el número de demandas del proceso con base en el riesgo percibido y la frecuencia tolerable del incidente?. El riesgo, según lo identificado durante el análisis de peligros del proceso, es esencialmente la "apuesta" colocada en la ranura roja. La apuesta puede consistir en lesiones, fatalidades, daños ambientales, daño de propiedad y equipo, violaciones del permiso y la licencia de operación de la planta. Si la apuesta es pequeña, es decir, alto nivel en un tanque que ocurre diez veces por año, con la consecuencia potencial del desborde de agua en un dique, diez ranuras son quizá aceptables con una frecuencia resultante del incidente de una vez al año.

Si la apuesta es grande, es decir, de alta presión en un recipiente de proceso con el potencial para la ruptura, fuga de gas inflamable, ignición subsecuente, y las fatalidades múltiples y daños catastróficos que ocurren una vez en 10 años, quizá se requieran 1,000 ranuras con una frecuencia resultante del incidente de 1 de 10,000 años.

En la mayoría de la literatura, SIL se refiere como criterio del funcionamiento y capacidad de la función de seguridad a realizarse en el momento que se necesita. Según lo explicado previamente, el SIL se relaciona más a menudo con el coste del incumplimiento. Sin embargo, no importa cómo se vea el SIL, el concepto representa una rotación importante en la actitud de la industria hacia el diseño del sistema de seguridad. SIL se debe elegir para reducir la frecuencia del incidente a un nivel tolerable. 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. Por lo tanto, SIL cierra el ciclo del diseño, riesgo identificado, requisitos cuantificados y diseño validado.

Una vista cualitativa del SIL se puede expresar en los términos de la consecuencia del incidente del SIS, en términos del daño del recurso, lesión de personal y de la exposición del público o comunidad.

SIL	VISTA CUALITATIVA
4	Impacto catastrófico en la comunidad
3	Impacto en la comunidad y el empleado
2	Protección de la propiedad y producción. Lesión posible del empleado
1	Protección de menor importancia de la propiedad y de la producción

Tabla III.3 Vista cualitativa de SIL

La visión cualitativa antedicha queda abierta para discusión. ¿Cuál es de menor importancia?, ¿Cuál es principal?, ¿En qué punto teórico de lesión o fatalidad ocurrirá? 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 SILs específicos para ciertos peligros del proceso. La asignación del SIL es una decisión corporativa o de compañía basada en la gerencia de riesgo y la filosofía de la tolerancia del riesgo. La advertencia es que, en un 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, la asignación de los niveles de seguridad debe ser realizada cuidadosamente y ser documentada a conciencia.

Fijar el SIL para un SIS implica típicamente la consideración de:

- consecuencia del acontecimiento
- probabilidad del acontecimiento
- Sistemas protectores adicionales para la prevención y mitigación del peligro

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

III.2 Métodos para determinar el SIL

Se asignan los niveles de seguridad después de que el PHA haya concluido que un SIS es requerido. Un PHA se realiza para identificar peligros potenciales en la operación de un proceso. El rango de PHA's va desde análisis muy simples hasta análisis complejos como el Estudio de Riesgos y Operabilidad de Procesos (HAZOP). El HAZOP es una examinación sistemática y metódica del diseño de proceso que utiliza a un equipo multidisciplinario para identificar peligros o problemas de operabilidad que podrían dar lugar a un accidente. El HAZOP proporciona a una base dada la prioridad para la puesta en práctica de las estrategias de mitigación del riesgo, tales como SIS o Sistemas de Paro de Emergencia (ESD).

Cuando se termina el HAZOP, el riesgo asociado al proceso, en términos de la severidad y probabilidad debe ser entendido. Se establece la severidad del acontecimiento con base en una cierta medida del impacto anticipado o consecuencia del incidente. Esto puede incluir:

- Consecuencias en sitio
 - lesión o muerte del trabajador
 - daños de equipo
- Consecuencias fuera del sitio
 - exposición de la comunidad, incluyendo lesión y muerte
 - daños materiales
- Consecuencias para el medio ambiente
 - emisión de productos químicos peligrosos
 - contaminación del aire, suelo y abastecimientos de agua
 - daños a las áreas ambientalmente sensibles

La probabilidad del riesgo es determinada estimando la probabilidad de la ocurrencia prevista. La probabilidad se clasifica como índice alto, medio o bajo de la ocurrencia. Esto a menudo se determina basándose en la experiencia de funcionamiento de la compañía o historia de operación de la industria.

La opción del método de la asignación de SIL es dependiente de la metodología corporativa existente del gravamen de riesgo. Existen varios métodos para convertir datos de HAZOP en los niveles de seguridad (SIL), incluyendo:

- HAZOP modificado
- Consecuencia solamente
- ALARP
- Matriz del riesgo
- Gráfico del riesgo
- Gravamen cuantitativo
- SIL asignado por mandato corporativo

Estos métodos serán discutidos abajo, junto con algunos criterios para elegir el método.

III.2.1 HAZOP Modificado

El HAZOP modificado es una extensión del proceso existente de HAZOP. Es una asignación subjetiva del SIL basada en la comprensión cualitativa que tenga el equipo de trabajo de la severidad y probabilidad del incidente. Este método confía principalmente en la experiencia y conocimiento de los miembros del equipo. La experiencia y conocimientos requeridos se extienden más allá de la comprensión simple de la operación del proceso. Debe incluir una comprensión del riesgo del proceso y de la tolerancia aceptable del riesgo de la compañía. El SIL es asignado cualitativamente examinando el potencial del riesgo y seleccionando un SIL que parezca apropiado por la valoración del equipo del riesgo. Puesto que la asignación es muy subjetiva, necesita existir coherencia entre el personal del equipo de la asignación del SIL y el equipo de PHA.

III.2.2 Consecuencia Solamente

La técnica más conservadora, consecuencia solamente, utiliza una valoración de la consecuencia potencial del incidente. La frecuencia del incidente no se considera, por lo tanto, todos los incidentes que den por resultado fatalidades posibles, tendrían el mismo SIL sin importar que tan frecuente o remoto pudiera ocurrir el incidente. Una tabla de decisión de la consecuencia solamente puede aparecer según lo mostrado en la Tabla III.4.

SIL	CONSECUENCIA
4	potencial para las fatalidades en la comunidad
3	potencial para las fatalidades múltiples
2	potencial para lesiones serias importantes o una fatalidad
1	potencial para lesiones de menor importancia

Tabla III.4 Tabla de decisión de la consecuencia solamente

Este método, mientras que conservador, es la herramienta más simple a utilizar, porque el equipo no necesita estimar la probabilidad del incidente, que es a menudo la valoración más difícil que el equipo tiene que hacer. Este método es especialmente apropiado cuando la historia del proceso es muy limitada, que contribuye substancialmente a la dificultad en definir la probabilidad.

III.2.3 ALARP

En esta metodología, el riesgo asociado a un proceso se ve en los términos de la ventaja y del coste asociados a esfuerzos para la reducción del riesgo. Según la metodología, el riesgo se debe reducir tan bajo como razonablemente practicable (ALARP, As Low As Reasonably Practicable), centrándose en una definición del riesgo tolerable. La figura III.1 muestra un diagrama de ALARP, donde el riesgo se representa gráficamente como triángulo invertido. Mientras se reduce el riesgo, el triángulo llega a ser más pequeño hasta que el riesgo llega a ser insignificante. El riesgo del proceso esencialmente se divide en tres porciones: riesgo inaceptable, ALARP y costo inaceptable. En la región de ALARP, el coste asociado al diseño de SIS se compara con la cantidad de reducción del riesgo alcanzada usando el SIS. El riesgo no se puede eliminar, incluso si se expande el dinero infinitamente (figura III.2).

Mientras que el coste contra la filosofía de la ventaja hace esto una metodología atractiva, se debe tener cuidado en la puesta en práctica. La ventaja asociada al instalar o mejorar un diseño del SIS es a menudo una reducción en el número de lesiones o fatalidades. Para cerciorarse de que las ventajas estén medidas tan cuidadosamente como los costes percibidos, el utilizador de este método debe poner un valor cuantificado a cada lesión o fatalidad potencial. Si no, un

presupuesto de proyecto individual determinaría el valor. Esto es inaceptable desde un punto de vista corporativo del riesgo.

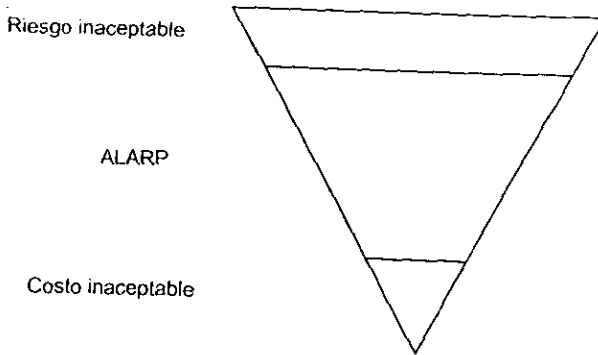


Figura III.1 Diagrama de ALARP para la tolerancia del riesgo (19)

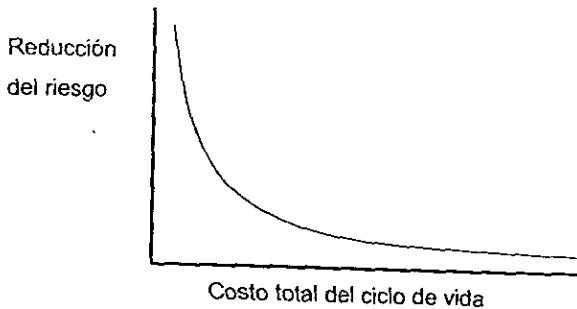


Figura III.2 Lazo entre la reducción del riesgo y el coste del ciclo de vida (19)

III.2.4 Matriz del riesgo

Una de las técnicas más comunes, entre las refinerías, compañías dedicadas a la elaboración de productos químicos y compañías petroquímicas, es la matriz del riesgo, que proporciona una correlación entre el SIL, la severidad y la probabilidad del riesgo. El método de matriz del riesgo permite que la probabilidad del acontecimiento potencial sea considerada durante la asignación de SIL.

Una matriz corporativa del riesgo proporciona control del SIL asignado para una severidad y probabilidad determinadas. Durante la fijación de la severidad y probabilidad del incidente, las

capas disponibles de protección deben ser evaluadas y el efecto sobre la severidad y probabilidad del incidente debe ser determinado. Para la consideración de la reducción del riesgo, las capas de protecciones deben ser independientes, comprobables, confiables y diseñadas para la mitigación del riesgo específico. La figura III.3 muestra una matriz dimensional.

Cuando se desea que el método proporcione la capacidad para considerar formalmente las capas independientes de protección, una matriz tridimensional del riesgo puede ser utilizada (figura III.4). La fijación de la probabilidad y severidad se hace sin la consideración de ninguna capa adicional de protección. La cantidad de crédito tomada para la reducción del riesgo inherente en cada capa es controlada por los valores de SIL asignados en la matriz tridimensional. Esto proporciona un control mejor en la cantidad de reducción del riesgo que es asumido por cada capa aplicada de la protección.

Para que este método sea utilizado con éxito, el proceso y su riesgo asociado deben ser bien entendidos para poder hacer la valoración cualitativa de la probabilidad y severidad. El gravamen de la probabilidad es lo más difícil que tiene que hacer el equipo asignado, debe haber una cierta comprensión general del equipo en cuanto a la frecuencia de los últimos incidentes en el sitio o grupo industrial general.



Figura III.3 Matriz dimensional del riesgo (19)

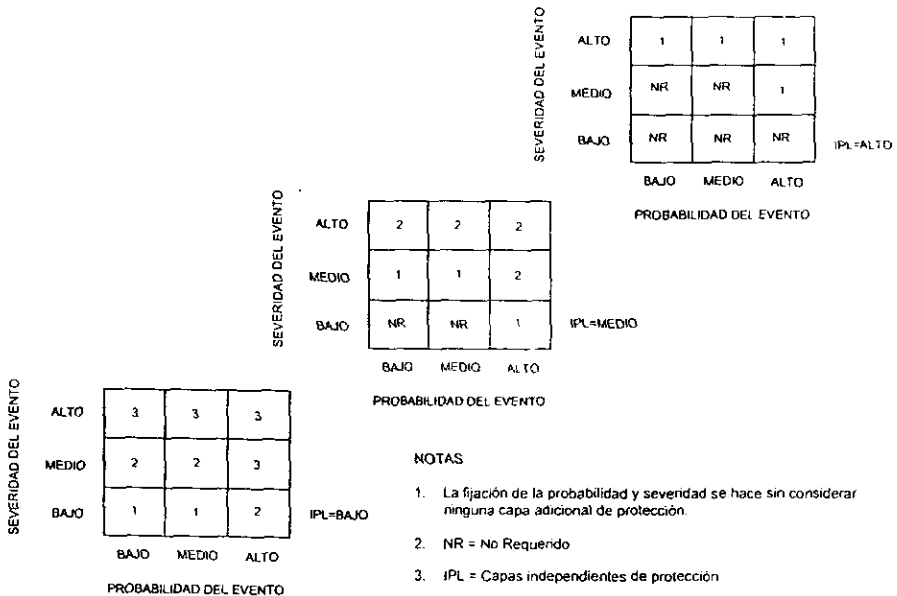


Figura III.4 Matriz tridimensional del riesgo (19)

III.2.5 Gráfico Del Riesgo

Los gráficos del riesgo son muy similares a las matrices del riesgo. Un gráfico del riesgo proporciona una correlación de SIL basada en cuatro factores:

- 1) consecuencia (C),
- 2) tiempo de la frecuencia y exposición (F),
- 3) posibilidad de evitar el acontecimiento peligroso (p), y
- 4) probabilidad de la ocurrencia indeseada (w).

Este método es una técnica cualitativa que requiere herramientas avanzadas para ser desarrollada, de tal forma que se asegure que los cuatro parámetros enumerados arriba están elegidos correctamente. La mayoría de la evaluación se centra en el riesgo de una persona individual. Los cuatro factores se evalúan desde el punto de vista de una persona teórica que

está en la zona de impacto del incidente. Para este método, la probabilidad y consecuencia son determinadas considerando las capas independientes de la protección durante el gravamen. Una vez que se determinen estos factores, el gráfico del riesgo se utiliza para determinar el nivel de reducción mínimo del riesgo y el SIL asociado. Como en el caso de la matriz del riesgo, un gráfico corporativo del riesgo debe ser desarrollado. Un ejemplo del gráfico del riesgo se muestra en la figura III.5.

CONSECUENCIA	DEFINICIÓN	PROBABILIDAD DE OCURRENCIA	DEFINICIÓN	NIVELES DE SEGURIDAD	DEFINICIÓN
C1	BAJO	W1	MUY PEQUEÑA	-	NO REQUERIDO
C2	INTERMEDIO	W2	PEQUEÑA	a	NO REQUERIMIENTOS ESPEC.
C3	ALTO	W3	RELATIVAMENTE ALTA	b, c	1
C4	MUY ALTO			d	2
				e, f	3
				g	4
				h	NO ES SUFICIENTE UN SOLO SIS

FRECUENCIA	DEFINICIÓN	POSIBILIDAD DE EVITAR EL ACCID.	DEFINICIÓN
F1	RARO A FRECUENTE	P1	A VECES POSIBLE
F2	FRECUENTE A CONTINUO	P2	CASI IMPOSIBLE

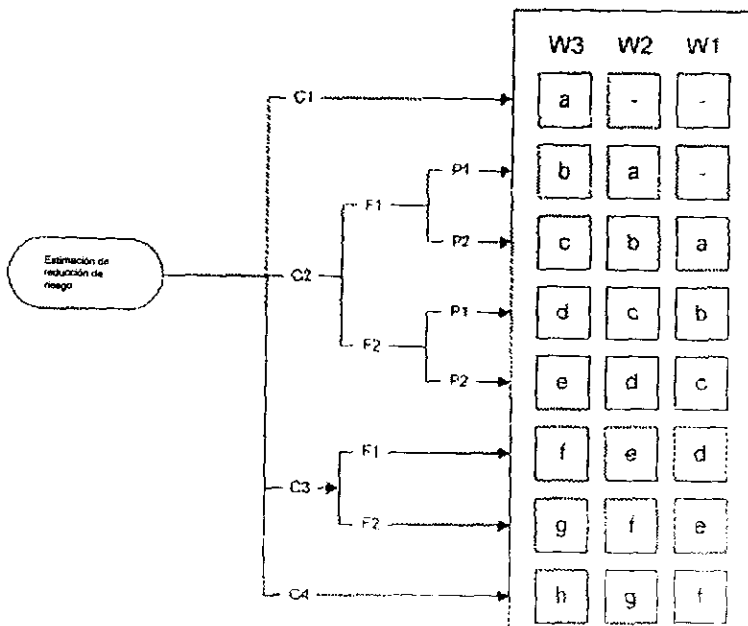


Figura III.5 Ejemplo de gráfico de riesgo

III.2.6 Análisis Cuantitativo

El acercamiento cuantitativo a la asignación del SIL es la técnica más rigurosa a utilizar. El SIL es asignado determinando la probabilidad de la demanda del proceso o del incidente cuantitativamente. Las causas potenciales del incidente se modelan usando una técnica cualitativa de fijación del riesgo, un árbol de incidentes, tal como se muestra en la figura III.6. La técnica cuantitativa se utiliza a menudo cuando hay información histórica muy limitada sobre el proceso, de modo que la determinación cualitativa de la probabilidad sea extremadamente difícil. El método requiere una comprensión completa de las causas potenciales del acontecimiento y de una probabilidad estimada de cada causa potencial.

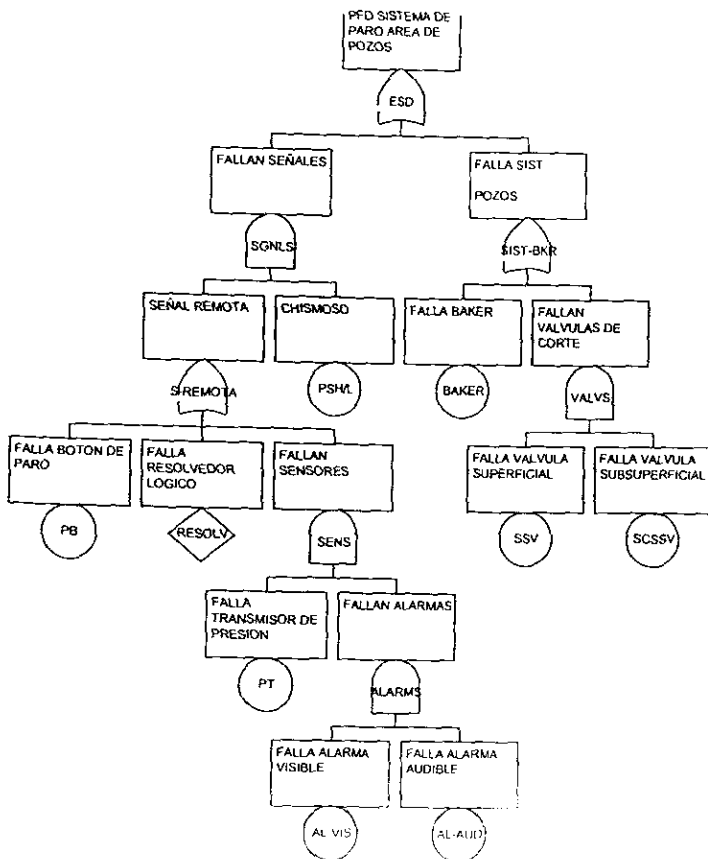


Figura III.6 Ejemplo de árbol de fallas (17)

Para determinar el SIL requerido, la frecuencia validada o tolerable del riesgo es dividida por la demanda del proceso calculada como sigue:

$$\text{Probabilidad de falla en demanda} = \text{Frecuencia tolerable del riesgo} / \text{Demanda del proceso}$$

El inverso de esta ecuación se utiliza para determinar el factor de reducción del riesgo (RRF).

$$\text{RRF} = \text{Demanda del proceso} / \text{Frecuencia tolerable del riesgo}$$

Sin importar que ecuación se utilice, la reducción calculada del riesgo se compara al nivel requerido de seguridad.

III.2.7 SIL asignado por mandato corporativo

La técnica final es el método que consume menos tiempo, este es adoptado por muchas plantas químicas pequeñas que no desean invertir en mano de obra extensa a las metodologías de la asignación de SIL. Este método reconoce que ocurre el aumento más grande del coste cuando se toma la decisión que el SIL debe ser más alto que SIL 1. La selección de SIL 2 o SIL 3 fuerza el diseño del SIS hacia redundancia y diversidad de dispositivos de control. Con este reconocimiento, muchas compañías pequeñas están tomando el acercamiento que " un sistema de seguridad es un sistema de seguridad y por lo tanto debe ser SIL 3 ". Esto elimina argumentos como: si el escape es posible, alguien será dañado o matado, el impacto será en sitio y/o fuera del sitio, etc. Salva tiempo en el proceso de PHA, reduce la documentación en la alineación de opción del SIL y asegura estado coherente a través de unidades de proceso.

IV DETERMINACIÓN DEL NIVEL DE INTEGRIDAD DE SEGURIDAD EN EL SISTEMA DE DETECCIÓN, ALARMA Y PARO DE EMERGENCIA PARA LA PLATAFORMA IXTOC-A (17).

IV.1 Etapas del Ciclo de Vida de Seguridad

A continuación se describen las etapas del Ciclo de Vida de la Seguridad de la ISA-S84.01-1996 involucradas en la determinación del SIL, Figura IV.1.

1. Diseño Conceptual del Proceso en estudio. En este caso nos referimos al sistema de paro de emergencia de la plataforma de perforación Ixtoc-A.
2. Análisis de Peligro del proceso (PHA, Process Hazard Analysis). Por medio de este se identifican los peligros potenciales o eventos no deseados inherentes en la operación del proceso. Específicamente para la identificación de los eventos no deseados de los sistemas involucrados en el proceso de producción de la plataforma Ixtoc-A, se utilizaron los resultados obtenidos del Estudio de Peligro y Operabilidad (HAZOP), elaborado por el IMP.
3. De lo anterior surge la necesidad de considerar la adición de una capa de protección al proceso denominada Sistema de Paro de Emergencia (SPE) para reducir la probabilidad de ocurrencia del evento no deseado, llevando al proceso a un estado seguro.
4. Puesto que se definió que para la reducción del riesgo se requiere de un SIS, este debe cumplir con un Nivel de Integridad de Seguridad (SIL).
5. La disponibilidad del SPE se mejora con la adición de redundancia en elementos sensores y finales de seguridad, mayor frecuencia en los periodos de prueba y uso de diagnóstico de fallas. También se mejora a través de una buena operación y procedimientos de mantenimiento.
6. Desarrollar Especificación de los Requerimientos de Seguridad (SRS, Safety Requirement Specification). SRS consiste de Requerimientos Funcionales y de Integridad de seguridad. Los requerimientos funcionales prueban la lógica y acciones que deben de tomarse por el SPE y las condiciones bajo las cuales estas acciones son iniciadas. De manera análoga, los requerimientos de Integridad documentan el SIL deseado para la ejecución de las funciones del SPE, incluyendo el SIL para cada interlock o sistema, requerimientos de confiabilidad y si los paros en falso pueden resultar en un evento peligroso.
7. El Diseño Conceptual del SPE debe cumplir con la Especificación de los Requerimientos de Seguridad (SRS). La arquitectura del SPE propuesto debe garantizar el SIL que se desea. Se considera un intervalo de prueba para alcanzar el SIL deseado y el diseño conceptual

debe ser verificado contra el SRS. Para esta determinación se considera un intervalo de prueba funcional en general que puede ser hasta de 6 meses en cada interlock o sistema para alcanzar el SIL requerido.

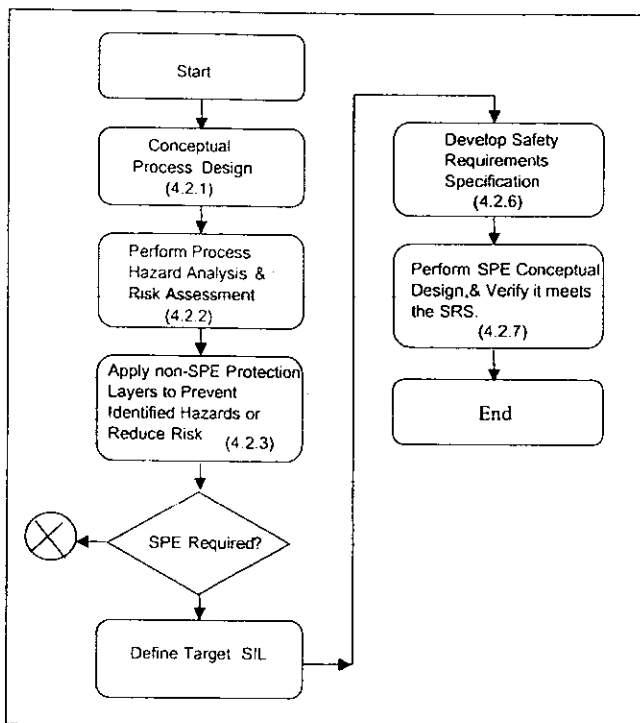


Figura IV.1 Etapas del Ciclo de Vida de Seguridad

IV.2 Análisis de Peligros del Proceso

En esta etapa se utilizó la técnica HAZOP para identificar los peligros potenciales inherentes al proceso de la plataforma Ixtoc-A, así como la matriz de riesgo en función de la severidad de la consecuencia y frecuencia de ocurrencia de las causas que originan una desviación. Lo anteriormente mencionado con el fin de jerarquizar los peligros desde el punto de vista de seguridad y operación del proceso.

Los resultados del HAZOP se encuentran contenidos en las tablas IV.1, IV.2 y IV.3; en la figura IV.2 se muestra la matriz de riesgo resultante.

VALOR	ORDEN DE LA MAGNITUD	DESCRIPCIÓN CUALITATIVA
1	Despreciable	Leves raspones o moretones por golpes de objetos. Mala operación con acción correctiva que no afecta al proceso y al equipo.
2	Muy Bajo	Cortaduras, conmociones por golpes o caídas. Pérdidas momentáneas del control de proceso.
3	Bajo	Pérdida de un dedo, mareo o contaminación por sustancias química. Daño menor de equipo.
4	Intermedio	Herido muy grave con pérdida de alguna extremidad o habilidad. Paro de equipo por daño severo.
5	Alto	Más de un muerto y daño permanente a equipo o estructura.
6	Muy Alto	Daño total de la plataforma, múltiples muertes, necesidad de reemplazar equipos y estructuras.

Tabla IV.1 Ponderación de Severidad de la Consecuencia (20).

VALOR	ORDEN DE LA MAGNITUD DE LA FRECUENCIA	DESCRIPCIÓN CUALITATIVA
1	Una vez en 10 000 años	Remotamente posible
2	Una vez en 1000 años	Sería sorprendente si ocurriera alguna vez durante el tiempo de vida de la planta
3	Una vez en 100 años	No se espera que ocurra durante el tiempo de vida de la planta, pero puede ocurrir
4	Una vez en 10 años	Probablemente ocurrirá más de una vez durante el tiempo de vida de la planta
5	Una vez al año	Ocurrencia ocasional / algunas veces durante el tiempo de vida de la planta
6	Una vez al mes	Ocurrencia frecuente o regular

Tabla IV.2 Ponderación de la Frecuencia (20).

NODO	DESVIACIONES	PONDERACION DE LA FRECUENCIA	PONDERACIÓN DE LA CONSECUENCIA	ACCIÓN (PONDERACIÓN DEL RIESGO)
1. Arbol y bajante de pozos	1.1 no-flujo	4	3	3 a 6 meses (12)
	1.2 mayor presión	3	4	3 a 6 meses (12)
	1.3 fuga/ruptura	2	5	3 a 6 meses (10)
2. Separador de prueba FA-1101	2.1 mayor presión	3	4	3 a 6 meses (12)
	2.2 fuga/ruptura	2	5	3 a 6 meses (10)
	2.3 mayor nivel	5	1	3 a 6 meses (5)
	2.4 menor nivel	4	1	6 a 12 meses (4)
3. Cabezal de producción 8"	3.1 no-flujo	3	3	3 a 6 meses (9)
	3.2 mayor presión	3	4	3 a 6 meses (12)
	3.3 fuga/ruptura	2	5	3 a 6 meses (10)
4. Acumulador de aire	4.1 menor presión	4	3	3 a 6 meses (12)
5. Quemador BOOM	5.1 no-ignición	4	3	3 a 6 meses (12)
6. Tanque de diesel sucio	6.1 fuga/ruptura	2	4	3 a 6 meses (8)
7. Centrífuga de diesel	7.1 mayor vibración	3	3	3 a 6 meses (9)
8. Tanque de diesel limpio	8.1 fuga/ruptura	2	3	3 a 6 meses (6)
Total desviaciones	15			

Tabla IV.3 Ponderación resultante del HAZOP para la plataforma Ixtoc-A (20)

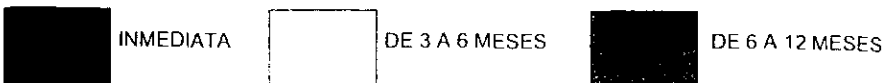
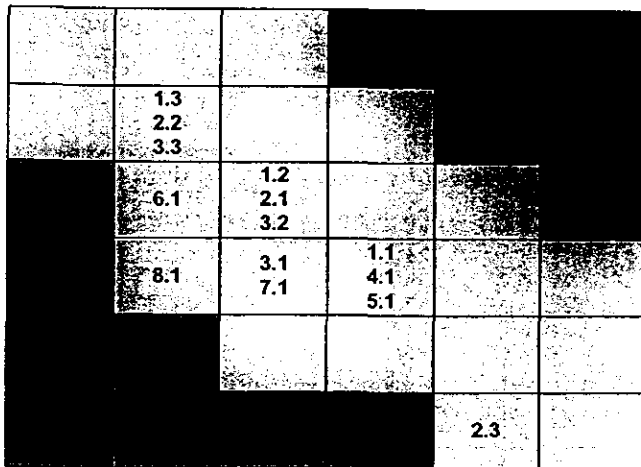


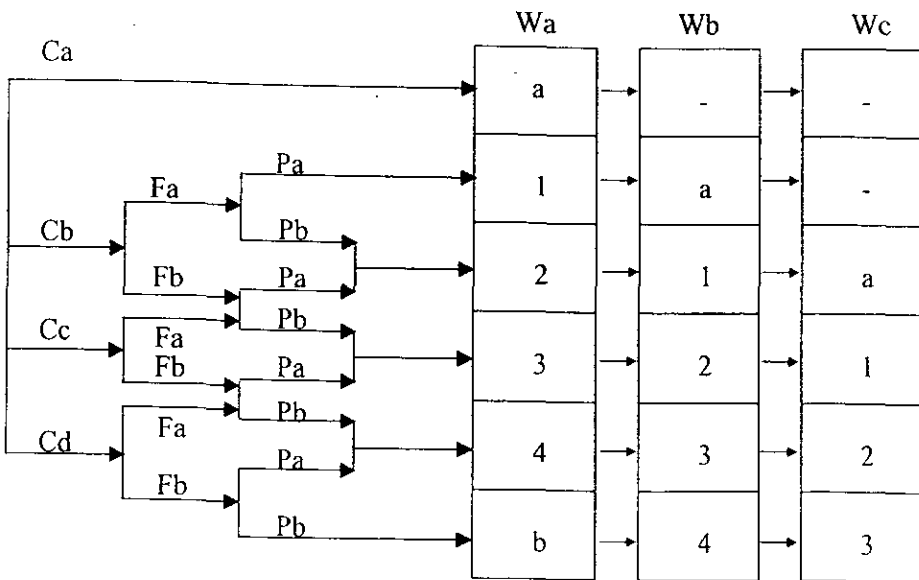
Figura IV.2 Matriz de riesgo y acciones generadas para la plataforma Ixtoc-A (20)

El estudio de HAZOP concluye que el 93.33% de las desviaciones quedan dentro de Riesgo Moderado cuyas acciones correctivas deben aplicarse en un periodo definido de 3 a 6 meses y el 6.67% restante en el área de Riesgo Bajo con un tiempo de 6 a 12 meses.

Los escenarios de mayor riesgo identificados son: 1.2 mayor presión en el árbol y bajante de pozo, 2.1 mayor presión en el separador de prueba FA-1101, 3.2 mayor presión en el cabezal de producción 8", 4.1 menor presión en el acumulador de aire, 5.1 no-ignición en el quemador Boom, 1.1 no-flujo en el árbol y bajante de pozo.

IV.3 Definición del Nivel de Seguridad

La definición del SIL para cada función de seguridad de los sistemas involucrados se realizó por medio del uso del método "gráfico del riesgo" que a continuación se muestra.



a = No requerimientos especiales de seguridad
 b = no es suficiente un solo SIS

Niveles de Integridad de Seguridad

Figura IV.3 Gráfico para la definición del SIL

- El método inicia con la determinación de los parámetros de las consecuencias Ca, Cb, Cc, Cd, que se podrían presentar si se diera el evento no deseado. Este punto se realizó durante la elaboración del estudio de HAZOP. Para cada uno de los escenarios se determinó la severidad de las consecuencias, asignándosele un número cuya descripción cualitativa es acorde a las definiciones de la Tabla IV.4, en la que también se muestra la equivalencia con los parámetros ya mencionados.

VALOR	ORDEN DE LA MAGNITUD	DESCRIPCIÓN CUALITATIVA	
1	Despreciable	Leves raspones o moretones por golpes de objetos. Mala operación con acción correctiva que no afecta al proceso y al equipo.	Ca
2	Muy Bajo	Cortaduras, conmociones por golpes o caídas. Pérdidas momentáneas del control de proceso.	Ca
3	Bajo	Pérdida de un dedo, mareo o contaminación por sustancias química. Daño menor de equipo.	Ca
4	Intermedio	Herido muy grave con pérdida de alguna extremidad o habilidad. Paro de equipo por daño severo.	Cb
5	Alto	Más de un muerto y daño permanente a equipo o estructura.	Cc
6	Muy Alto	Daño total de la plataforma, múltiples muertes, necesidad de reemplazar equipos y estructuras.	Cd

Tabla IV.4 Parámetros de Severidad de la Consecuencia.

En donde Ca = Daño Menor

Cb = Daño serio al personal, una muerte, daño a equipo

Cc = Varias Muertes, daño severo a equipos

Cd = Muchas Muertes, daño total a equipos.

- A continuación se determina la frecuencia y/o exposición del personal Fa y/o Fb, esto es, la frecuencia con la que el personal permanece dentro del área de riesgo. Considerando que el proceso puede ser continuo, es posible que la exposición no lo sea.

Fa = Raro a Frecuente

Fb = Frecuente a continuo

- Posteriormente se considera la posibilidad de evitar el accidente (Pa o Pb), esto es, si el tiempo de reacción del proceso es lo suficientemente lento para que se puedan tomar las acciones necesarias o si existen indicadores locales (sensores, alarmas) que muestren que

pasa en el proceso y además se deberá considerar si los operadores están capacitados realmente para actuar ante una situación anormal e incluso si las rutas de evacuación son las adecuadas para, de ser posible, abandonar el área.

En donde P_a = A veces posible

P_b = Casi Imposible

- Por último se determina el valor de la frecuencia o probabilidad de ocurrencia (W_a , W_b , W_c), este valor corresponde al valor de la frecuencia estipulada para los eventos no deseados y establecidas en la elaboración del estudio de HAZOP. En este valor están implícitas las capas de protección existentes tales como el control básico de proceso, alarmas y dispositivos mecánicos como PSV entre otros. En la Tabla IV.5 se indican los valores utilizados así como también se muestra la descripción cualitativa para cada valor, del mismo modo se indica también la equivalencia con los parámetros de interés para determinar el nivel de integridad de seguridad.

VALOR	ORDEN DE LA MAGNITUD DE LA FRECUENCIA	DESCRIPCIÓN CUALITATIVA	
1	Una vez en 10 000 años	Remotamente posible	W_a
2	Una vez en 1000 años	Sería sorprendente si ocurriera alguna vez durante el tiempo de vida de la planta	W_a
3	Una vez en 100 años	No se espera que ocurra durante el tiempo de vida de la planta, pero puede ocurrir	W_b
4	Una vez en 10 años	Probablemente ocurrirá más de una vez durante el tiempo de vida de la planta	W_b
5	Una vez al año	Ocurrencia ocasional / algunas veces durante el tiempo de vida de la planta	W_c
6	Una vez al mes	Ocurrencia frecuente o regular	W_c

Tabla IV.5 Parámetros de la Frecuencia.

La descripción de los parámetros es como se indica a continuación.

W_a = muy pequeña

W_b = pequeña

W_c = Relativamente alta

Con los parámetros establecidos y por medio de la Figura IV.3 se determina el valor del SIL requerido para la función de seguridad evaluada.

Es importante mencionar que básicamente esta metodología fue desarrollada para evaluar el riesgo solo al personal, pero es necesario indicar que en este tipo de instalaciones petroleras las pérdidas de producción y/o daños al equipo representan graves pérdidas económicas, por lo que es de relevante importancia incluir este tipo de daños dentro de los parámetros anteriormente mencionados. En la tabla IV.6 se muestran las consideraciones y el SIL resultante para los Pozos de Producción, Separador de prueba y Línea de Salida de Producción utilizando el método del "gráfico de riesgo".

DESCRIPCIÓN	EVENTO/NO DESEADO	CONSECUENCIA	FRECUENCIA Y/O EXPOSICIÓN	POSIBILIDAD DE EVITAR EL AC.	PROBABILIDAD DE OCURRENCIA	SIL
Pozos de producción	Sobrepresión	Cb (intermedio)	Fb (frecuente a continuo)	Pa (a veces posible)	Wb (1 vez en 100 años)	1
Separador de prueba	Sobrepresión	Cb (intermedio)	Fb (frecuente a continuo)	Pa (a veces posible)	Wb (1 vez en 100 años)	1
Línea de salida de producción	Sobrepresión	Cb (intermedio)	Fb (frecuente a continuo)	Pa (a veces posible)	Wb (1 vez en 100 años)	1

Tabla IV.6 Definición del SIL utilizando gráfico del riesgo

IV.4 Análisis con árbol de fallas

A través de la técnica de Análisis de Árbol de Fallas, (FTA, Fault Tree Analysis) se calculó el SIL como función de la Probabilidad de Falla en Demanda (PFD) o No-Disponibilidad para cada sistema en estudio.

Se identifica el evento No-Deseado (*Top Event*) con la finalidad de determinar el SIL, como la probabilidad de que el SPE falle ante una demanda. Esto se hace para cada uno de los "interlocks" o sistemas ante un evento no deseado, por ejemplo Sobrepresión o Fuga. También basándose en él se estiman los Paros en Falso para cada sistema.

Una vez que ha sido definido el "Top Event" (PFD y Disparos en Falso) se construyen los árboles de falla usando la lógica de falla apropiada mediante símbolos. La Figura IV.4 muestra algunos ejemplos de símbolos.

El nivel detallado del árbol de falla depende en gran medida de interacción que tengan los eventos básicos iniciantes para llegar al "Top Event".

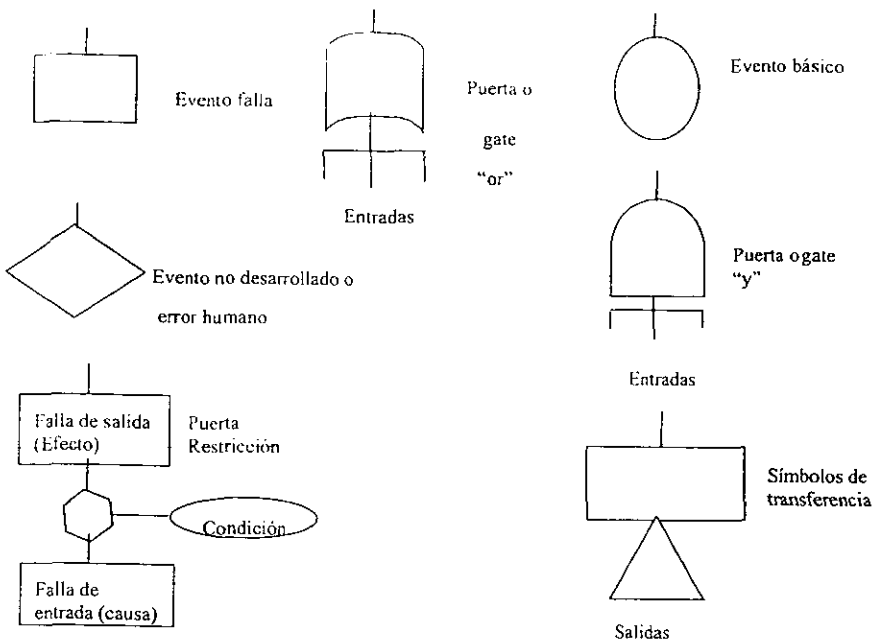


Figura IV.4 Ejemplos de símbolos utilizados en la construcción de Árboles de Falla

Para poder evaluar cuantitativamente los árboles de falla y consigo calcular cada una de las Probabilidades de Falla en Demanda y Disparos en Falso ante los eventos no deseados del SPE, se debe recurrir a datos de Tasa de Falla (λ) de cada componente o dispositivo, tales como: sensores, ejecutores lógicos, elementos finales, válvulas solenoides, etc., involucrados en el sistema a evaluar. La solución matemática se efectuó mediante simulación por computadora con el software de CARA Fault-Tree (Computer Aided Reliability Analysis) Ver. 4.02, 1996 licenciado al I.M.P por Det Norske Veritas.

En la Tabla IV.7 se presenta una lista detallada de datos de Tasa de Falla utilizados para el análisis de los sistemas evaluados, así como la fuente donde fue obtenida esta información.

Dispositivo	Falla en Demanda (Fallas / hora)	Disparos en Falso (Fallas / hora)	Fuente
Transmisor de Presión	0.70 E-06	0.42 E-06	OREDA-97
Switch de Presión	0.40 E-06	0.42 E-06	CCPS
Detector de fuego	1.32 E-06	6.10 E-06	OREDA-92
Resolvidor Lógico	0.5 E-06	0.5 E-06	FABRICANTE
Válvula Solenoide	1.00 E-06	0.41 E-06	D.J. SMITH
Válvula Superficial SSV	2.98 E-06	0.97 E-06	OREDA 92
Válvula Sub-Superficial SCSSV	5.01 E-06	1.43 E-06	OREDA 92
Válvula de Corte	4.39 E-06	0.25 E-06	OREDA 97
Alarma Audible	6.0 E-06	3.2 E-06	OREDA 92
Alarma Visible	4.0 E-06	3.2 E-06	OREDA 92
Detector de Gas	3.26 E-06	---	OREDA 92
Botón de Paro	0.5 E-06	---	OREDA 97

Tabla IV.7 Datos de Tasa de Falla para los dispositivos involucrados en el SPE

IV.5 Determinación del Nivel de Integridad de Seguridad

IV.5.1 Pozos de Producción No. 16 y 18:

Eventos: Sobrepresión
 Fuego Externo
 Fuga de Gas Tóxico y/o de Gas Combustible
 Baja presión/ruptura

Dispositivos de Detección

Transmisor de presión: con indicación de alarma visible en pantalla del tablero de control y alarma audiovisual, localizado en cada bajante de los pozos. Calibrado tanto por alta y baja presión.

Interruptor por alta y baja presión: con acción hacia el modulo Baker del pozo de donde se accionan las válvulas superficial (SSV) y subsuperficial (SCSSV). Localizados en cada bajante del pozo.

Detectores de Fuego del tipo combinado UV/IR, Detectores de gas tóxico, Detectores de gas combustible: con acción sobre alarmas tanto audible como visible y localizados en puntos estratégicos del área de pozos.

Resolvidor Lógico

La resolución de la lógica del sistema se realiza a través de un sistema diseñado para cumplir con certificación TUV/AK4 que proporciona un nivel de seguridad de SIL=2 como elemento independiente.

Elementos Finales

Se cuenta con dos válvulas: la válvula superficial (SSV), la válvula subsuperficial (SCSSV), alarmas audibles y visibles, así como el sistema Baker que actúa a través de un botón destinado para este efecto.

A continuación se muestran los árboles de falla para los eventos antes mencionados, así como las corridas efectuadas con el software CARA-Fault-Tree versión 4.02, en las que se muestran los grupos de corte (cut sets) utilizados, la importancia de cada uno de estos y la no-disponibilidad resultante para cada grupo de corte.

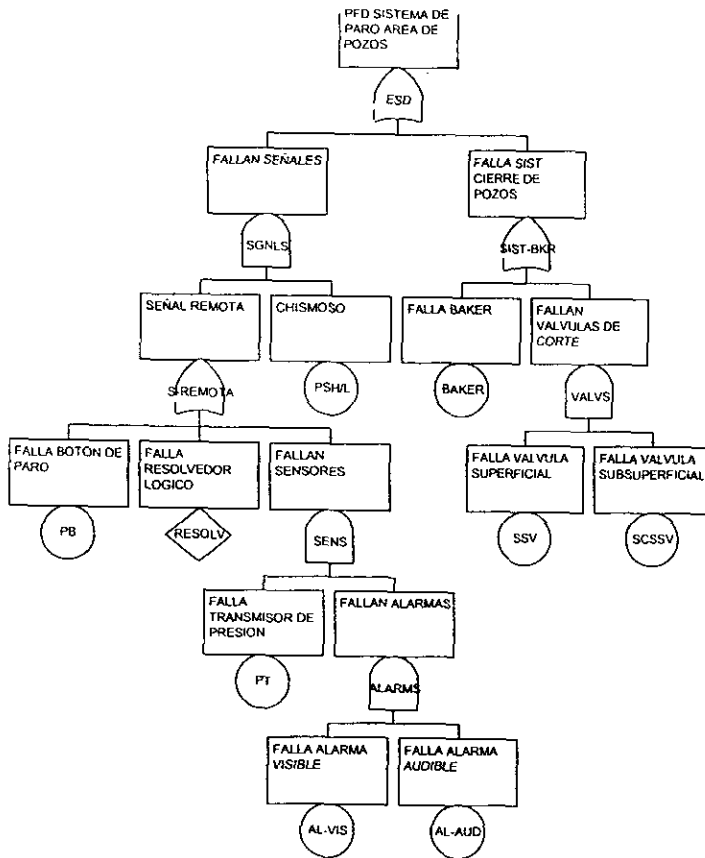


Figura IV.5 Arbol de fallas para sobrepresion en Pozos de Producción

CARA Fault Tree version 4.0 (c) SINTEF 1996
 Licenced to: Instituto Mexicano Del Petroleo,
 Mexico

Supported by: DNV Technica
 Date: 04/04/00 Time: 09:19:42

Cut set(s) with 1 component (Total: 1)
 {BAKER}
 Cutset importance = 9.44E-001
 Cutset unavailability = 4.89E-003

Cut set(s) with 2 components (Total: 3)
 {PSHL,PB}
 Cutset importance = 8.09E-004
 Cutset unavailability = 3.83E-006

{PSHL,RESOLV}
 Cutset importance = 8.09E-004
 Cutset unavailability = 3.83E-006

{SSV,SCSSV}
 Cutset importance = 5.44E-002
 Cutset unavailability = 2.81E-004

Cut set(s) with 3 components (None found)

Cut set(s) with 4 components (Total: 1)
 {PSHL,PT,AL-VIS,AL-AUD}
 Cutset importance = 4.66E-007
 Cutset unavailability = 2.41E-009

Total number of cut sets up to order 4: 5

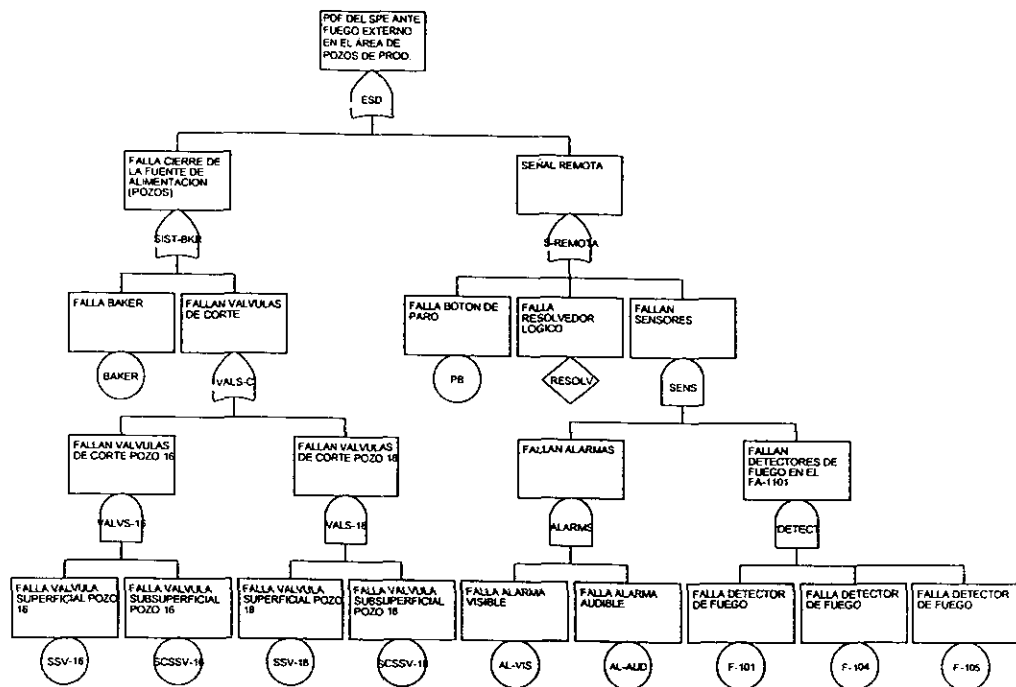


Figura IV.6 Arbol de fallas para Fuego externo en Pozos de Producción

CARA Fault Tree version 4.0 (c) SINTEF 1996
 Licenced to: Instituto Mexicano Del Petroleo,
 Mexico

Supported by: DNV Technica

Date: 04/04/00 Time: 04:48:07

Cut set(s) with 1 component (Total: 3)

{BAKER}

Cutset importance = 4.99E-001

Cutset unavailability = 4.89E-003

{PB}

Cutset importance = 2.22E-001

Cutset unavailability = 2.19E-003

{RESOLV}

Cutset importance = 2.22E-001

Cutset unavailability = 2.19E-003

Cut set(s) with 2 components (Total: 2)

{SSV-16,SCSSV-16}

Cutset importance = 2.85E-002

Cutset unavailability = 2.81E-004

{SSV-18,SCSSV-18}

Cutset importance = 2.85E-002

Cutset unavailability = 2.81E-004

Cut set(s) with 3 components (None found)

Cut set(s) with 4 components (None found)

Cut set(s) with 5 components (Total: 1)

{AL-VIS,AL-AUD,F-101,F-104,F-105}

Cutset importance = 8.81E-009

Cutset unavailability = 8.63E-011

Cut set(s) with 6 components (None found)

Cut set(s) with 7 components (None found)

Cut set(s) with 8 components (None found)

Cut set(s) with 9 components (None found)

Total number of cut sets up to order 9: 6

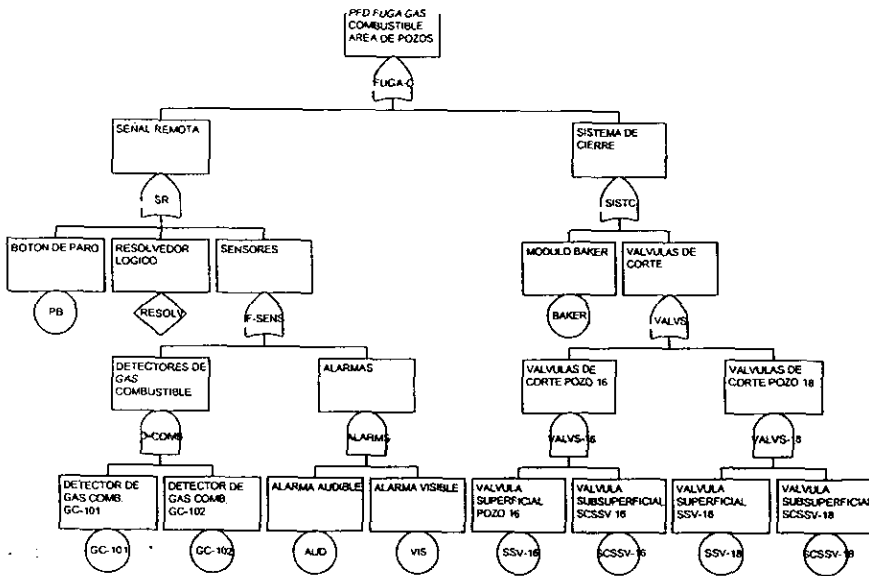


Figura IV.7 Arbol de fallas para Fuga de Gas Combustible en Pozos de Producción

CARA Fault Tree version 4.0 (c) SINTEF 1996
 Licenced to: Instituto Mexicano Del Petroleo, Mexico

Supported by: DNV Technica
 Date: 04/04/00 Time: 04:54:01

Cut set(s) with 1 component (Total: 3)
 {PB}

Cutset importance = 2.12E-001
 Cutset unavailability = 2.19E-003
 {RESOLV}

Cutset importance = 2.12E-001
 Cutset unavailability = 2.19E-003
 {BAKER}

Cutset importance = 4.75E-001
 Cutset unavailability = 4.89E-003

Cut set(s) with 2 components (Total: 4)
 {GC-101,GC-102}

Cutset importance = 3.23E-003
 Cutset unavailability = 3.32E-005

{AUD,VIS}

Cutset importance = 4.36E-002

Cutset unavailability = 4.50E-004

{SSV-16,SCSSV-16}

Cutset importance = 2.71E-002

Cutset unavailability = 2.81E-004

{SSV-18,SCSSV-18}

Cutset importance = 2.71E-002

Cutset unavailability = 2.81E-004

Cut set(s) with 3 components (None found)

Cut set(s) with 4 components (None found)

Cut set(s) with 5 components (None found)

Cut set(s) with 6 components (None found)

Cut set(s) with 7 components (None found)

Cut set(s) with 8 components (None found)

Cut set(s) with 9 components (None found)

Total number of cut sets up to order 9: 7

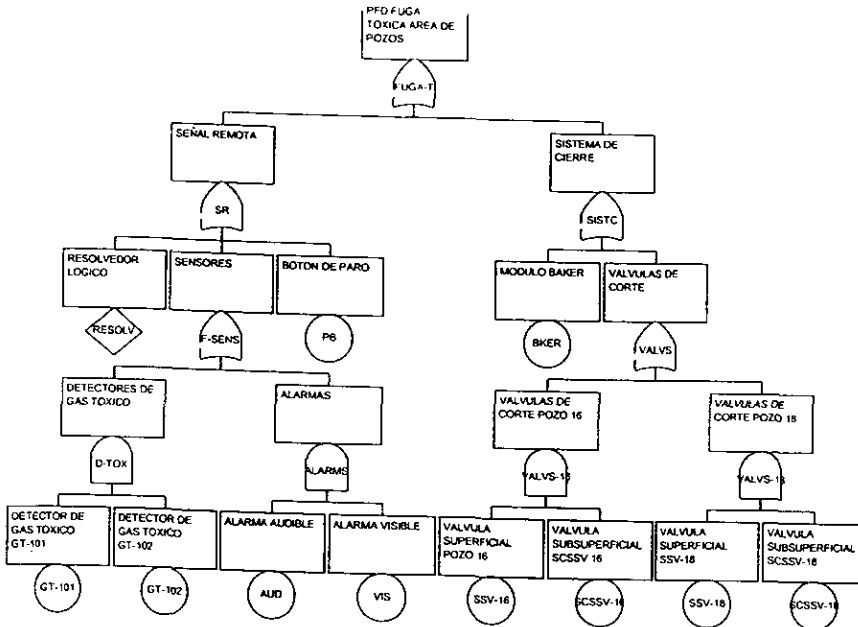


Figura IV.8 Arbol de fallas para Fuga de Gas Tóxico en Pozos de Producción

CARA Fault Tree version 4.0 (c) SINTEF 1996
 Licenced to: Instituto Mexicano Del Petroleo, Mexico

Supported by: DNV Technica
 Date: 04/04/00 Time: 04:57:43

Cut set(s) with 1 component (Total: 3)
 {RESOLV}

Cutset importance = 2.08E-001
 Cutset unavailability = 2.19E-003
 {PB}

Cutset importance = 2.08E-001
 Cutset unavailability = 2.19E-003
 {BKER}

Cutset importance = 4.68E-001
 Cutset unavailability = 4.89E-003
 Cut set(s) with 2 components (Total: 4)
 {GT-101,GT-102}

Cutset importance = 1.92E-002
 Cutset unavailability = 2.01E-004

{AUD,VIS}

Cutset importance = 4.32E-002

Cutset unavailability = 4.50E-004

{SSV-16,SCSSV-16}

Cutset importance = 2.68E-002

Cutset unavailability = 2.81E-004

{SSV-18,SCSSV-18}

Cutset importance = 2.68E-002

Cutset unavailability = 2.81E-004

Cut set(s) with 3 components (None found)

Cut set(s) with 4 components (None found)

Cut set(s) with 5 components (None found)

Cut set(s) with 6 components (None found)

Cut set(s) with 7 components (None found)

Cut set(s) with 8 components (None found)

Cut set(s) with 9 components (None found)

Total number of cut sets up to order 9: 7

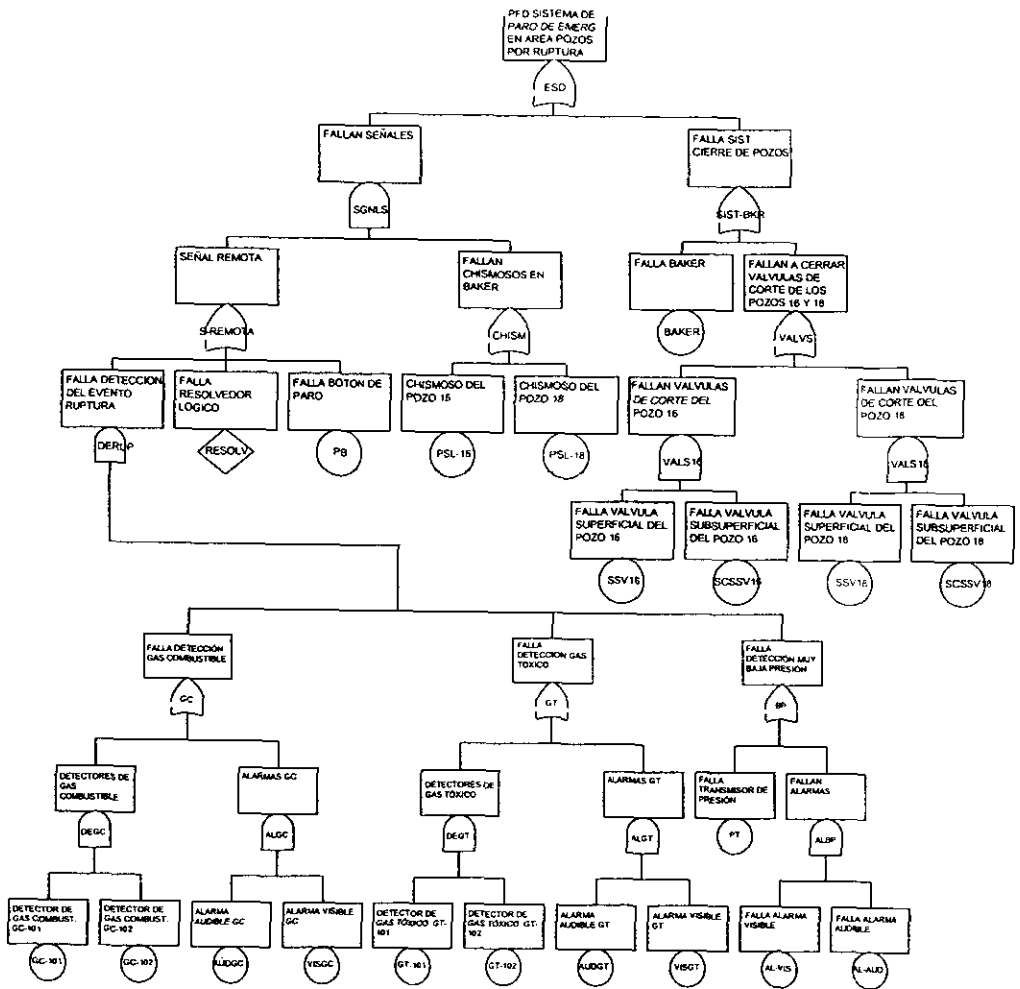


Figura IV.9 Arbol de fallas para Ruptura en Pozos de Producción

CARA Fault Tree version 4.0 (c) SINTEF 1996
 Licenced to: Instituto Mexicano Del Petroleo, Mexico
 Supported by: DNV Technica
 Date: 04/04/00 Time: 05:02:10

Cut sel(s) with 1 component (Total: 1)
 {BAKER}
 Cutset importance = 8.95E-001
 Cutset unavailability = 4.89E-003
 Cut sel(s) with 2 components (Total: 6)

{RESOLV,PSL-16}	{PSL-16,AUDGC,VISGC,AUDGT,VISGT,PT}
Cutset importance = 7.00E-004	Cutset importance = 1.99E-010
Cutset unavailability = 3.83E-006	Cutset unavailability = 1.09E-012
{RESOLV,PSL-18}	{PSL-18,AUDGC,VISGC,AUDGT,VISGT,PT}
Cutset importance = 7.00E-004	Cutset importance = 1.99E-010
Cutset unavailability = 3.83E-006	Cutset unavailability = 1.09E-012
{PB,PSL-16}	Cut set(s) with 7 components (Total: 8)
Cutset importance = 7.00E-004	{PSL-16,GC-101,GC-102,GT-101,GT-102,AL-
Cutset unavailability = 3.83E-006	VIS,AL-AUD}
{PB,PSL-18}	Cutset importance = 9.63E-013
Cutset importance = 7.00E-004	Cutset unavailability = 5.27E-015
Cutset unavailability = 3.83E-006	{PSL-18,GC-101,GC-102,GT-101,GT-102,AL-
{SSV16,SCSSV16}	VIS,AL-AUD}
Cutset importance = 5.11E-002	Cutset importance = 9.63E-013
Cutset unavailability = 2.81E-004	Cutset unavailability = 5.27E-015
{SSV18,SCSSV}	{PSL-16,GC-101,GC-102,AUDGT,VISGT,AL-
Cutset importance = 5.11E-002	VIS,AL-AUD}
Cutset unavailability = 2.81E-004	Cutset importance = 2.16E-012
Cut set(s) with 3 components (None found)	Cutset unavailability = 1.18E-014
Cut set(s) with 4 components (None found)	{PSL-18,GC-101,GC-102,AUDGT,VISGT,AL-
Cut set(s) with 5 components (None found)	VIS,AL-AUD}
Cut set(s) with 6 components (Total: 8)	Cutset importance = 2.16E-012
{PSL-16,GC-101,GC-102,GT-101,GT-102,PT}	Cutset unavailability = 1.18E-014
Cutset importance = 6.55E-012	{PSL-16,AUDGC,VISGC,GT-101,GT-102,AL-
Cutset unavailability = 3.58E-014	VIS,AL-AUD}
{PSL-18,GC-101,GC-102,GT-101,GT-102,PT}	Cutset importance = 1.31E-011
Cutset importance = 6.55E-012	Cutset unavailability = 7.14E-014
Cutset unavailability = 3.58E-014	{PSL-18,AUDGC,VISGC,GT-101,GT-102,AL-
{PSL-16,GC-101,GC-102,AUDGT,VISGT,PT}	VIS,AL-AUD}
Cutset importance = 1.47E-011	Cutset importance = 1.31E-011
Cutset unavailability = 8.02E-014	Cutset unavailability = 7.14E-014
{PSL-18,GC-101,GC-102,AUDGT,VISGT,PT}	{PSL-16,AUDGC,VISGC,AUDGT,VISGT,AL-
Cutset importance = 1.47E-011	VIS,AL-AUD}
Cutset unavailability = 8.02E-014	Cutset importance = 2.93E-011
{PSL-16,AUDGC,VISGC,GT-101,GT-102,PT}	Cutset unavailability = 1.60E-013
Cutset importance = 8.87E-011	{PSL-18,AUDGC,VISGC,AUDGT,VISGT,AL-
Cutset unavailability = 4.85E-013	VIS,AL-AUD}
{PSL-18,AUDGC,VISGC,GT-101,GT-102,PT}	Cutset importance = 2.93E-011
Cutset importance = 8.87E-011	Cutset unavailability = 1.60E-013
Cutset unavailability = 4.85E-013	Cut set(s) with 8 components (None found)
	Cut set(s) with 9 components (None found)

Total number of cut sets up to order 9: 23

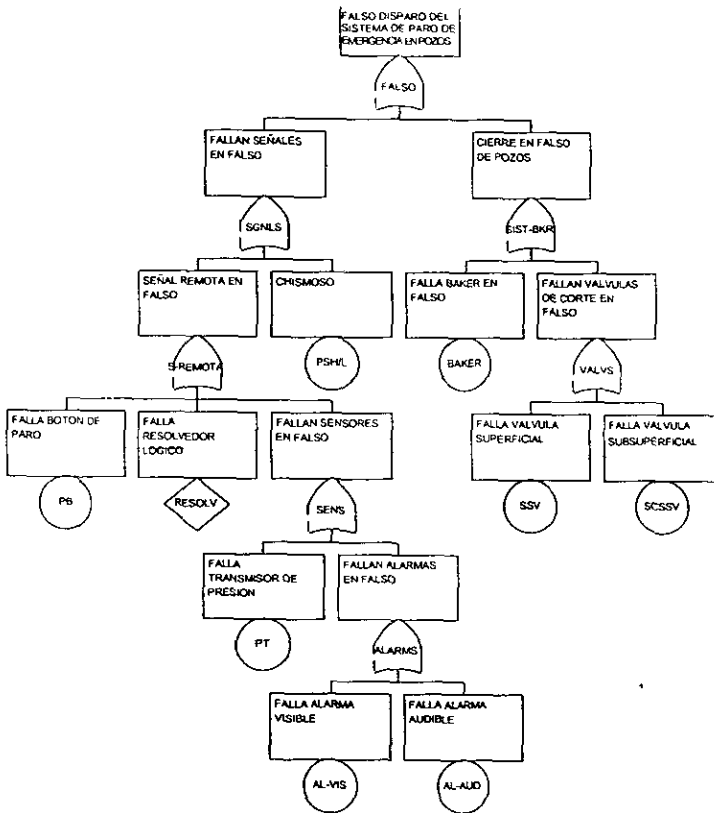


Figura IV.10 Arbol de fallas para Disparo en Falso en Pozos de Producción

CARA Fault Tree version 4.0 (c) SINTEF 1996

Licensed to: Instituto Mexicano Del Petroleo, Mexico

Supported by: DNV Technica

Date: 04/04/00 Time: 05:13:34

Cut set(s) with 1 component (Total: 9)

{AL-VIS}

Cutset importance = 2.77E-001

Cutset unavailability = 1.39E-002

{AL-AUD}

Cutset importance = 2.77E-001

Cutset unavailability = 1.39E-002

{PT}

Cutset importance = 3.73E-002

Cutset unavailability = 1.84E-003

{PB}

Cutset importance = 9.02E-003

Cutset unavailability = 4.38E-004

{RESOLV}

Cutset importance = 4.51E-002

Cutset unavailability = 2.19E-003

{PSHL}

Cutset importance = 3.73E-002

Cutset unavailability = 1.84E-003

{SSV}

Cutset importance = 8.73E-002

Cutset unavailability = 4.24E-003

{SCSSV}

Cutset importance = 1.29E-001

Cutset unavailability = 6.24E-003

{BAKER}

Cutset importance = 1.01E-001

Cutset unavailability = 4.89E-003

Cut set(s) with 2 components (None found)

Cut set(s) with 3 components (None found)

Cut set(s) with 4 components (None found)

Cut set(s) with 5 components (None found)

Cut set(s) with 6 components (None found)

Cut set(s) with 7 components (None found)

Cut set(s) with 8 components (None found)

Cut set(s) with 9 components (None found)

Total number of cut sets up to order 9: 9

Frequency of Top event (FALSO): 1.09148e-005
{Occ. per Hours}

IV.5.2 Separador de Prueba FA-1101:

Eventos: Sobrepresión
 Fuego Externo
 Fuga de Gas Tóxico y/o Gas Combustible

Dispositivos de Detección:

Transmisor de presión: con indicación local y en el tablero de control, localizado en el cuerpo del recipiente, detectores de gas tóxico, gas combustible y de fuego

Resolvidor Lógico

La resolución de la lógica del sistema se realiza a través de un resolvidor lógico que tiene como característica de confiabilidad la certificación TUV AK4, el cual proporciona un nivel de seguridad de 2 (SIL=2).

Elementos Finales

Como elemento final se tiene la indicación de presión en el cuarto de control, alarmas audibles, visibles y la acción sobre el sistema de seguridad de los pozos a través de un botón de paro de emergencia.

A continuación se muestran los árboles de falla para los eventos antes mencionados, así como las corridas efectuadas con el software CARA-Fault-Tree versión 4.02, en las que se muestran los grupos de corte (cut sets) utilizados, la importancia de cada uno de estos y la no-disponibilidad resultante para cada grupo de corte.

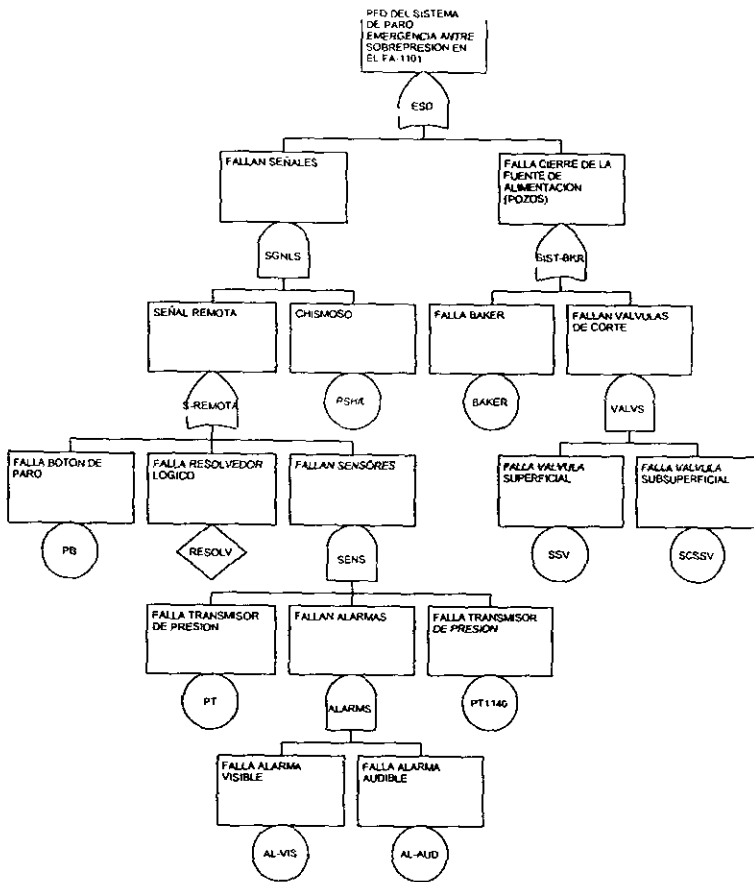


Figura IV.11 Arbol de fallas para sobrepresion en Separador de Prueba

CARA Fault Tree version 4.0 (c) SINTEF 1996
 Licenced to: Instituto Mexicano Del Petroleo, Mexico

Supported by: DNV Technica

Date: 04/04/00 Time: 05:45:15

Cut set(s) with 1 component (Total: 1)
 {BAKER}

Cutset importance = 9.44E-001

Cutset unavailability = 4.89E-003

Cut set(s) with 2 components (Total: 3)
 {PSHL,PB}

Cutset importance = 8.09E-004

Cutset unavailability = 3.83E-006

{PSHL,RESOLV}

Cutset importance = 8.09E-004

Cutset unavailability = 3.83E-006

{SSV,SCSSV}

Cutset importance = 5.44E-002

Cutset unavailability = 2.81E-004

Cut set(s) with 3 components (None found)

Cut set(s) with 4 components (None found)

Cut set(s) with 5 components (Total: 1)

{PSHL,PT,PT1140,AL-VIS,AL-AUD}

Cutset importance = 1.43E-009

Cutset unavailability = 7.39E-012

Cut set(s) with 6 components (None found)

Cut set(s) with 7 components (None found)

Cut set(s) with 8 components (None found)

Cut set(s) with 9 components (None found)

Total number of cut sets up to order 9: 5

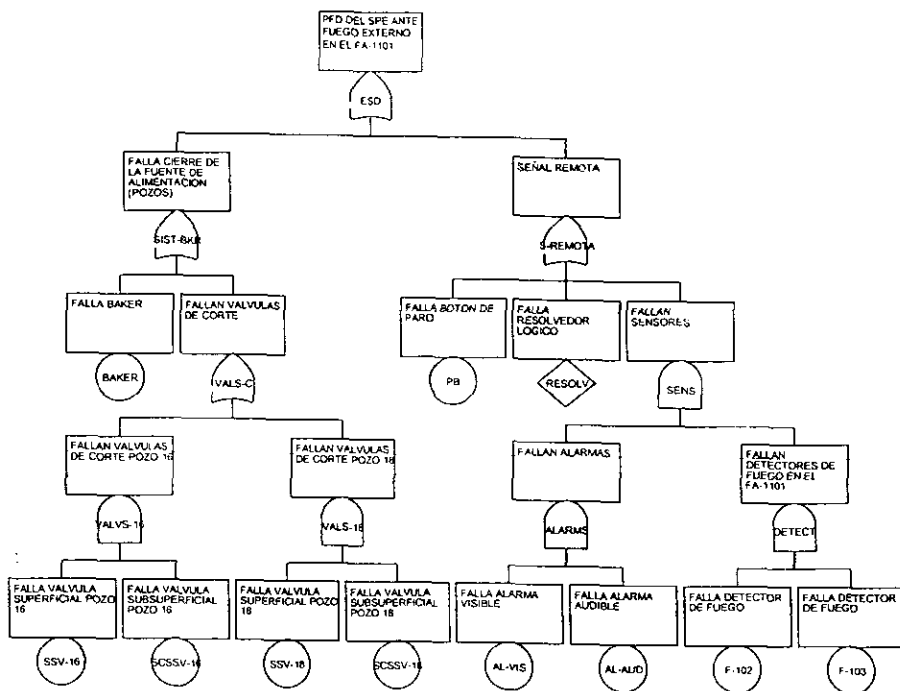


Figura IV.12 Arbol de fallas para Fuego externo en Separador de Prueba

CARA Fault Tree version 4.0 (c) SINTEF 1996

Licensed to: Instituto Mexicano Del Petroleo, Mexico

Supported by: DNV Technica

Date: 04/04/00 Time: 06:04:27

Cut set(s) with 1 component (Total: 3)

{BAKER}

Cutset importance = 4.99E-001

Cutset unavailability = 4.89E-003

{PB}

Cutset importance = 2.22E-001

Cutset unavailability = 2.19E-003

{RESOLV}

Cutset importance = 2.22E-001

Cutset unavailability = 2.19E-003

Cut set(s) with 2 components (Total: 2)

{SSV-16,SCSSV-16}

Cutset importance = 2.85E-002

Cutset unavailability = 2.81E-004

{SSV-18,SCSSV-18}

Cutset importance = 2.85E-002

Cutset unavailability = 2.81E-004

Cut set(s) with 3 components (None found)

Cut set(s) with 4 components (Total: 1)

{AL-VIS,AL-AUD,F-102,F-103}

Cutset importance = 1.53E-006

Cutset unavailability = 1.50E-008

Cut set(s) with 5 components (None found)

Cut set(s) with 6 components (None found)

Cut set(s) with 7 components (None found)

Cut set(s) with 8 components (None found)

Cut set(s) with 9 components (None found)

Total number of cut sets up to order 9: 6

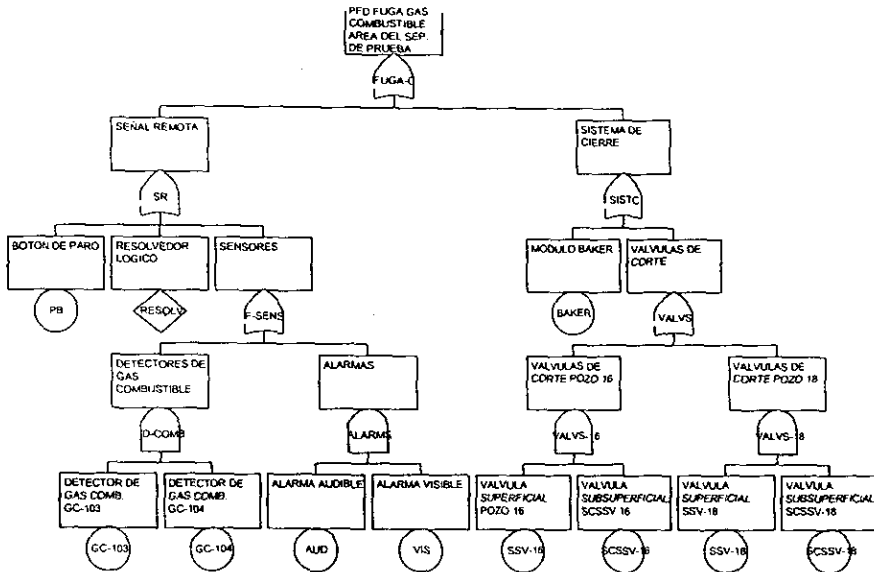


Figura IV.13 Arbol de fallas para Fuga de gas combustible en Separador de Prueba

CARA Fault Tree version 4.0 (c) SINTEF 1996
 Licenced to: Instituto Mexicano Del Petroleo, Mexico
 Supported by: DNV Technica
 Date: 04/04/00 Time: 06:07:13

Cut set(s) with 1 component (Total: 3)
 {PB}
 Cutset importance = 2.12E-001
 Cutset unavailability = 2.19E-003

{RESOLV}
 Cutset importance = 2.12E-001
 Cutset unavailability = 2.19E-003

{BAKER}
 Cutset importance = 4.75E-001
 Cutset unavailability = 4.89E-003

Cut set(s) with 2 components (Total: 4)
 {GC-103,GC-104}
 Cutset importance = 3.23E-003
 Cutset unavailability = 3.32E-005

{AUD,VIS}
 Cutset importance = 4.36E-002
 Cutset unavailability = 4.50E-004

{SSV-16,SCSSV-16}
 Cutset importance = 2.71E-002
 Cutset unavailability = 2.81E-004

{SSV-18,SCSSV-18}
 Cutset importance = 2.71E-002
 Cutset unavailability = 2.81E-004

Cut set(s) with 3 components (None found)
 Cut set(s) with 4 components (None found)
 Cut set(s) with 5 components (None found)
 Cut set(s) with 6 components (None found)
 Cut set(s) with 7 components (None found)
 Cut set(s) with 8 components (None found)
 Cut set(s) with 9 components (None found)

Total number of cut sets up to order 9: 7

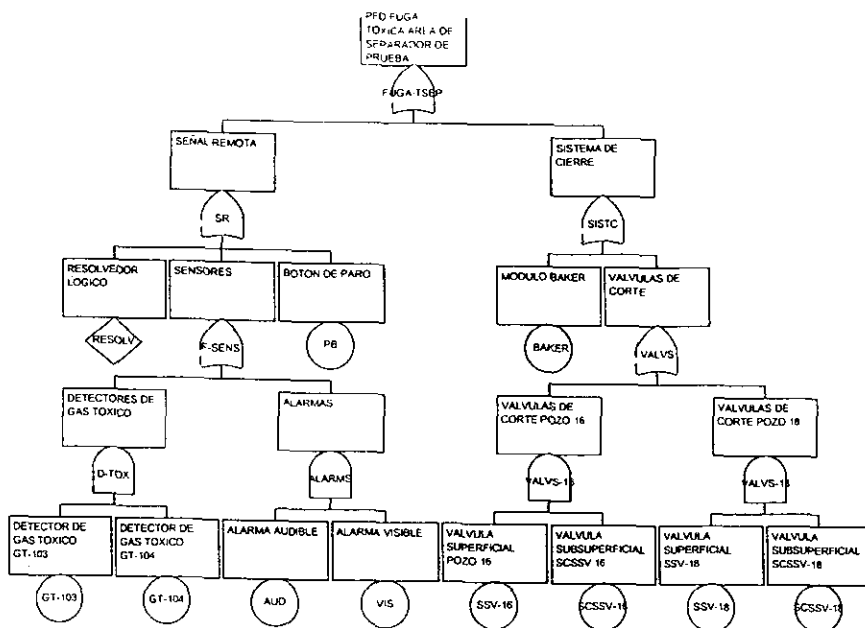


Figura IV.14 Arbol de fallas para Fuga de gas tóxico en Separador de Prueba

CARA Fault Tree version 4.0 (c) SINTEF 1996
 Licenced to: Instituto Mexicano Del Petroleo, Mexico

Supported by: DNV Technica
 Date: 04/04/00 Time: 06:11:00

Cut set(s) with 1 component (Total: 3)
 {RESOLV}

Cutset importance = 2.08E-001
 Cutset unavailability = 2.19E-003

{PB}

Cutset importance = 2.08E-001
 Cutset unavailability = 2.19E-003

{BAKER}

Cutset importance = 4.68E-001
 Cutset unavailability = 4.89E-003

Cut set(s) with 2 components (Total: 4)
 {GT-103,GT-104}

Cutset importance = 1.92E-002
 Cutset unavailability = 2.01E-004

{AUD,VIS}

Cutset importance = 4.32E-002
 Cutset unavailability = 4.50E-004

{SSV-16,SCSSV-16}

Cutset importance = 2.68E-002
 Cutset unavailability = 2.81E-004

{SSV-18,SCSSV-18}

Cutset importance = 2.68E-002
 Cutset unavailability = 2.81E-004

Cut set(s) with 3 components (None found)
 Cut set(s) with 4 components (None found)
 Cut set(s) with 5 components (None found)
 Cut set(s) with 6 components (None found)
 Cut set(s) with 7 components (None found)
 Cut set(s) with 8 components (None found)
 Cut set(s) with 9 components (None found)

Total number of cut sets up to order 9: 7

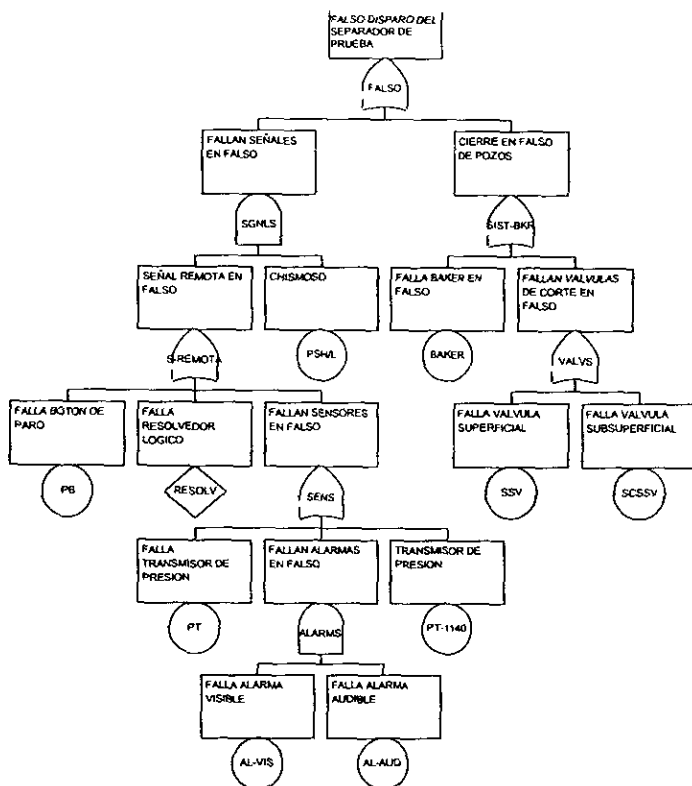


Figura IV.15 Arbol de fallas para Disparo en Falso en Separador de Prueba

CARA Fault Tree version 4.0 (c) SINTEF 1996

Licensed to: Instituto Mexicano Del Petroleo, Mexico

Supported by: DNV Technica

Date: 04/04/00 Time: 05:13:34

Cut set(s) with 1 component (Total: 9)

{AL-VIS}

Cutset importance = 2.77E-001

Cutset unavailability = 1.39E-002

{AL-AUD}

Cutset importance = 2.77E-001

Cutset unavailability = 1.39E-002

{PT}

Cutset importance = 3.73E-002

Cutset unavailability = 1.84E-003

{PB}

Cutset importance = 9.02E-003

Cutset unavailability = 4.38E-004

{RESOLV}

Cutset importance = 4.51E-002

Cutset unavailability = 2.19E-003

{PSH/L}

Cutset importance = 3.73E-002

Cutset unavailability = 1.84E-003

{SSV}

Cutset importance = 8.73E-002

Cutset unavailability = 4.24E-003

{SCSSV}

Cutset importance = 1.29E-001

Cutset unavailability = 6.24E-003

{BAKER}

Cutset importance = 1.01E-001

Cutset unavailability = 4.89E-003

Cut set(s) with 2 components (None found)

Cut set(s) with 3 components (None found)

Cut set(s) with 4 components (None found)

Cut set(s) with 5 components (None found)

Cut set(s) with 6 components (None found)

Cut set(s) with 7 components (None found)

Cut set(s) with 8 components (None found)

Cut set(s) with 9 components (None found)

Total number of cut sets up to order 9: 9

Frequency of Top event (FALSO): 1.09148E-005

{Occ. per Hours}

IV.5.3 Línea de Salida 8" P-1108:

Eventos: Sobrepresión
 Baja presión/ruptura
 Fuga de Gas Combustible y/o Tóxico

Dispositivos de Detección:

Transmisores Indicadores de presión: con indicación local y en tablero de control, calibrados por alta y baja presión con acción a alarmas visible en pantalla del tablero de control y alarma audiovisual, así como también con señal para registro de la presión. Localizados en la línea de salida de producción 8" P 1108. Se tienen instalados un detector de gas combustible y un detector de gas tóxico.

Resolvidor Lógico

La resolución de la lógica del sistema se realiza a través de un sistema modular triple redundante localizado en la plataforma de telecomunicaciones.

Elementos Finales

Como elemento final se cuenta con la válvula de corte SDV-1170, así como alarmas activadas por los detectores de gas tóxico y/o gas combustible.

A continuación se muestran los árboles de falla para los eventos antes mencionados, así como las corridas efectuadas con el software CARA-Fault-Tree versión 4.02, en las que se muestran los grupos de corte (cut sets) utilizados, la importancia de cada uno de estos y la no-disponibilidad resultante para cada grupo de corte.

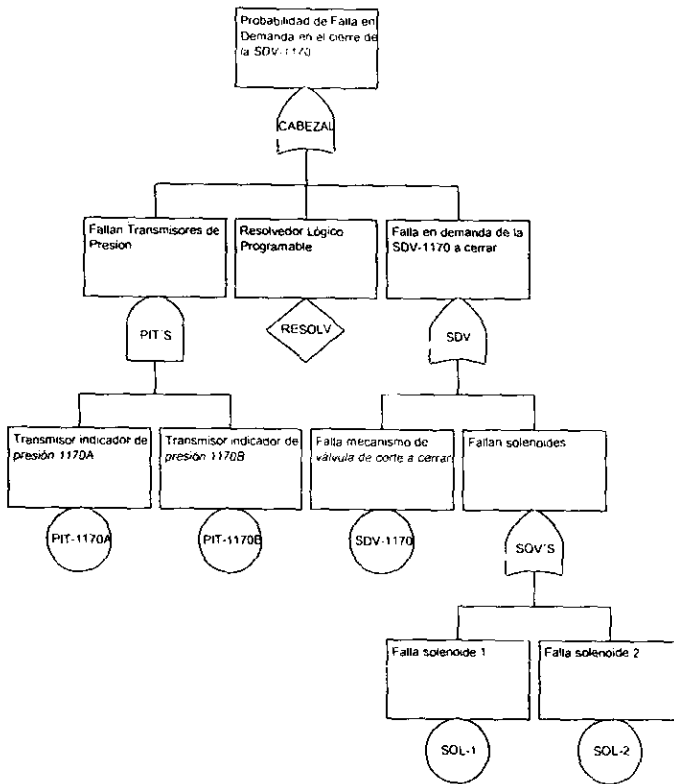


Figura IV.16 Arbol de fallas para sobrepresion en línea de salida

CARA Fault Tree version 4.0 (c) SINTEF 1996
 Licenced to: Instituto Mexicano Del Petroleo, Mexico

Supported by: DNV Technica

Date: 04/04/00 Time: 07:04:39

Cut set(s) with 1 component (Total: 4)

{SOL-1}

Cutset importance = 1.47E-001

Cutset unavailability = 4.37E-003

{SOL-2}

Cutset importance = 1.47E-001

Cutset unavailability = 4.37E-003

{SDV-1170}

Cutset importance = 6.32E-001

Cutset unavailability = 1.90E-002

{RESOLV}

Cutset importance = 7.37E-002

Cutset unavailability = 2.19E-003

Cut set(s) with 2 components (Total: 1)

{PIT-1170A,PIT-1170B}

Cutset importance = 3.15E-004

Cutset unavailability = 9.37E-006

Cut set(s) with 3 components (None found)

Cut set(s) with 4 components (None found)

Cut set(s) with 5 components (None found)

Cut set(s) with 6 components (None found)

Cut set(s) with 7 components (None found)

Cut set(s) with 8 components (None found)

Cut set(s) with 9 components (None found)

Total number of cut sets up to order 9: 5

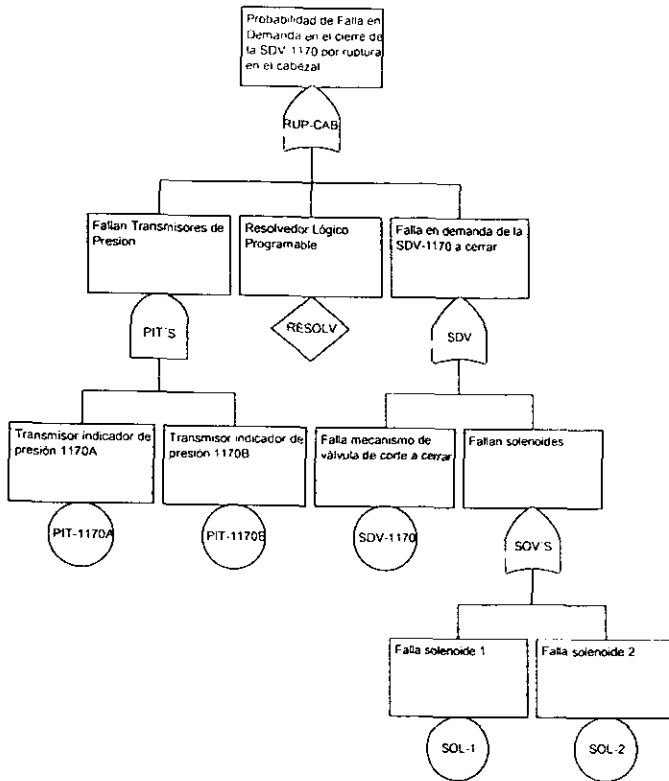


Figura IV.17 Arbol de fallas para ruptura en línea de salida

CARA Fault Tree version 4.0 (c) SINTEF 1996
 Licenced to: Instituto Mexicano Del Petroleo, Mexico
 Supported by: DNV Technica
 Date: 04/04/00 Time: 07:04:39

Cut set(s) with 1 component (Total: 4)
 {SOL-1}

Cutset importance = 1.47E-001
 Cutset unavailability = 4.37E-003

{SOL-2}

Cutset importance = 1.47E-001
 Cutset unavailability = 4.37E-003

{SDV-1170}

Cutset importance = 6.32E-001
 Cutset unavailability = 1.90E-002

{RESOLV}

Cutset importance = 7.37E-002
 Cutset unavailability = 2.19E-003

Cut set(s) with 2 components (Total: 1)
 {PIT-1170A,PIT-1170B}

Cutset importance = 3.15E-004
 Cutset unavailability = 9.37E-006

Cut set(s) with 3 components (None found)
 Cut set(s) with 4 components (None found)
 Cut set(s) with 5 components (None found)
 Cut set(s) with 6 components (None found)
 Cut set(s) with 7 components (None found)
 Cut set(s) with 8 components (None found)
 Cut set(s) with 9 components (None found)

Total number of cut sets up to order 9: 5

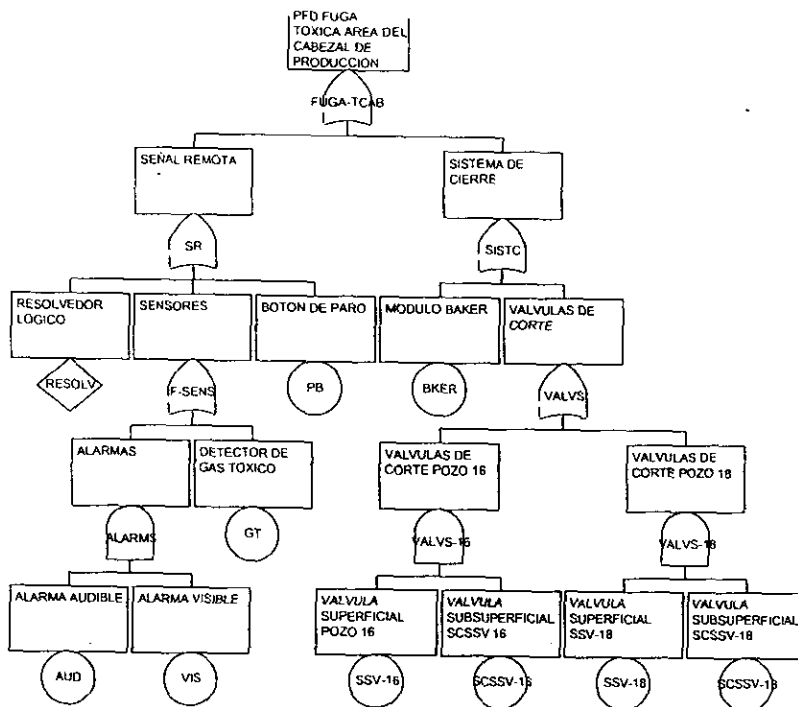


Figura IV.18 Arbol de fallas para Fuga de gas tóxico en línea de salida.

CARA Fault Tree version 4.0 (c) SINTEF 1996
 Licenced to: Instituto Mexicano Del Petroleo,
 Mexico

Supported by: DNV Technica
 Date: 04/04/00 Time: 07:21:45

Cut set(s) with 1 component (Total: 4)
 {GT}

Cutset importance = 5.76E-001
 Cutset unavailability = 1.42E-002

{RESOLV}
 Cutset importance = 9.01E-002
 Cutset unavailability = 2.19E-003

{PB}
 Cutset importance = 9.01E-002
 Cutset unavailability = 2.19E-003

{BKER}
 Cutset importance = 2.02E-001
 Cutset unavailability = 4.89E-003
 Cut set(s) with 2 components (Total: 3)

{AUD,VIS}
 Cutset importance = 1.86E-002
 Cutset unavailability = 4.50E-004

{SSV-16,SCSSV-16}
 Cutset importance = 1.16E-002
 Cutset unavailability = 2.81E-004

{SSV-18,SCSSV-18}
 Cutset importance = 1.16E-002
 Cutset unavailability = 2.81E-004

Cut set(s) with 3 components (None found)
 Cut set(s) with 4 components (None found)
 Cut set(s) with 5 components (None found)
 Cut set(s) with 6 components (None found)
 Cut set(s) with 7 components (None found)
 Cut set(s) with 8 components (None found)
 Cut set(s) with 9 components (None found)

Total number of cut sets up to order 9: 7

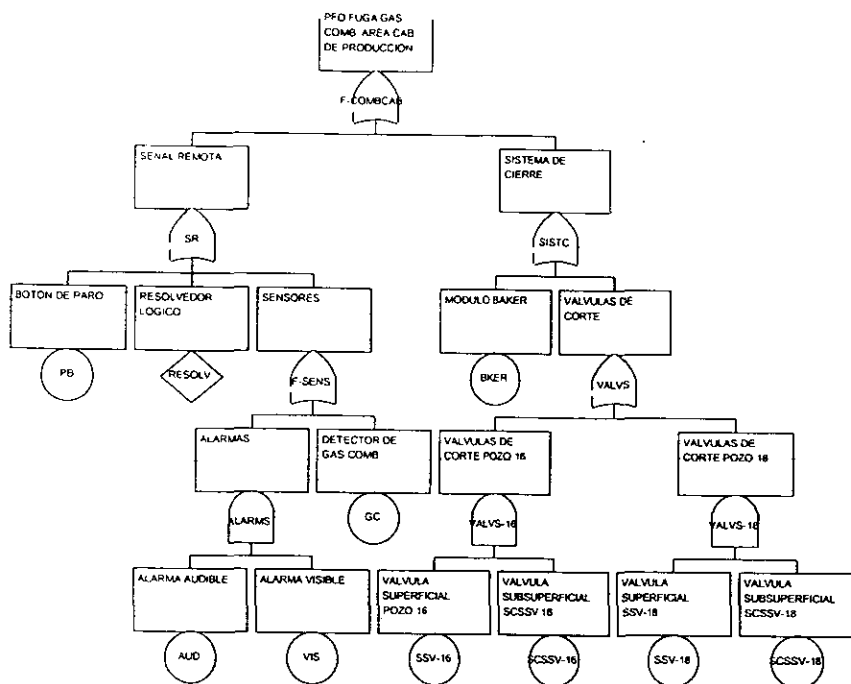


Figura IV.19 Arbol de fallas para Fuga de gas combustible en línea de salida

CARA Fault Tree version 4.0 (c) SINTEF 1996
 Licenced to: Instituto Mexicano Del Petroleo, Mexico
 Supported by: DNV Technica
 Date: 04/04/00 Time: 07:31:50

Cut set(s) with 1 component (Total: 4)
 {GC}

Cutset importance = 3.60E-001
 Cutset unavailability = 5.76E-003

{PB}
 Cutset importance = 1.36E-001
 Cutset unavailability = 2.19E-003

{RESOLV}
 Cutset importance = 1.36E-001
 Cutset unavailability = 2.19E-003

{BKER}
 Cutset importance = 3.06E-001
 Cutset unavailability = 4.89E-003

Cut set(s) with 2 components (Total: 3)
 {AUD,VIS}

Cutset importance = 2.72E-002
 Cutset unavailability = 4.50E-004

{SSV-16,SCSSV-16}
 Cutset importance = 1.74E-002
 Cutset unavailability = 2.81E-004

{SSV-18,SCSSV-18}
 Cutset importance = 1.74E-002
 Cutset unavailability = 2.81E-004

Cut set(s) with 3 components (None found)
 Cut set(s) with 4 components (None found)
 Cut set(s) with 5 components (None found)
 Cut set(s) with 6 components (None found)
 Cut set(s) with 7 components (None found)
 Cut set(s) with 8 components (None found)
 Cut set(s) with 9 components (None found)

Total number of cut sets up to order 9: 7

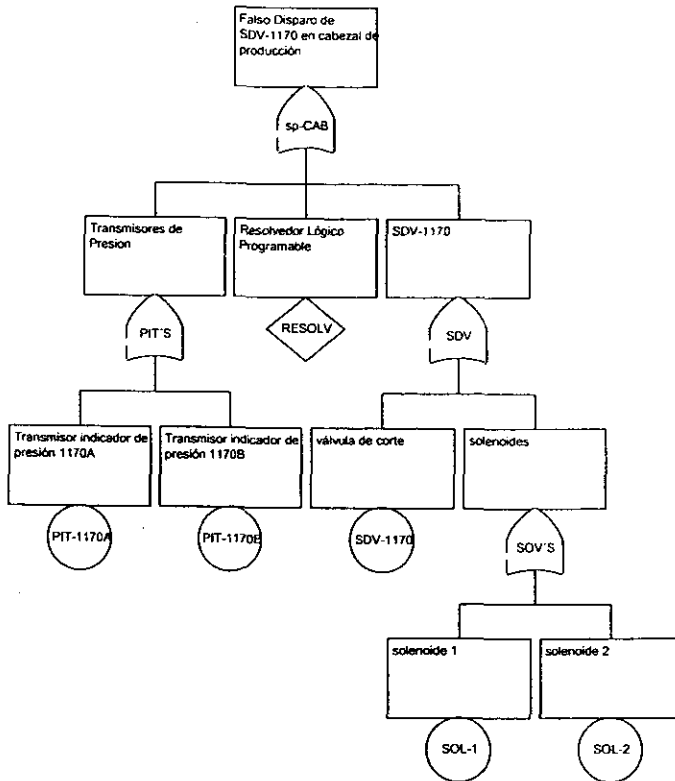


Figura IV.20 Arbol de fallas para Disparo en Falso en Línea de salida

CARA Fault Tree version 4.0 (c) SINTEF 1996
 Licenced to: Instituto Mexicano Del Petroleo, Mexico

Supported by: DNV Technica

Date: 04/04/00 Time: 07:51:08

Cut set(s) with 1 component (Total: 6)

{PIT-1170A}

Cutset importance = 1.74E-001

Cutset unavailability = 1.84E-003

{PIT-1170B}

Cutset importance = 1.74E-001

Cutset unavailability = 1.84E-003

{SOL-1}

Cutset importance = 1.71E-001

Cutset unavailability = 1.79E-003

{SOL-2}

Cutset importance = 1.71E-001

Cutset unavailability = 1.79E-003

{SDV-1170}

Cutset importance = 1.03E-001

Cutset unavailability = 1.09E-003

{RESOLV}

Cutset importance = 2.07E-001

Cutset unavailability = 2.19E-003

Cut set(s) with 2 components (None found)

Cut set(s) with 3 components (None found)

Cut set(s) with 4 components (None found)

Cut set(s) with 5 components (None found)

Cut set(s) with 6 components (None found)

Cut set(s) with 7 components (None found)

Cut set(s) with 8 components (None found)

Cut set(s) with 9 components (None found)

Total number of cut sets up to order 9: 6

Calculation of Freq(Top event: sp-CAB)

Frequency of Top event (sp-CAB): 2.38904e-006

[Occ. per Hours]

IV.5.4 Sistema global de producción

Eventos: Sobrepresión y ruptura
 Disparo en falso

Dispositivos de Detección:

Los contemplados en pozos de producción, separador de prueba y línea de salida.

Resolvedor Lógico

Los contemplados en pozos de producción, separador de prueba y línea de salida.

Elementos Finales

Los contemplados en pozos de producción, separador de prueba y línea de salida.

A continuación se muestran los árboles de falla para los eventos antes mencionados, así como las corridas efectuadas con el software CARA-Fault-Tree versión 4.02, en las que se muestran los grupos de corte (cut sets) utilizados, la importancia de cada uno de estos y la no-disponibilidad resultante para cada grupo de corte.

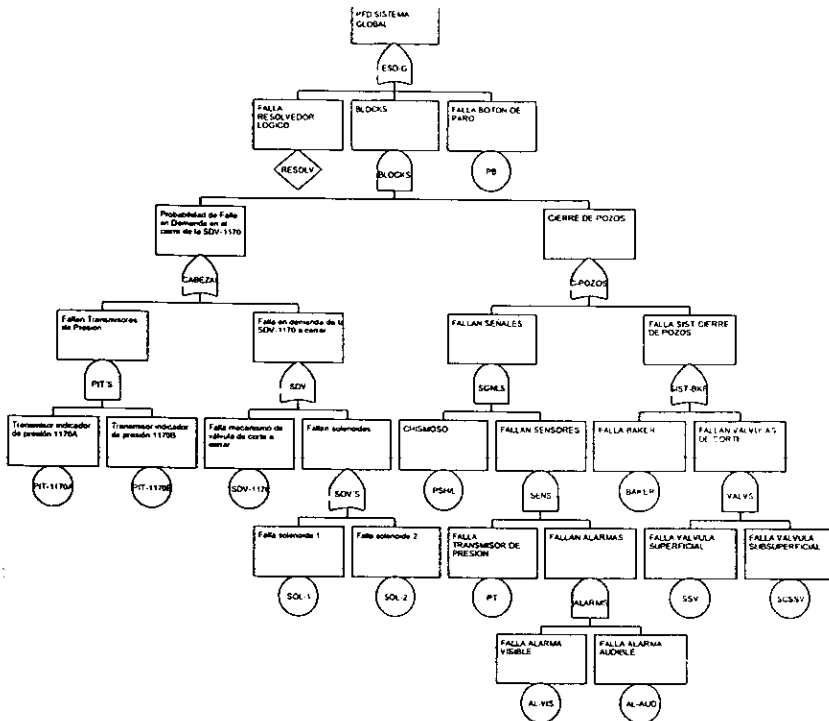


Figura IV.21 Arbol de Fallas para sobrepresión y ruptura del Sistema Global

CARA Fault Tree version 4.0 (c) SINTEF 1996

Licensed to: Instituto Mexicano Del Petroleo, Mexico

Supported by: DNV Technica

Date: 05/04/00 Time: 07:14:16

Cut set(s) with 1 component (Total: 2)
{RESOLV}

Cutset importance = 4.84E-001

Cutset unavailability = 2.19E-003

{PB}

Cutset importance = 4.84E-001

Cutset unavailability = 2.19E-003

Cut set(s) with 2 components (Total: 3)

{SOL-1,BAKER}

Cutset importance = 4.74E-003

Cutset unavailability = 2.14E-005

{SOL-2,BAKER}

Cutset importance = 4.74E-003

Cutset unavailability = 2.14E-005

{SDV-1170,BAKER}

Cutset importance = 2.08E-002

Cutset unavailability = 9.32E-005

Cut set(s) with 3 components (Total: 4)

{PIT-1170A,PIT-1170B,BAKER}

Cutset importance = 1.02E-005

Cutset unavailability = 4.59E-008

{SOL-1,SSV,SCSSV}

Cutset importance = 2.73E-004

Cutset unavailability = 1.23E-006

{SOL-2,SSV,SCSSV}

Cutset importance = 2.73E-004

Cutset unavailability = 1.23E-006

{SDV-1170,SSV,SCSSV}

Cutset importance = 1.19E-003

Cutset unavailability = 5.36E-006

Cut set(s) with 4 components (Total: 1)

{PIT-1170A,PIT-1170B,SSV,SCSSV}

Cutset importance = 5.84E-007

Cutset unavailability = 2.64E-009

Cut set(s) with 5 components (Total: 3)

{SOL-1,PSHL,PT,AL-VIS,AL-AUD}

Cutset importance = 2.34E-009

Cutset unavailability = 1.05E-011

{SOL-2,PSHL,PT,AL-VIS,AL-AUD}

Cutset importance = 2.34E-009

Cutset unavailability = 1.05E-011

{SDV-1170,PSHL,PT,AL-VIS,AL-AUD}

Cutset importance = 1.02E-008

Cutset unavailability = 4.60E-011

Cut set(s) with 6 components (Total: 1)

{PIT-1170A,PIT-1170B,PSHL,PT,AL-VIS,AL-AUD}

Cutset importance = 5.01E-012

Cutset unavailability = 2.26E-014

Total number of cut sets up to order 9: 14

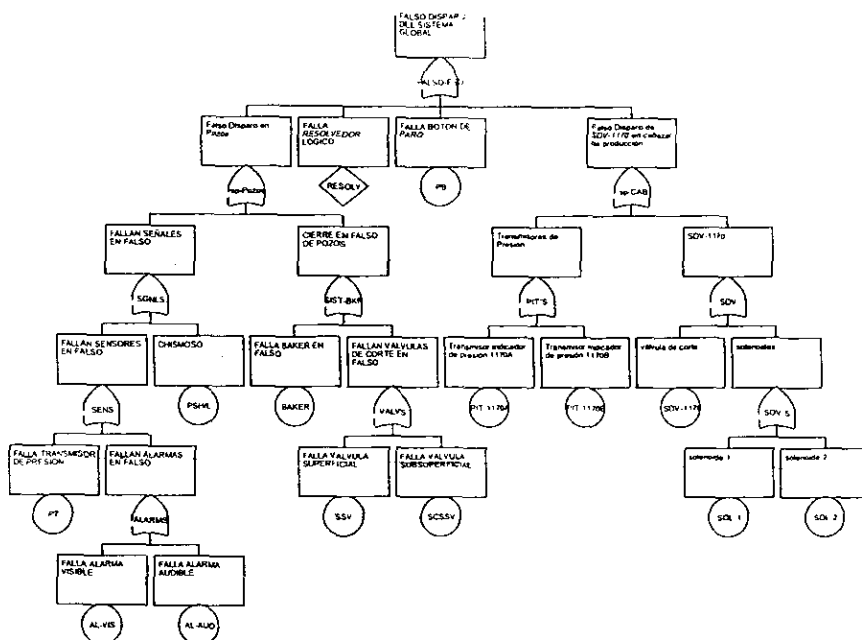


Figura IV.22 .Arbol de fallas para Disparo en Falso del sistema global.

CARA Fault Tree version 4.0 (c) SINTEF 1996
 Licenced to: Instituto Mexicano Del Petroleo, Mexico

Supported by: DNV Technica
 Date: 05/04/00 Time: 01:54:31
 Cut set(s) with 1 component (Total: 14)

- {AL-VIS}
- Cutset importance = 2.46E-001
- Cutset unavailability = 1.39E-002
- {AL-AUD}
- Cutset importance = 2.46E-001
- Cutset unavailability = 1.39E-002
- {PT}
- Cutset importance = 3.25E-002
- Cutset unavailability = 1.84E-003
- {PSHL}
- Cutset importance = 3.25E-002
- Cutset unavailability = 1.84E-003
- {SSV}
- Cutset importance = 7.51E-002
- Cutset unavailability = 4.24E-003
- {SCSSV}
- Cutset importance = 1.11E-001
- Cutset unavailability = 6.24E-003
- {BAKER}
- Cutset importance = 8.67E-002
- Cutset unavailability = 4.89E-003

- {PIT-1170A}
- Cutset importance = 3.25E-002
- Cutset unavailability = 1.84E-003
- {PIT-1170B}
- Cutset importance = 3.25E-002
- Cutset unavailability = 1.84E-003
- {SOL-1}
- Cutset importance = 3.18E-002
- Cutset unavailability = 1.79E-003
- {SOL-2}
- Cutset importance = 3.18E-002
- Cutset unavailability = 1.79E-003
- {SDV-1170}
- Cutset importance = 1.94E-002
- Cutset unavailability = 1.09E-003
- {RESOLV}
- Cutset importance = 3.87E-002
- Cutset unavailability = 2.19E-003
- {PB}
- Cutset importance = 7.76E-003
- Cutset unavailability = 4.38E-004
- Total number of cut sets up to order 9: 14

Calculation of Freq(Top event: FALSO-ESD)
 Frequency of Top event (FALSO-ESD) 1.26291e-005 [Occ. per Hours]

V. ANÁLISIS DE RESULTADOS

V.1 Pozos de producción No. 16 y 18

En las Tablas V.1, V.2, V.3, V.4 y V.5 se muestra la combinación de los Grupos de Cortes Mínimos o Minimal Cut Set de acuerdo a su importancia y contribución a la no-disponibilidad para el sistema de paro de emergencia en los pozos de producción Ixtoc-A, ante los siguientes eventos: **Sobrepresión, Fuego externo, Fuga de gas combustible, Fuga de gas tóxico y Ruptura**, respectivamente.

Sobrepresión. La Probabilidad de Falla en Demanda (PFD) del Sistema de Paro de Emergencia (SPE) ante el evento de Sobrepresión es de $5.18E-03$ equivalente a una Disponibilidad del **99.48%** lo cual implica que se encuentra entre el rango de 99.0% a 99.9% correspondiente a un Nivel de Integridad de la Seguridad **SIL=2**, con un Factor de Reducción del Riesgo de **193.1 años**. Lo anterior se establece con un periodo máximo de prueba propuesto de 6 meses para los componentes involucrados. Por otra parte, la acción del SPE ante dicho el evento, es tener la capacidad de cerrar de manera parcial o total los pozos 16 y 18, ya sea en forma local desde la consola baker gracias a la señal del piloto de alta presión "chismoso" o en forma remota por la acción del operador desde un botón de paro de emergencia que desencadene el cierre de las válvulas superficial SSV y subsuperficial SCSSV de los pozos.

Fuego Externo. La PFD del SPE ante el evento de Fuego externo es de $9.83E-03$ equivalente a una Disponibilidad del **99.02%**, correspondiente también a **SIL=2**, Factor de Reducción del Riesgo de **101.7 años**, con un periodo máximo de prueba propuesto de 6 meses para los componentes. Es importante mencionar que la acción del sistema es el cierre total de los dos pozos una vez detectada la condición de fuego, en forma local por la red de tapones fusibles existente o remota gracias a los tres detectores UV/IR instalados en el área F-101, F-104 y F-105, los cuales mandarán señal de alarma audible y visible a cuarto de control para que el operador desde el botón de paro de emergencia desencadene el cierre de dichos pozos.

Fuga de gas combustible y/o Tóxico. La Disponibilidad resultante ante este evento es **98.97%** para la fuga de gas combustible y **98.95%** para la fuga de gas tóxico, ambas corresponden a que el SPE tenga para este evento **SIL=1**, Factor de Reducción de Riesgo de **96.9 años y 95.4**

años, respectivamente y con un periodo máximo de prueba propuesto de 6 meses para los componentes. Es importante mencionar aquí, que si se reduce el periodo de prueba o mantenimiento por lo menos a 3 meses se tendría una PFD de $4.937E-03$ para poder lograr un SIL=2. Por otra parte, la acción del SPE se efectúa cuando los detectores de gas combustible GC-101, GC-102 y los detectores de gas tóxico GT-101, GT-102 mandan en forma independiente alarmar visible y audible para que el operador desde el botón de paro de emergencia desencadene el cierre de dichos pozos, cuando la concentración alcanza niveles como máximos del 60% del límite inferior de explosividad LEL para gas combustible y valores superiores a 40 p.p.m de H₂S para el gas tóxico.

Ruptura. La PFD resultante del SPE es de $5.47E-03$ equivalente a **99.45%** para SIL=2 y Factor de Reducción de Riesgo de **182.9 años**. Logrado con un periodo de prueba de 6 meses. Aquí la acción de cierre de los pozos se efectúa cuando se detecta baja presión por medio de los pilotos de baja presión "chismosos" instalados en ambas bajantes o cuando el operador active el SPE desde el botón de paro de emergencia con cualquier alarma de gas tóxico y/o combustible activada por las altas concentraciones detectadas de gas tóxico y combustible.

Disparo en Falso. En la Tabla V.6 se muestra la importancia del minimal cut set o componentes básicos de este sistema a contribuir al cierre en falso de cada pozo de manera independiente o parcial (Tiempo Medio de Paro en Falso) **MTTF^{spurious}** equivalente a **10.46 años**.

Por otra parte, es importante mencionar que el SIL del Sistema de Paro de Emergencia para el área de pozos está supeditado por la contribución a la probabilidad de falla de la consola Baker que va desde un 46% hasta un 94% ante los eventos analizados.

MINIMAL CUT SET (Grupo de Corte Mínimo)	% DE CONTRIBUCION Y/O IMPORTANCIA	NO-DISPONIBILIDAD DEL MINIMAL CUT SET
{BAKER}	94.40	4.89E-03
{PSH/L,RESOLV}	0.08	3.83E-06
{PSH/L,PB}	0.08	3.83E-06
{SSV,SCSSV}	5.44	2.81E-04
{PSH/L,PT,AL-VIS,AL-AUD}	0.00	2.41E-09
	100.00	5.18E-03
Factor de Reducción del Riesgo:	193.10 años	

Tabla V.1 Resultados ante el evento de Sobrepresión en Pozos de Producción.

MINIMAL CUT SET (Grupo de Corte Mínimo)	% DE CONTRIBUCION Y/O IMPORTANCIA	NO-DISPONIBILIDAD DEL MINIMAL CUT SET
{BAKER}	49.90	4.89E-03
{PB}	22.20	2.19E-03
{RESOLV}	22.20	2.19E-03
{SSV-16,SCSSV-16}	2.85	2.81E-04
{SSV-18,SCSSV-18}	2.85	2.81E-04
{AL-VIS,AL-AUD,F-101,F-104,F-105}	0.00	8.63E-11
	100.00	9.83E-03
Factor de Reducción del Riesgo: 101.71 años		

Tabla V.2 Resultados ante el evento de fuego externo en Pozos de Producción.

MINIMAL CUT SET (Grupo de Corte Mínimo)	% DE CONTRIBUCION Y/O IMPORTANCIA	NO-DISPONIBILIDAD DEL MINIMAL CUT SET
{BAKER}	47.50	4.89E-03
{PB}	21.20	2.19E-03
{RESOLV}	21.20	2.19E-03
{AUD,VIS}	4.36	4.50E-04
{SSV-16,SCSSV-16}	2.71	2.81E-04
{SSV-18,SCSSV-18}	2.71	2.81E-04
{GC-101,GC-102}	0.32	3.32E-05
	100.00	1.03E-02
Factor de Reducción del Riesgo: 96.94 años		

Tabla V.3 Resultados ante el evento de fuga de gas combustible en Pozos de Producción.

MINIMAL CUT SET (Grupo de Corte Mínimo)	% DE CONTRIBUCION Y/O IMPORTANCIA	NO-DISPONIBILIDAD DEL MINIMAL CUT SET
{BAKER}	46.80	4.89E-03
{RESOLV}	20.80	2.19E-03
{PB}	20.80	2.19E-03
{SSV-16,SCSSV-16}	2.68	2.81E-04
{SSV-18,SCSSV-18}	2.68	2.81E-04
{GT-101,GT-102}	1.92	2.01E-04
{AUD,VIS}	4.32	4.50E-04
	100.00	1.05E-02
Factor de Reducción del Riesgo: 95.39 años		

Tabla V.4 Resultados ante el evento de fuga de gas tóxico en Pozos de Producción.

MINIMAL CUT SET (Grupo de Corte Mínimo)	% DE CONTRIBUCION Y/O IMPORTANCIA	NO-DISPONIBILIDAD DEL MINIMAL CUT SET
{BAKER}	89.50	4.89E-03
{SSV16,SCSSV16}	5.11	2.81E-04
{SSV18,SCSSV}	5.11	2.81E-04
{RESOLV,PSL-16}	0.07	3.83E-06
{RESOLV,PSL-18}	0.07	3.83E-06
{PB,PSL-16}	0.07	3.83E-06
{PB,PSL-18}	0.07	3.83E-06
{PSL-16,GC-101,GC-102,GT-101,GT-102,PT}	0.00	3.58E-14
	100.00	5.47E-03
Factor de Reducción del Riesgo: 182.90 años		

Tabla V.5 Resultados ante el evento de Ruptura en Pozos de Producción.

MINIMAL CUT SET (Grupo de Corte Mínimo)	% DE CONTRIBUCION Y/O IMPORTANCIA
{AL-VIS}	27.70
{AL-AUD}	27.70
{SCSSV}	12.90
{BAKER}	10.10
{SSV}	8.73
{RESOLV}	4.51
{PT}	3.73
{PSH/L}	3.73
{PB}	0.90
Tiempo medio de Paro en Falso (MTF^{Spurious})	10.46 años

Tabla V.6 Resultados ante el evento de Paro en Falso en pozos de producción.

V.2 Separador de prueba FA-1101

La operación de aforo de pozos mediante la que se efectúa la medición de la cantidad de gas y aceite que tiene la mezcla de cada uno de los pozos 16 y 18, se efectúa de manera intermitente según el programa general de aforo de pozos del Activo, bajo la estricta supervisión y control del personal de operación. Por lo anterior, esto implica que ante un evento o condición anormal el separador de prueba FA-1101 quede protegido, lo cual se lleva a cabo cerrando la fuente de alimentación o Pozos de producción 16 y 18 cualesquiera o ambos que se encuentren alineados a prueba.

Por lo tanto, los resultados de Probabilidad de Falla en Demanda, Nivel de Integridad de la Seguridad, Factor de Reducción de Riesgo e importancia y contribución a la no-disponibilidad de este sistema, son exactamente los mismos a los analizados anteriormente para los pozos de producción No. 16 y 18, con un ligero cambio en la combinación de los Grupos de Cortes Mínimos o Minimal Cut Set del caso de fuego externo en donde en lugar de tres detectores UV/IR intervienen solo dos detectores y no es significativo el cambio en la no-disponibilidad dado a la ubicación de dichos detectores en el árbol de falla.

En las siguientes Tablas V.7, V.8, V.9, V.10 y V.11 se muestra la combinación de los Grupos de Cortes Mínimos o Minimal Cut Set de acuerdo a su importancia y contribución a la no-disponibilidad para el sistema de paro de emergencia en el separador de prueba FA-1101 de Ixtoc-A, ante los siguientes eventos: **Sobrepresión, Fuego externo, Fuga de gas combustible, Fuga de gas tóxico y Ruptura**, respectivamente. Y en la tabla VI.12 la importancia del minimal cut set o componentes básicos de este sistema a contribuir a un paro en falso del mencionado separador en operación de aforo.

Como podrá observarse, los resultados obtenidos en ambos sistemas, Pozos de Producción No. 16, 18 y Separador de Prueba FA-1101 son idénticos, esto se debe a que los elementos básicos involucrados o que forman el sistema configurado al SPE son los mismos (Transmisor, detectores, ejecutor lógico, baker, válvula SSV, válvula SCSSV y botón de paro de emergencia en cuarto de control) y poseen la misma Tasa de Falla.

MINIMAL CUT SET (Grupo de Corte Mínimo)	% DE CONTRIBUCION Y/O IMPORTANCIA	NO-DISPONIBILIDAD DEL MINIMAL CUT SET
{BAKER}	94.40	4.89E-03
{PSH/L,RESOLV}	0.08	3.83E-06
{PSH/L,PB}	0.08	3.83E-06
{SSV,SCSSV}	5.44	2.81E-04
{PSH/L,PT,AL-VIS,AL-AUD}	0.00	2.41E-09
	100.00	5.18E-03
Factor de Reducción del Riesgo:	193.10 años	

Tabla V.7 Resultados ante el evento de Sobrepresión en Separador de Prueba.

MINIMAL CUT SET (Grupo de Corte Mínimo)	% DE CONTRIBUCION Y/O IMPORTANCIA	NO-DISPONIBILIDAD DEL MINIMAL CUT SET
{BAKER}	49.90	4.89E-03
{PB}	22.20	2.19E-03
{RESOLV}	22.20	2.19E-03
{SSV-16,SCSSV-16}	2.85	2.81E-04
{SSV-18,SCSSV-18}	2.85	2.81E-04
{AL-VIS,AL-AUD,F-102,F-103}	0.00	8.63E-11
	100.00	9.83E-03
Factor de Reducción del Riesgo:	101.71 años	

Tabla V.8 Resultados ante el evento de fuego externo en Separador de Prueba.

MINIMAL CUT SET (Grupo de Corte Mínimo)	% DE CONTRIBUCION Y/O IMPORTANCIA	NO-DISPONIBILIDAD DEL MINIMAL CUT SET
{BAKER}	47.50	4.89E-03
{PB}	21.20	2.19E-03
{RESOLV}	21.20	2.19E-03
{AUD,VIS}	4.36	4.50E-04
{SSV-16,SCSSV-16}	2.71	2.81E-04
{SSV-18,SCSSV-18}	2.71	2.81E-04
{GC-103,GC-104}	0.32	3.32E-05
	100.00	1.03E-02
Factor de Reducción del Riesgo:	96.94 años	

Tabla V.9 Resultados ante el evento de fuga de gas combustible en Separador de Prueba.

MINIMAL CUT SET (Grupo de Corte Mínimo)	% DE CONTRIBUCION Y/O IMPORTANCIA	NO-DISPONIBILIDAD DEL MINIMAL CUT SET
{BAKER}	46.80	4.89E-03
{RESOLV}	20.80	2.19E-03
{PB}	20.80	2.19E-03
{SSV-16,SCSSV-16}	2.68	2.81E-04
{SSV-18,SCSSV-18}	2.68	2.81E-04
{GT-103,GT-104}	1.92	2.01E-04
{AUD,VIS}	4.32	4.50E-04
	100.00	1.05E-02
Factor de Reducción del Riesgo:	95.39 años	

Tabla V.10 Resultados ante el evento de fuga de gas tóxico en Separador de Prueba

ESTA TESIS NO SALE DE LA BIBLIOTECA

Capítulo 7
Análisis de resultados

MINIMAL CUT SET (Grupo de Corte Mínimo)	% DE CONTRIBUCION Y/O IMPORTANCIA	NO-DISPONIBILIDAD DEL MINIMAL CUT SET
{BAKER}	89.50	4.89E-03
{SSV16,SCSSV16}	5.11	2.81E-04
{SSV18,SCSSV}	5.11	2.81E-04
{RESOLV,PSL-16}	0.07	3.83E-06
{RESOLV,PSL-18}	0.07	3.83E-06
{PB,PSL-16}	0.07	3.83E-06
{PB,PSL-18}	0.07	3.83E-06
{PSL-16,GC-103,GC-104,GT-103,GT-104,PT}	0.00	3.58E-14
	100.00	5.47E-03
Factor de Reducción del Riesgo: 182.90 años		

Tabla V.11 Resultados ante el evento de Ruptura en Separador de Prueba.

MINIMAL CUT SET (Grupo de Corte Mínimo)	% DE CONTRIBUCION Y/O IMPORTANCIA
{AL-VIS}	27.70
{AL-AUD}	27.70
{SCSSV}	12.90
{BAKER}	10.10
{SSV}	8.73
{RESOLV}	4.51
{PT}	3.73
{PSH/L}	3.73
{PB}	0.90
Tiempo medio de Paro en Falso (MTTF^{Spurious})	10.46 años

Tabla V.12 Resultados ante el evento de Paro en Falso en Separador de Prueba

V.3 Línea de salida 8" P-1108

En forma análoga en las siguientes Tablas V.13, V.14, V.15 y V.16 se muestra la combinación de los Grupos de Cortes Mínimos o Minimal Cut Set de acuerdo a su importancia y contribución a la no-disponibilidad para el sistema de paro de emergencia en la Línea de Salida 8" P-1108 Ixtoc-A, ante los siguientes eventos: **Sobrepresión, Fuga de gas combustible, Fuga de gas tóxico y Ruptura**, respectivamente.

Sobrepresión. La Probabilidad de Falla en Demanda (PFD) del Sistema de Paro de Emergencia (SPE) ante el evento de Sobrepresión es de 2.99E-02 equivalente a una Disponibilidad del 97.01% lo cual implica que se encuentra entre el rango de 90.0% a 99.0%

correspondiente a un Nivel de Integridad de la Seguridad SIL=1, con un Factor de Reducción del Riesgo de 33.4 años. Lo anterior se establece con un periodo máximo de prueba propuesto de 6 meses para los componentes involucrados y aún reduciendo el periodo de prueba o mantenimiento seguiría el sistema teniendo SIL=1. Por otra parte, la lógica del SPE para este sistema ante el evento mencionado es la siguiente: La válvula de paro de emergencia denominada SDV-1170 se cierra cuando el SPE por medio de cualesquiera de los transmisores indicadores de presión PIT-1170A o PIT-1170B detecta una presión mayor con respecto a la máxima presión de operación (MAOP) permisible en la tubería de proceso corriente arriba de dicha válvula SDV-1170. Es obvio e importante mencionar que la activación de estos transmisores también desencadenan el cierre total de los pozos.

Fuga de gas combustible. Para este escenario la Disponibilidad resultante del SPE es 98.4% que corresponde a SIL=1, con un Factor de Reducción de Riesgo de 62.3 años y con un periodo máximo de prueba propuesto de 6 meses. La acción del SPE se efectúa cuando el detector de gas combustible GC-104 detecta y alarma de manera visible y audible para que el operador desde el botón de paro de emergencia desencadene el cierre de la válvula SDV-1170, cuando la concentración alcanza niveles como máximos del 60% del límite inferior de explosividad LEL para gas combustible.

Fuga de gas tóxico. La no-disponibilidad es 2.45E-02 resultante del SPE equivalente al 97.55% que corresponde a SIL=1, con un Factor de Reducción de Riesgo de 40.85 años y con un periodo máximo de prueba propuesto de 6 meses. La acción del SPE se efectúa cuando el detector de gas tóxico GT-104 detecta y alarma de manera visible y audible para que el operador desde el botón de paro de emergencia desencadene el cierre de la válvula SDV-1170, cuando la concentración alcanza niveles como máximos a 40 p.p.m de H₂S de gas tóxico.

Ruptura. La PFD resultante del SPE es de 2.99E-02 equivalente a una Disponibilidad del 97.01% lo cual implica un SIL=1, con un Factor de Reducción del Riesgo de 33.4 años y periodo de prueba de 6 meses. Aquí la acción de cierre de la válvula de paro de emergencia SDV-1170 se lleva a cabo, cuando el SPE por medio de cualesquiera de los transmisores indicadores de presión PIT-1170A o PIT-1170B detecta una baja presión en la tubería de proceso corriente arriba de dicha válvula SDV-1170. También es importante mencionar que la activación de estos transmisores desencadenan el cierre total de los pozos.

Disparo en Falso. Por último, como análisis a este sistema se muestra en la Tabla V.17 la importancia del minimal cut set o componentes básicos de este sistema a contribuir al cierre en falso de la válvula de corte SDV- 1170 (Tiempo Medio de Paro en Falso) $MTTF^{spurious}$ equivalente a 47.8 años.

El mayor contribuyente a la no-disponibilidad del SPE en la Línea de Salida 8" P-1108 ante los eventos o condiciones anormales analizadas, es la válvula de corte SDV-1170 con un 63% en referencia a los demás componentes que intervienen, solenoides, transmisores y resolvidor lógico programable.

MINIMAL CUT SET (Grupo de Corte Mínimo)	% DE CONTRIBUCION Y/O IMPORTANCIA	NO-DISPONIBILIDAD DEL MINIMAL CUT SET
{SDV-1170}	63.20	1.90E-02
{SOL-1}	14.70	4.37E-03
{SOL-2}	14.70	4.37E-03
{RESOLV}	7.37	2.19E-03
{PIT-1170A,PIT-1170B}	0.03	9.37E-06
	100.00	2.99E-02
Factor de Reducción del Riesgo:		33.4 años

Tabla V.13 Resultados ante el evento de Sobrepresión en Línea de Salida.

MINIMAL CUT SET (Grupo de Corte Mínimo)	% DE CONTRIBUCION Y/O IMPORTANCIA	NO-DISPONIBILIDAD DEL MINIMAL CUT SET
{GC}	36.00	5.76E-03
{BKER}	30.60	4.89E-03
{PB}	13.60	2.19E-03
{RESOLV}	13.60	2.19E-03
{AUD,VIS}	2.72	4.50E-04
{SSV-16,SCSSV-16}	1.74	2.81E-04
{SSV-18,SCSSV-18}	1.74	2.81E-04
	100.00	1.60E-02
Factor de Reducción del Riesgo:		62.3 años

Tabla V.14 Resultados ante el evento de fuga de gas combustible en Línea de Salida.

MINIMAL CUT SET (Grupo de Corte Mínimo)	% DE CONTRIBUCION Y/O IMPORTANCIA	NO-DISPONIBILIDAD DEL MINIMAL CUT SET
{GT}	57.60	1.42E-02
{BKER}	20.20	4.89E-03
{RESOLV}	9.01	2.19E-03
{PB}	9.01	2.19E-03
{AUD,VIS}	1.86	4.50E-04
{SSV-16,SCSSV-16}	1.16	2.81E-04
{SSV-18,SCSSV-18}	1.16	2.81E-04
	100.00	2.45E-02
Factor de Reducción del Riesgo: 40.85 años		

Tabla V.15 Resultados ante el evento de fuga de gas tóxico en Línea de Salida.

MINIMAL CUT SET (Grupo de Corte Mínimo)	% DE CONTRIBUCION Y/O IMPORTANCIA	NO-DISPONIBILIDAD DEL MINIMAL CUT SET
{SDV-1170}	63.20	1.90E-02
{SOL-1}	14.70	4.37E-03
{SOL-2}	14.70	4.37E-03
{RESOLV}	7.37	2.19E-03
{PIT-1170A,PIT-1170B}	0.03	9.37E-06
	100.00%	2.99E-02
Factor de Reducción del Riesgo: 33.4 años		

Tabla V.16 Resultados ante el evento de Ruptura en Línea de Salida.

MINIMAL CUT SET (Grupo de Corte Mínimo)	% DE CONTRIBUCION Y/O IMPORTANCIA
{RESOLV}	20.70
{PIT-1170A}	17.40
{PIT-1170B}	17.40
{SOL-1}	17.10
{SOL-2}	17.10
{SDV-1170}	10.30
	100.00
Tiempo medio de Paro en Falso (MTTF^{Spurious}) 47.8 años	

Tabla V.17 Resultados ante el evento de Paro en Falso en Línea de Salida

V.4 Sistema global de producción

La Tabla V.18 muestra la combinación de los Grupos de Cortes Mínimos o Minimal Cut Set de acuerdo a su importancia y contribución a la no-disponibilidad para que el sistema de paro de emergencia opere de manera global en todo el proceso de producción ante el evento de **Sobrepresión y Ruptura**. La Probabilidad de Falla en Demanda es $4.52E-03$ equivalente a una Disponibilidad del **99.58%** que representa que el sistema global de producción tiene un Nivel de **Integridad de la Seguridad SIL=2**. Con periodos de prueba de hasta 6 meses como máximo. Por último, la Tabla V.19 representa los componentes básicos a contribuir al cierre o **Disparo en Falso** del sistema global de proceso (Tiempo Medio de Paro en Falso) $MTTF^{spurious}$ equivalente a **9.04 años**, siendo el disparo en falso de las alarmas audibles y visibles el factor limitante que pondría a decisión del operador accionar el botón de paro de emergencia para desencadenar el cierre.

MINIMAL CUT SET (Grupo de Corte Mínimo)	% DE CONTRIBUCIÓN Y/O IMPORTANCIA	NO-DISPONIBILIDAD DEL MINIMAL CUT SET
{RESOLV}	48.40	2.19E-03
{PB}	48.40	2.19E-03
{SDV-1170,BAKER}	2.08	9.32E-05
{SDV-1170,SSV,SCSSV}	0.12	5.36E-06
{SOL-1,BAKER}	0.47	2.14E-05
{SOL-2,BAKER}	0.47	2.14E-05
{SOL-1,SSV,SCSSV}	0.03	1.23E-06
{SOL-2,SSV,SCSSV}	0.03	1.23E-06
{PIT-1170A,PIT-1170B,BAKER}	0.00	4.59E-08
{PIT-1170A,PIT-1170B,SSV,SCSSV}	0.00	2.64E-09
{SOL-1,PSHL,PT,AL-VIS,AL-AUD}	0.00	1.05E-11
{SOL-2,PSHL,PT,AL-VIS,AL-AUD}	0.00	1.05E-11
{SDV-1170,PSHL,PT,AL-VIS,AL-AUD}	0.00	4.60E-11
	100.00	4.52E-03
Factor de Reducción del Riesgo:	221.0 años	

Tabla V.18 Resultados ante Sobrepresión y Ruptura del sistema global.

MINIMAL CUT SET (Grupo de Corte Mínimo)	% DE CONTRIBUCION Y/O IMPORTANCIA
{AL-VIS}	24.40
{AL-AUD}	24.40
{SCSSV}	10.10
{BAKER}	8.66
{SSV}	6.51
{RESOLV}	3.86
{PT}	3.25
{PSH/L}	3.25
{PIT-1170A}	3.25
{PIT-1170B}	3.25
{SOL-1}	3.18
{SOL-2}	3.18
{SDV-1170}	1.93
{PB}	0.78
	100.00
Tiempo medio de Paro en Falso ($MTTF^{Spurious}$)	9.04 años

Tabla V.19 Resultados ante paro en falso del sistema global.

VI. CONCLUSIONES Y RECOMENDACIONES

Se determinó mediante la técnica cuantitativa de árbol de fallas el Nivel de Integridad de Seguridad (SIL) del Sistema de Paro de Emergencia (SPE) de los sistemas de proceso de la plataforma Ixtoc-A ante la presencia de eventos no deseados tales como, Sobrepresión, Fuego externo, Ruptura, Fuga de gas combustible y tóxico, que de presentarse se debe llevar al proceso a un estado seguro mediante la acción del Sistema de Paro de Emergencia

Los sistemas de proceso analizados y su correspondiente SIL definido y calculado fueron los siguientes:

Sistema	SIL (Definido)	SIL (Calculado)
Pozos de producción No. 16 y 18	1	2
Separador de prueba FA-1101	1	2
Línea de Salida 8" P-1108	1	1
Sistema global de producción	2	2

El disparo en falso encontrado para los sistemas analizados fue el siguiente:

Sistema	Disparo en Falso (años)
Pozos de producción No. 16 y 18	10.46
Separador de prueba FA-1101	10.46
Línea de Salida 8" P-1108	47.80
Sistema global de producción	9.04

Se puede apreciar que la ingeniería del SPE se integra de tres partes básicas de control según la normatividad API-RP-14C, ISA-S84.01, ISA-S84.02 e ISA-S91:

1. Dispositivos de detección (sensores)
2. Sistema electrónico programable
3. Elementos de acción de respuesta

Con esto se garantiza que el proceso se llevará a un estado seguro ante eventos no deseados como los antes mencionados mediante la acción del SPE.

Es importante mencionar que los cálculos se realizaron considerando establecer periodos de prueba o mantenimiento de los componentes involucrados en el sistema, como máximo cada 6 meses para lograr el SIL calculado, pero se recomienda que estos periodos sean mas cortos.

por ejemplo cada 3 meses, dependiendo obviamente de los programas del Activo, para que la disponibilidad del sistema de paro de emergencia se vea asegurada.

Se puede apreciar en el capítulo de análisis de resultados que la contribución porcentual de la consola baker a la probabilidad de falla en demanda es alta. **Por tal motivo, y dado que el SPE depende en gran medida de ella, se recomienda realizar un estudio de confiabilidad para obtener la tasa de falla real de las consolas baker en las instalaciones costa fuera de PEP.**

Desgraciadamente, no hay respuesta fácil cuando se asignan StL's. La opción implica examinar la seguridad de la comunidad, del ambiente y los riesgos económicos. Lo más importante, las herramientas se deben desarrollar en el nivel corporativo para asegurarse de que la opción del SIL es constante con la filosofía de la gerencia de riesgo de una compañía y de que el método de la asignación es congruente con las características existentes de las metodologías corporativas del gravamen de riesgo. Los métodos presentados son todos igualmente útiles en convertir datos de PHA en los niveles de seguridad (SIL), incluyendo HAZOP modificado, consecuencia solamente, ALARP, matriz del riesgo, gráfico del riesgo, gravamen cuantitativo y SIL asignado por mandato corporativo. Al elegir un método, hay un número de factores que deben ser considerados:

1. ¿Qué tipo de método se utiliza actualmente para el análisis corporativo del riesgo?
2. ¿Qué tan complejo es el proceso?
3. ¿Se entiende bien el proceso?
4. ¿Cuál es la experiencia y el conocimiento del funcionamiento de la dinámica del proceso?
5. ¿El equipo de la asignación del SIL será constante con el equipo de PHA?

Al elegir cualquier método, es necesario que el personal designado a determinar el SIL, desarrolle procedimientos y guías de consulta para asegurarse de que el método está utilizado correctamente.

VII. BIBLIOGRAFÍA

1. API RP-14C: *Recommended Practice for Analysis, Design, Installation, and Testing of Basic Surface Safety Systems for Offshore Production Platforms*. American Petroleum Institute, 5th Edition, March, 1994.
2. *Application of Safety Instrumented System for the Process Industries*, ISA-S84.01 Standard, 1996.
3. *Guidelines for Hazard Evaluation Procedures*. Center for Chemical Process Safety. AICHE, 1992.
4. *Guidelines for Process Equipment Reliability Data*. Center for Chemical Process Safety. AICHE, 1989.
5. *Guidelines for Safe Automation of Chemical Processes*. Center for de Chemical Process Safety. AICHE, 1993.
6. *Hazard Evaluation: Quantitative Risk Assessment Failure Data*, PSI, Knoxville, TN, November, 1997.
7. Melo González R., Estrada García R., Martínez Fernández J., Meléndez Hernández J., "Evaluación del Nivel de Integridad de la Seguridad (SIL) de un Sistema de Paro de Emergencia empleando metodologías Rigurosas de Confiabilidad", Instituto Mexicano del Petróleo, Julio de 1999, Registro en Trámite.
8. *Offshore Reliability Data Handbook*, OREDA, 1st Edition 1984.
9. *Offshore Reliability Data Handbook*, OREDA, 2nd Edition, 1992.
10. *Offshore Reliability Data Handbook*, OREDA, 3rd Edition, 1997.
11. *Process Safety Management of Highly Hazardous Chemicals. Explosive, and Blasting Agents*, OSHA, Federal regulation 29 CFR 1910.119, Final Rule, February 24, 1992.

12. Safety Instrumented Systems (SIS). Safety Integrity Level (SIL). Evaluation Techniques, ISA dRT84.0.02 Part 2 Determining the SIL of a SIS via Simplified Equations, April, 1998.
13. Safety Instrumented Systems (SIS). Safety Integrity Level (SIL). Evaluation Techniques, ISA dRT84.0.02 Part 3 Fault Tree Analysis Methodology, April, 1998.
14. Vesely, W. E., et. al, "Fault Tree Handbook", NUREG-0492, 1981.
15. Metodologías de análisis de riesgo, Instituto Nacional de Ecología, página de internet: <http://www.ine.gob.mx/dgmrar/ra/tecnicas.htm>.
16. Filosofía del Sistema de Paro de Emergencia plataforma Ixtoc-A, Instituto Mexicano del Petróleo, marzo de 2000.
17. Estrada García R., Martínez Fernández J., "Determinación del Nivel de Integridad de Seguridad", Instituto Mexicano del Petróleo, proyecto: F.01340, marzo de 2000.
18. Dra. Angela E. Summers, "Understanding Safety Integrity Levels", Control Engineering online, página de internet: <http://www.controleng.com/archives/2000/ct10201.00/0002we3.htm>.
19. Dra. Angela E. Summers, "Draft IEC 61508 target safety integrity levels", Institute of Instrumentation and Control Australia Inc., página de internet: <http://www.iica.org.au/journal/143/DIECTSIL.htm>.
20. Estudio de peligro y operabilidad (HAZOP), Activo Ek-Balam, plataforma Ixtoc-A, Instituto Mexicano del Petróleo, junio de 1999