



UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES ZARAGOZA

**DETERMINACIÓN DE LOS SISTEMAS INSTRUMENTADOS DE
SEGURIDAD (SIS) TÍPICOS Y DE SU NIVEL INTEGRAL DE SEGURIDAD
(SIL) DE UNA PLANTA DE DESINTEGRACIÓN CATALÍTICA DE
GASÓLEOS PESADOS**

T E S I S

PARA OBTENER EL TÍTULO DE:

INGENIERO QUÍMICO

QUE PRESENTA:

MARTÍNEZ VEGA ROGELIO

ASESORADO POR:

DR. M. JAVIER CRUZ GÓMEZ



MÉXICO, DISTRITO FEDERAL, 17 DE AGOSTO DEL 2012



Universidad Nacional
Autónoma de México



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: I.Q. XXXXXXXXXXXXXXXXXXXX

Vocal: Dr. M. Javier Cruz Gómez.

Secretario: I.Q. XXXXXXXXXXXXXXXXXXXX

1° Suplente: Dr. Néstor Noé López Castillo.

2° Suplente: I.Q. XXXXXXXXXXXXXXXXXXXX

SITIO DONDE SE DESARROLLÓ EL TEMA:



Torre de Ingeniería, UNAM.

Ciudad Universitaria.

Asesor del tema:

Supervisor técnico:

Dr. M. Javier Cruz Gómez

M. en A. Claudia Mendoza Monroy

Sustentante:

Martínez Vega Rogelio



AGRADECIMIENTOS



DEDICATORIAS



ÍNDICE

ÍNDICE DE FIGURAS	8
ÍNDICE DE TABLAS	9
SÍMBOLOS Y ABREVIATURAS	10
RESUMEN	11
CAPÍTULO 1: INTRODUCCIÓN	12
1.1. Introducción	13
1.2. Planteamiento del problema	14
1.3. Objetivo general	15
1.4. Objetivos específicos	15
1.5. Hipótesis	15
1.6. Justificación	16
1.7. Alcance	17
CAPÍTULO 2: MARCO TEÓRICO	18
2.1. La confusión entre peligro y riesgo	19
2.2. Niveles de riesgo	20
2.3. Reducción del riesgo	21
2.4. Capas de protección independientes	22
2.4.1. Diseño del proceso y la planta	24
2.4.2. Control Básico del Proceso (BPCS)	24
2.4.3. Sistemas de alarma	25
2.4.4. Sistemas Instrumentados de Seguridad (SIS)	26
2.4.5. Dispositivos mecánicos activos de protección (Dispositivos de relevo)	31
2.4.6. Dispositivos mecánicos pasivos de protección (Dispositivos de contención)	31
2.4.7. Sistemas de respuesta a emergencias de la planta	32
2.4.8. Sistemas de respuesta a emergencias de la comunidad	32
2.5. SIS y la Administración de la Seguridad de los Procesos (PSM)	32
2.6. Seguridad funcional	34
2.7. Normatividad	35
2.7.1 IEC 61508	35
2.7.2. ANSI/ISA-84.00.01-2004 (IEC 61511 Mod) y ANSI/ISA-84.01-1996	37



2.8. Ciclo de vida de seguridad	37
2.9. Modos de falla de un SIS.....	38
2.9.1. Falla segura	39
2.9.2. Falla peligrosa	39
2.10. Medida del Desempeño de los SIS	39
2.10.1. Disponibilidad	40
2.10.2. Confiabilidad.....	40
2.10.3. Probabilidad de falla en demanda	41
2.10.4. Nivel Integral de Seguridad (SIL)	41
2.11. Modos de operación del SIS.....	43
2.11.1. Modo de demanda.....	43
2.11.2. Modo continuo	44
2.12. Métodos de cálculo del SIL	44
2.12.1. Método por matriz de riesgos.....	45
2.12.2. Matriz de capas de seguridad	48
2.12.3. Gráfica de riesgo	48
2.12.4. Método LOPA.....	50
2.13. Redundancia.....	55
2.14. SIS vs BPCS	58
CAPÍTULO 3: DESCRIPCIÓN DEL PROCESO DE LA PLANTA BAJO ESTUDIO	59
3.1. Introducción	60
3.2. Química del proceso FCC	60
3.3. La planta FCC en la refinería	61
3.4. Descripción del flujo de la planta catalítica (FCC).....	62
3.4.1. Sección de carga y reacción.....	62
3.4.2. Sección de fraccionamiento	66
3.4.3. Sección de recuperación de vapores.....	68
3.4.4. Sección de tratamiento con amina.....	71
3.4.5. Sección de tratamiento de Merox.....	73



CAPÍTULO 4: DETERMINACIÓN DEL NIVEL INTEGRAL DE SEGURIDAD (SIL)	76
4.1. Información necesaria para la aplicación de la metodología LOPA	77
4.2 Descripción de la metodología.....	78
4.2.1 Definición de los criterios de aceptabilidad de riesgos	79
4.2.2 Identificación de los eventos peligrosos y evaluación de su gravedad	81
4.2.3 Identificación de los eventos iniciales y evaluación de su frecuencia.....	84
4.3.4 Identificación de las capas de protección independientes (IPL's) aplicables	85
4.3.5 Evaluación de la efectividad de las IPL's	87
4.3.6 Obtención de la efectividad total de las capas de protección independientes.....	87
4.3.7. Determinación de la efectividad mínima requerida del evento peligroso considerando las capas de protección independientes	88
4.3.8. Determinación de las capas adicionales de protección y determinación del SIL	89
4.3.9. En caso de requerir un SIS, proponer el diseño conceptual del SIS	90
4.4. Resultados	92
4.5. Análisis de Resultados	117
CONCLUSIONES Y RECOMENDACIONES	121
BIBLIOGRAFÍA	125
ANEXOS	127
ANEXO A: Tablas empleadas en la determinación del SIL.....	128
ANEXO B. Lazos de control del SIS propuesto para el convertidor 1-D	130
ANEXO C. DFP's de una planta FCC.....	134



ÍNDICE DE FIGURAS

Figura 2.1. Diagrama ALARP ⁽³⁾	20
Figura 2.2. Reducción del riesgo ⁽⁴⁾	21
Figura 2.3. Capas de protección independientes ⁽¹⁾	23
Figura 2.4. Definición de un sistema instrumentado de seguridad ⁽⁷⁾	27
Figura 2.5. SIS y su importancia en las capas de protección	28
Figura 2.6. Relación entre SIS y SIL	28
Figura 2.7. Selección de las funciones instrumentadas de seguridad ⁽⁷⁾	29
Figura 2.8. Fallas probables que pretende cubrir IEC 61508.....	36
Figura 2.9. Ciclo de vida de diseño de un sistema instrumentado de seguridad (IEC-61511) ⁽⁷⁾	38
Figura 2.10. Porcentaje de fallas del sistema ⁽¹⁾	39
Figura 2.11. Confusión con el término “Disponibilidad” ⁽¹⁾	40
Figura 2.12. Efecto del SIL en la reducción de riesgos de proceso ⁽¹¹⁾	43
Figura 2.13. Matriz de riesgo tridimensional para seleccionar el SIL.....	48
Figura 2.14. Gráfico de riesgo ⁽¹⁾	50
Figura 2.15. Transformación de HAZOP a LOPA ⁽¹²⁾	52
Figura 2.16. Diagrama de flujo de cálculo del SIL usando el método LOPA ⁽¹²⁾	54
Figura 2.17. Redundancia diversificada	55
Figura 2.18. (A) Ejemplo de configuración SIL 1, (B) SIL 1 alta confiabilidad	57
Figura 2.19. (A) Ejemplo de configuración SIL 2, (B) SIL 2 alta confiabilidad	57
Figura 2.20. (A) Ejemplo de configuración SIL 3, (B) Sil 3 alta confiabilidad	57
Figura 2.21. Independencia del SIS y el BPCS	58
Figura 3.1. Un ejemplo de craqueo catalítico fluidizado de hidrocarburos	60
Figura 3.2. El proceso FCC dentro de la refinería	61
Figura 4.1. Representación de los criterios de aceptabilidad de riesgos en un diagrama frecuencia – gravedad ⁽¹⁵⁾	79
Figura 4.2. Representación de los criterios de aceptación de riesgos para este trabajo.....	81
Figura 4.3. Matriz de riesgos de Pemex refinación utilizada en el análisis	81
Figura 4.4. Formato para la aplicación de la metodología del SIL requerido	91
Figura 4.5. Lazos de control críticos del convertidor 1-D.....	95
Figura 4.6. Sistema de paro de emergencia del convertidor	109
Figura 4.7. Detalle de función instrumentada por paro de compresor	114
Figura 4.8. Instalación típica de las válvulas VAAR para el caso del compresor.....	117



ÍNDICE DE TABLAS

Tabla 2.1. Niveles SIL para operación en modo demanda ⁽⁷⁾	44
Tabla 2.2. Niveles SIL para operación en modo continuo ⁽⁷⁾	44
Tabla 2.3. Frecuencia del riesgo (solo ejemplo)	46
Tabla 2.4. Gravedad del riesgo (solo ejemplo)	47
Tabla 2.5. Riesgo total (solo ejemplo).....	47
Tabla 2.6. Redundancia por votación ⁽¹⁾	56
Tabla 3.1. Distribución de productos generados en una planta FCC ⁽¹³⁾	62
Tabla 4.1. Frecuencia límite en la zona de criterio variable para cada categoría de consecuencia.....	79
Tabla 4.2. Criterios de frecuencia meta asociada a cada categoría de gravedad (G) de las consecuencias ⁽¹⁵⁾	80
Tabla 4.3. Guía para evaluar la gravedad (G) de las consecuencias en función de la cantidad de sustancia derramada y sus características ⁽¹⁵⁾	82
Tabla 4.4. Guía para evaluar la gravedad (G) de las consecuencias en función del receptor ⁽¹⁵⁾	83
Tabla 4.5. Guía para evaluar la gravedad (G) de las consecuencias en función del costo del evento ⁽¹⁵⁾	83
Tabla 4.6. Guía para evaluar la gravedad (G) de las consecuencias en función de la afectación a la producción y a las instalaciones ⁽¹⁵⁾	84
Tabla 4.7. Calificación de frecuencia (F) para los eventos iniciales ⁽¹⁵⁾	85
Tabla 4.8. Protecciones o salvaguardas que usualmente no se consideran IPL's ⁽¹⁵⁾	86
Tabla 4.9. Calificación de la efectividad (E) de las IPL's ⁽¹⁵⁾	87
Tabla 4.10. Determinación del SIL requerido a partir del valor de E_{min}	90
Tabla 4.11. Emergencias en el convertidor 1-D de una planta FCC	92
Tabla 4.12. Entradas del sistema de paro de emergencia del convertidor 1-D de la planta FCC	108
Tabla 4.13. Salidas del sistema de paro de emergencia del convertidor	110
Tabla 4.14. Entradas del sistema de paro de emergencia por pérdida del compresor 2-J de la planta FCC..	113
Tabla 4.15. Salidas del sistema de paro de emergencia por pérdida del compresor 2-J de la planta FCC.....	115
Tabla 4.16. Resumen de las funciones instrumentadas de seguridad obtenidas	118
Tabla 4.17. Reducción del riesgo en la planta FCC de estudio	120



SÍMBOLOS Y ABREVIATURAS

AIChE: American Institute of Chemical Engineering (Instituto Americano de Ingenieros Químicos)

ALARP: As Low As Reasonably Practicable (Tan Bajo Como Sea Razonablemente Factible)

ANSI: American National Standards Institute (Instituto Nacional de Normalización Estadounidense)

CCPS: Center fo Chemical Process Safety (Centro de Seguridad de Procesos Químicos)

DTI: Diagrama de Tubería e Instrumentación.

E/E/PES: Electrical/Electronic/Programmable Electronic System (Sistema Eléctrico, Electrónico, Electrónico Programable)

FCCU: Fluidized Catalytic Cracking Unit (Unidad de Desintegración Catalítica Fluidizada)

HAZOP: Hazard and Operability (Análisis de Peligros y Operabilidad)

IEC: International Electrotechnical Commission (Comisión Electrotécnica Internacional)

IPL: Independient Protection Layer (Capa de Protección Independiente)

ISA: International Society of Automation (Sociedad Internacional de Automatización)

LOPA: Layer Of Protection Analysis (Análisis de Capas de Protección)

PFD. Probability of Failure on Demand (Probabilidad de Falla en Demanda)

PFDavg. Average Probability of Failure on Demand (Probabilidad de Falla en Demanda Pomedio)

RRF: Risk Reduction Factor (Factor de Reducción de Riesgo).

SIF: Safety Instrumented Function (Función Instrumentada de Seguridad)

SIL: Safety Integrity Level (Nivel Integral de Seguridad)

SIS: Safety Instrumented Systems (Sistemas Instrumentados de Seguridad)



RESUMEN

A continuación se presenta un trabajo donde se determinan los Sistemas Instrumentados de Seguridad (SIS) típicos que requiere una planta de desintegración catalítica (FCCU) con el fin de dar seguimiento a las recomendaciones expresadas en el análisis HAZOP para los escenarios con riesgo del tipo A y B, ya que esto ayudará a reducir estos riesgos a un nivel aceptable, y que de no llevarse a cabo, representarían un daño potencial a los trabajadores, al medio ambiente y a la planta. De igual forma se determina el Nivel Integral de Seguridad (SIL) para medir el desempeño necesario de estos sistemas, y de esta forma reducir la cantidad de riesgo detectado.

Para ello se emplea una metodología semicuantitativa simplificada derivada del método LOPA, que selecciona los escenarios de máximo riesgo del estudio HAZOP de la planta y con base en los criterios de aceptabilidad del riesgo para grandes empresas de productos químicos, petroquímicos y de refinación de petróleo, evaluar las capas de protección existentes para el escenario y determina primeramente si un SIS es necesario y de ser afirmativo, determina su SIL objetivo.

Para llevar a cabo todo esto previamente se realiza un análisis profundo de la normatividad internacional vigente así como del proceso de desintegración catalítica (FCC).

Una vez realizada la determinación del SIS y su SIL, inherentemente se ha generado su hoja de cálculo del SIL, posteriormente se propone un lazo de control que simboliza propiamente a los SIS determinados en el DTI y se da una descripción de la función que realiza y cómo es que lo hace. Todo esto con el fin de ubicar el papel del ingeniero químico y el impacto que este tiene en una tarea multidisciplinaria como esta.

Palabras Clave: Sistemas Instrumentados de Seguridad, Nivel Integral de Seguridad, Función Instrumentada de Seguridad, FCC, LOPA.

CAPÍTULO 1: INTRODUCCIÓN





1.1. Introducción

Al entrar en una etapa de globalización, las industrias químicas de proceso y de refinación de petróleo necesitan producir la mayor cantidad de productos terminados, para lograr satisfacer la demanda existente de los millones de consumidores y así mismo poder competir con otras empresas globales. Esto ha traído como consecuencia el incremento del tamaño de las plantas y con ello el manejo de grandes cantidades de sustancias como materia prima.

Muchas de estas sustancias naturalmente tienen propiedades tóxicas, reactivas, corrosivas e inflamables, y algunas de ellas son sometidas a condiciones de operación extremas (presiones y temperaturas demasiado altas), por lo que en cualquier momento existe la posibilidad de una liberación accidental de alguna de estas sustancias peligrosas provocando un accidente potencialmente desastroso.

Los incidentes catastróficos en Bhopal (India), San Juan Ixhuatepec (México), Texas City (EUA) y Buncefield (Inglaterra) sirven como recordatorios de lo que puede suceder cuando las cosas se hacen mal. Como consecuencia, hoy en día las industrias de procesos químicos y de refinación de petróleo de todo el mundo, han visto la imperiosa necesidad de maximizar la seguridad de los trabajadores y de las instalaciones, así como la protección del medio ambiente.

Uno de los esfuerzos que se realiza actualmente para lograr este objetivo es mediante la implementación de un Sistema de Gestión de la Seguridad de los Procesos, una herramienta analítica que ayuda proactiva y sistemáticamente en la identificación, evaluación, mitigación o prevención de las emisiones de productos químicos altamente peligrosos que podrían ocurrir como resultado de fallas en los procesos, procedimientos o en los equipos.

La industria química y de refinación del petróleo es muy dinámica y la rapidez del cambio tecnológico es un componente que abona a la maximización de la seguridad, y dentro de ese sistema de gestión de la seguridad de procesos se encuentran los Sistemas Instrumentados de Seguridad (SIS). Estos han tomado gran relevancia durante los últimos años y son muy importantes en la administración de riesgos como capa de protección, ya que cumplen una función primordial evitando los eventos de riesgo o minimizando la severidad de las consecuencias al personal, medio ambiente e instalaciones.



1.2. Planteamiento del problema

En vista de que el proceso FCC es dinámico y opera a altas temperaturas, las perturbaciones operativas rápidamente pueden causar serios problemas que ponen en peligro a los trabajadores, el medio ambiente, la producción y las instalaciones.

Cuando ocurre un descontrol en una unidad FCC, la primera preocupación es mantener la planta trabajando y de ser posible, operando a plena capacidad. Esto se debe a que la planta FCC es fuente de carga de otras plantas, por lo que los paros de emergencia repentinos en la unidad interrumpen su fuente de alimentación, sobre todo cuando existe sólo una unidad FCC en toda la refinería. De igual forma, al ser la fuente que más aporta gasolina a la refinería, un paro en esta planta significa grandes pérdidas económicas para la empresa.

La única consideración que se opone a la preocupación de un descontrol en la unidad FCC es que esta perturbación provoque una emergencia severa que ponga en riesgo al personal, al medio ambiente y a las instalaciones. Sin embargo la detección apropiada e inmediata de las condiciones anormales y las respuestas adecuadas de los sistemas de seguridad ayudan a evitar daños al personal y a las instalaciones además de que reducen al mínimo el tiempo de inactividad de la unidad, asegurando una recuperación rápida de su funcionamiento.

Es por ello que la implementación de funciones instrumentadas de seguridad (SIF) en una planta FCC ha venido cobrando fuerza, porque sin duda puede ayudar a reducir los riesgos, sin embargo, no es una tarea fácil ni mucho menos que se tome a la ligera por todo lo que representa un paro de planta de esta magnitud.

Lo que se quiere lograr es una tendencia sobre implementar los sistemas instrumentados de seguridad (SIS) en secciones de la planta donde se ha detectado un riesgo potencial justificado por un análisis de riesgos. Lo más importante de todo es que estas funciones llevarán a la planta a un estado seguro, pero sobre todo, colocarán a la planta en condiciones adecuadas para una muy rápida puesta en marcha, lo que no significa un paro completo de planta como tal. Para lograr esto, se debe tener un amplio conocimiento del proceso FCC, además de entender claramente los riesgos inherentes del proceso.



Ahora bien, el problema como tal no es determinar el Sistema Instrumentado de Seguridad (SIS) que necesita la planta, más bien, el problema radica en evaluar la confiabilidad de ese sistema, es decir, la probabilidad de que el dispositivo de seguridad ejecute la función asignada cuando ésta es requerida, de tal forma que el sistema no quede sobredimensionado o corto, a esto se le conoce como el Nivel Integral de Seguridad (SIL) y además de eso, hacer una buena estimación de la magnitud de reducción de riesgo al implementar el SIS.

1.3. Objetivo general

Determinar los Sistemas Instrumentados de Seguridad (SIS) y su Nivel de Integridad de Seguridad (SIL), con el fin de alcanzar un nivel de confiabilidad que permita la operación segura, así como un nivel de riesgos aceptable en una planta de desintegración catalítica de gasóleos pesados (FCC) basado en los resultados del análisis HAZOP de la planta.

1.4. Objetivos específicos

- ✓ Analizar la normatividad internacional vigente referente a los Sistemas Instrumentados de Seguridad (SIS) aplicada a la industria de procesos químicos (IEC 61508, IEC 61511/ISA84).
- ✓ Analizar el proceso de una planta típica de desintegración catalítica de gasóleos pesados (FCC).
- ✓ Determinar si es requerido un SIS en la planta con base en el HAZOP y calcular su SIL.
- ✓ Generar las hojas de cálculo del SIL de cada función instrumentada de seguridad.
- ✓ Presentar una propuesta de lazo de control del SIS requerido y dar una descripción general de la lógica de funcionamiento.

1.5. Hipótesis

Es posible determinar los sistemas instrumentados de seguridad y su respectivo nivel integral de seguridad, a partir de un análisis HAZOP realizado con anterioridad a una planta de desintegración catalítica de gasóleos pesados, tomando en cuenta solo los escenarios con un nivel de riesgo tipo A y tipo B, utilizando una metodología semicuantitativa simplificada, que entre otras cosas permitirá reducir los riesgos detectados a un nivel aceptable mediante la implementación de un SIS que no tendrá un valor de SIL mayor a 1.



1.6. Justificación

La publicación de las normas internacionales de seguridad funcional IEC 61508 (1999), IEC 61511/ISA84 (2004) e IEC-62061 (2005) fueron hitos importantes en el esfuerzo por incrementar la certidumbre de equipos y procesos. Desafortunadamente, la publicación de normas de este tipo por sí mismas no hacen del mundo un lugar más seguro, hace falta contar con personas competentes que tengan conocimiento y experiencia en la aplicación sobre estas normas de seguridad funcional.

Conforme avanza el tiempo se han desarrollado diversos métodos para determinar los sistemas instrumentados de seguridad de una planta y evaluar su desempeño, algunos demasiado simples y otros más complejos que presentan metodologías confusas, tediosas y sin fundamentos, y peor aún, ninguna de estas justifica la implementación de dichos sistemas en la planta.

Hasta hoy, todos los proyectos de ingeniería relacionados con la industria química de procesos y de refinación del petróleo a nivel mundial están solicitando entre sus actividades de ingeniería la determinación del nivel integral de seguridad y el posterior diseño del sistema instrumentado de seguridad de acuerdo a la normatividad internacional. Inclusive, se están realizando esfuerzos en implementar este tipo de sistemas a plantas que llevan operando por décadas, debido a que cuando fueron concebidas no existían tales herramientas de seguridad.

Pero debido a la confusión generada sobre este tema, muchas empresas que se dedican a la consultoría sobre seguridad y sobre todo los vendedores de sistemas de seguridad se aprovechan de la situación y al realizar la determinación del nivel integral de seguridad, complican aún más los conceptos, aumentando la confusión en el cliente, traduciéndose en un sistema sobredimensionado sumamente caro, difícilmente operable y en algunos casos inseguros para el proceso.

Otro elemento que aporta a la confusión del tema es que a menudo, para muchos ingenieros químicos, los “sistemas de seguridad” se refiere a la administración de procedimientos y prácticas y no al sistema de control, por lo que con este trabajo se pretende ubicar el papel del ingeniero químico y la importancia que tiene en el desarrollo de procesos más seguros.



Por lo tanto, este trabajo resulta de la necesidad de emplear una metodología sistemática, que incluya un análisis de capas de protección (LOPA) para determinar el nivel de integridad de seguridad de los sistemas instrumentados de seguridad. Esta es la forma adecuada de reducir el riesgo.

1.7. Alcance

En este trabajo se aplicará la normatividad internacional vigente IEC-508 y IEC-511 para la determinación de los Sistemas Instrumentados de Seguridad (SIS) y de su Nivel Integral de Seguridad (SIL) debido a que esta es la base de todas las normas que se han desarrollado actualmente dentro de este ámbito como las normas de Pemex Refinación o de alguna otra compañía petrolera de otro país.

En vista de que en el ámbito internacional actual aún se debate rigurosamente si es que los sistemas de detección de gas y fuego (F&GS, Fire & Gas System, por sus siglas en inglés) pertenecen a los sistemas instrumentados de seguridad (SIS), además de la forma en que deben ser diseñados sin que se llegue a un consenso generalizado por parte de los especialistas, en este trabajo se dejará fuera este aspecto y por ello no se determinarán sistemas que tengan que ver con la detección de gas y fuego ni se evaluará su nivel integral de seguridad (SIL).

Un punto importante es que el proceso al que se está refiriendo en este trabajo como la determinación de los SIS y de su SIL permite varias connotaciones, incluso se ha llegado a pensar que este proceso significa el diseño del SIS, por lo que se hace hincapié que no se diseñará por completo un sistema instrumentado de seguridad, porque se está consciente que para lograr esto se deben cumplir todos los aspectos de la especificación de requisitos de seguridad (SRS) y existen puntos de esta que sería difícil que un ingeniero químico determinara e interpretara debido a que son términos puramente electrónicos.

Por lo tanto, el alcance de este trabajo resultará en el aporte que un ingeniero químico puede dar a este campo de la seguridad funcional debido a sus amplios conocimientos del proceso y de la cuantificación del riesgo para la determinación de los SIS, primeramente justificando plenamente su existencia, asignándole la función que realizará, y posteriormente determinando su SIL.

CAPÍTULO 2: MARCO TEÓRICO





2.1. La confusión entre peligro y riesgo

Para comenzar, se vuelve necesario detenerse en dos conceptos fundamentales que se relacionan estrechamente con la seguridad, que es la parte medular de esta tesis: peligro y riesgo.

Una de las causas principales de los precarios resultados que se obtuvieron durante la mayor parte del siglo XX en la seguridad de las plantas químicas y de refinación del petróleo alrededor del mundo, es la confusión conceptual que se ha venido arrastrando entre peligro y riesgo. ⁽¹⁾

El problema radica en la claridad con que deben ser definidos estos conceptos ya que en la vida cotidiana muchas personas no entienden su significado y diferencia, esto los lleva a confundirse al usar estas palabras en diversas situaciones riesgosas o peligrosas.

La CCPS (Center of Chemical Process Safety) define **peligro** como una condición física o química que tiene el potencial de causar daños a las personas, al medio ambiente y/o a las instalaciones; mientras que el **riesgo** es el resultado de la combinación de la probabilidad de ocurrencia (evento/año) y severidad (efecto/evento) de un incidente aislado o un grupo de incidencias. La probabilidad está en función de la frecuencia y duración de la exposición al peligro. ⁽²⁾

El peligro es, por consiguiente, una situación de hecho, es decir que está presente inherentemente, mientras que el riesgo es una probabilidad de que haya una causa o evento iniciador que haga que un peligro provoque algún daño.

En las plantas químicas y de refinación del petróleo, el peligro está constituido, en sí mismo, por las sustancias tóxicas, corrosivas, reactivas e inflamables que se utilizan, las condiciones de operación extremas a las que son sometidas estas sustancias para su transformación, las energías que se manejan para llegar a tener esas condiciones de operación extremas, etc. El riesgo es la probabilidad de que una o más de esas sustancias altamente peligrosas sea liberada en forma accidental (llamada usualmente como pérdida de contención) y cause algún daño a los trabajadores, al medio ambiente o a las instalaciones.

A diferencia del peligro, que es una condición inherente de las cosas y que depende de su naturaleza, el riesgo se puede cuantificar y reducir su magnitud.

2.2. Niveles de riesgo

El principio **ALARP** (As Low As Reasonably Practicable) que en español es “tan bajo como sea razonablemente posible” reconoce que hay tres grandes categorías de riesgos y esto se puede apreciar en la **figura 2.1**.

En la región intolerable, el nivel de riesgo es tan alto que exige acciones significativas y urgentes para reducir su magnitud. La región ALARP, es una región donde el riesgo es tolerable. Para que un riesgo sea considerado ALARP debe ser posible demostrar que el costo de continuar reduciendo ese riesgo es desproporcionado en comparación con el beneficio que se obtendría. El principio ALARP se origina en el hecho de que para conseguir reducir el riesgo residual a cero sería necesario emplear recursos económicos, tiempo y esfuerzo infinitos. ALARP no es una medida cuantitativa de beneficio contra perjuicio, sino una práctica de juicio para obtener un equilibrio entre riesgo y beneficio a la sociedad. ALARP es un requisito fundamental para la gestión de los riesgos industriales. En la región ampliamente aceptable, el nivel de riesgos es muy bajo y no requiere acciones para reducir la magnitud en el futuro. Pero debe ser manejado y monitoreado en todo momento. ^{(1) (3)}

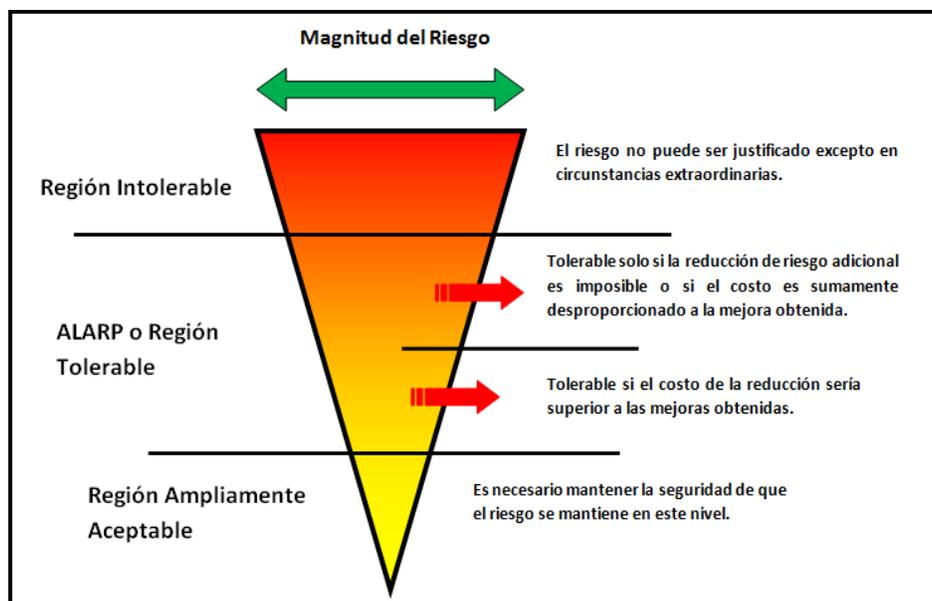


Figura 2.1. Diagrama ALARP ⁽³⁾

2.3. Reducción del riesgo

Si bien es cierto que no se puede eliminar el riesgo por completo, cada proceso químico tiene un cierto grado de riesgo asociado a él, al que le llamamos riesgo inherente del proceso y los esfuerzos se enfocan en disminuir este a una cierta magnitud que sea tolerable o aceptable. ⁽¹⁾

Para hacer frente al problema anterior, se puede observar en la **figura 2.2** que la reducción del riesgo es el trabajo de las capas de protección, tales como, un sistema instrumentado de seguridad o un sistema de alarmas etc. Cuando se propone diseñar un sistema de protección, se tiene que decidir lo eficaz que debe ser, es decir, la cantidad de riesgo que se necesita reducir. ⁽¹⁾

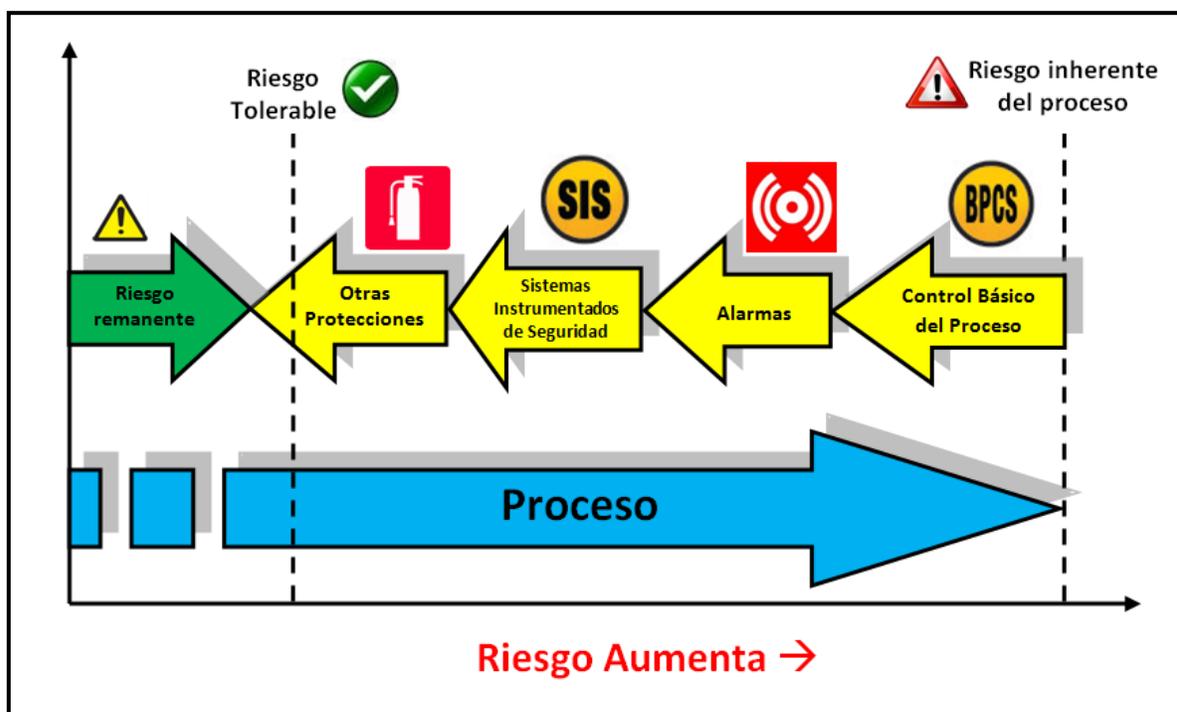


Figura 2.2. Reducción del riesgo ⁽⁴⁾

Muchas veces, el principio ALARP ayuda a definir el objetivo de riesgo aceptable para una instalación en función de los factores sociales, políticos y económicos que son de interés para la empresa. Este principio también es utilizado por muchas empresas para definir el objetivo de riesgo aceptable para la seguridad de los trabajadores, impacto ambiental y pérdida de la producción. ⁽³⁾



Para lograr este objetivo se implementan una serie de capas de protección que sirven para reducir el riesgo a un nivel aceptable. Aun con esto, existe un nivel de riesgo remanente o residual después de que estas capas de protección han sido implementadas. Este nivel de riesgo es aceptado en un contexto basado en valores actuales de la sociedad. ⁽²⁾

2.4. Capas de protección independientes

A grandes rasgos, al realizar una evaluación de peligros y riesgos, se logran identificar las necesidades globales de reducción de riesgo y con ellos se asignan las capas de protección independientes necesarias (IPL, Independent Layer Protección, por sus siglas en inglés). ⁽⁴⁾

Ninguna medida de seguridad es capaz de eliminar el riesgo y proteger al personal y la planta contra el daño, o mitigar la propagación del daño si se produce un incidente peligroso. Por esta razón, existen las capas de protección: *que son dispositivos, sistemas o acciones capaces de prevenir o mitigar el que un escenario continúe hacia consecuencias indeseables independientemente del evento inicial y de la acción o falla de cualquier otra capa de protección asociada con el escenario.* ⁽⁵⁾

Las capas de protección deben cumplir con ciertas consideraciones como:

- Eficacia en la prevención de la consecuencia cuando funciona según lo diseñado.
- Independiente del evento inicial y de los componentes de cualquier otra capa de protección demandada para el mismo escenario.
- Auditable; la eficacia asumida en términos de la prevención de la consecuencia debe ser capaz de validarse de alguna manera (por la documentación, la revisión, pruebas, etc.). ⁽⁶⁾

Si una capa de protección falla, debido a que son independientes, capas sucesivas estarán disponibles para llevar el proceso a un estado seguro. Conforme el número de capas de protección se incrementa, la seguridad del proceso irá en aumento. La **figura 2.3** muestra la sucesión de capas de seguridad conforme al orden de activación ante un incidente.

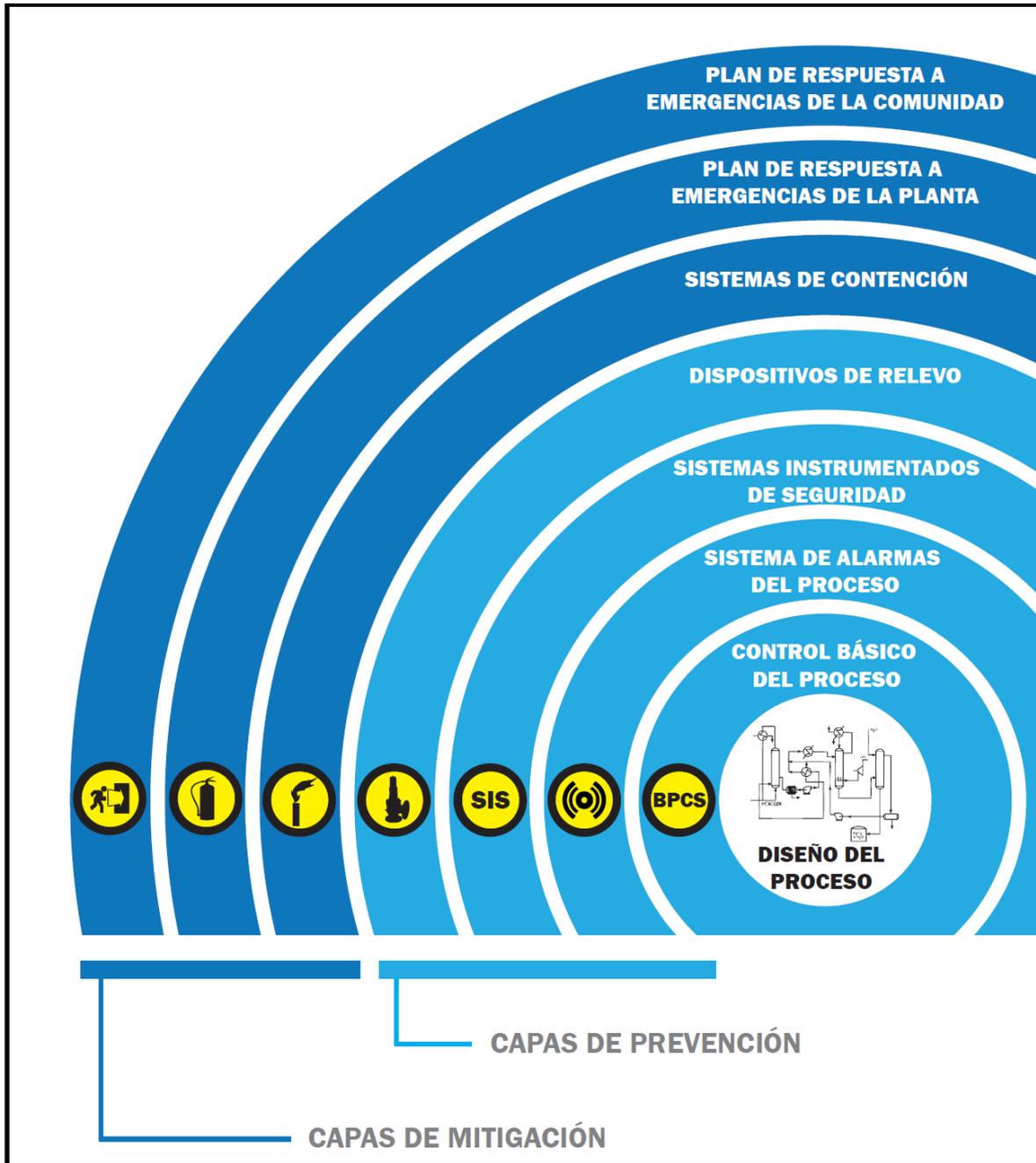


Figura 2.3. Capas de protección independientes⁽¹⁾

Las capas de prevención se aplican para reducir la probabilidad o posibilidad de que ocurra un evento peligroso. Se diseñan considerando la frecuencia de exposición al riesgo de las personas, la probabilidad de la presencia del evento iniciador del riesgo, y la severidad de las consecuencias si el mismo es eventualmente iniciado.⁽¹⁾



Las capas de mitigación de riesgos se diseñan para controlar los eventos peligrosos iniciados, y para reducir el impacto del evento a las instalaciones, el medio ambiente y la vida humana.⁽¹⁾

2.4.1. Diseño del proceso y la planta

Con demasiada frecuencia, las consideraciones de seguridad se dejan para las etapas finales del diseño de los procesos químicos y se considera que hacer una planta más segura resultará en un proceso más caro. Si no se consideran los posibles riesgos asociados a las plantas químicas (fundamentalmente incendios, explosiones y emisiones de productos tóxicos), los problemas que posteriormente se plantean requieren soluciones complejas y habitualmente costosas. Sin embargo, en muchos casos, una seguridad mayor no supone un costo mayor. La mejor estrategia es considerar la seguridad cuando se desarrolla el diseño del proceso. Las plantas diseñadas de este modo se llaman de seguridad inherente y el esfuerzo por realizar estas plantas va en aumento.⁽¹⁾

Es por ello que se insiste en la necesidad de que los estudios de análisis de riesgos y detección de peligros deben nacer con la ingeniería conceptual del proyecto. Así, la seguridad debe influir en las decisiones de diseño desde los primeros momentos del proyecto. Eliminar o reducir los peligros a menudo lleva a diseños más simples, lo que puede en sí mismo, reducir el riesgo.⁽²⁾

2.4.2. Control Básico del Proceso (BPCS)

El sistema de control básico del proceso (BPCS) es la segunda capa de protección, pero se convierte en la primera para procesos que no fueron desarrollados inherentemente seguros. Se encarga por medio de lazos de control, de mantener todas las variables de proceso como la presión, la temperatura, el nivel, el flujo, etc., dentro de límites seguros, es decir, dentro de los límites en que se diseñaron los equipos y tuberías para operar. Además de que sirve para mantener un uso eficiente de energía, también es usado para lograr una calidad óptima en los productos y al mismo tiempo es considerado una capa de seguridad. Sin embargo, hay que tener en cuenta que una falla del sistema de control también podrá iniciar un evento peligroso.⁽⁴⁾



Sin duda, la automatización ha evolucionado drásticamente durante los últimos años llegando al grado de automatizar todas las operaciones en las industrias químicas de procesos y de refinación del petróleo. Es fácil pensar que la tecnología es buena y que va a resolver todos los problemas que se presenten, sin embargo, solo es cuestión de tiempo para que los sistemas de control fallen. Aunado a esto, la automatización no elimina a los seres humanos del sistema. ⁽¹⁾

Los procesos automatizados modernos normalmente se “operan” a sí mismos en condiciones óptimas, pero cuando hay un problema, los operadores no saben qué hacer o toman malas decisiones, porque:

- No entienden el proceso, el control y/o las condiciones que dan lugar a los eventos anormales que se presentaron.
- Tienen que tomar decisiones complejas en poco tiempo.
- Información incompleta: algunos instrumentos tienen fallas, algunas alarmas no se activaron (falla bajo demanda), algunos sistemas de seguridad están desactivados o no funcionan.
- Las políticas empresariales en caso de emergencias son confusas: dicen que “la seguridad es primero”, pero hay sanciones si se detiene la producción.
- Largos periodos de monitoreo pasivo pueden hacer que los operadores no estén preparados para actuar en situaciones de emergencia.

2.4.3. Sistemas de alarma

Si el sistema de control básico de procesos no cumple con su función (por cualquier número de razones, tales como una falla interna, atascamiento de una válvula o un lazo que se coloca en directo) las alarmas se utilizan para alertar a los operadores de que alguna variable se está saliendo de control y se requiere que intervenga.

La función de los sistemas de alarma y monitoreo es detectar los problemas tan pronto como sea posible, para realizar una acción antes de que las condiciones peligrosas se alcancen y deben ser:



- Ser independientes del control básico de procesos.
- Ser de los más simples como sea posible.
- Ser fáciles de mantener, comprobar y calibrar. ⁽³⁾

Los sistemas de alarma y monitoreo son considerados como la capa de seguridad donde los operadores participan activamente. El operador humano manipula bajo prácticas y conocimientos obtenidos de su capacitación y adiestramiento continuo, las variables del proceso que pueden quedar fuera de control ante la presencia de desviaciones y de situaciones de emergencia. Entre estas situaciones se encuentran los cortes inesperados de energía eléctrica, fallas en el suministro de vapor, agua de enfriamiento, aire de instrumentos, el descontrol de la operación de la planta, la falla de algún equipo, etc. ⁽⁶⁾

El operador humano ejecuta las acciones necesarias para llevar la operación de su planta de proceso a condiciones de falla segura en un estado de riesgo remanente aceptado. Estas actividades del operador humano están documentadas en los procedimientos operativos de arranque y procedimientos de paro normal y de emergencia de la planta de proceso y sus equipos.

2.4.4. Sistemas Instrumentados de Seguridad (SIS)

Si el sistema de control básico del proceso (BPCS) y los operadores no actúan correctamente al responder a una alarma, los sistemas instrumentados de seguridad (SIS) comienzan a tomar medidas, detectando fallas o desviaciones dentro del proceso y desencadenan las acciones apropiadas y necesarias para salvaguardar tanto la vida de las personas, los equipos, la continuidad de la producción y las exigentes regulaciones ambientales. Estos sistemas son totalmente independientes del control básico del proceso y del sistema de alarmas, con sus propios elementos desde el sensor hasta el elemento final, incluyendo entradas, salidas, fuente de alimentación y solucionadores de la lógica como lo muestra la **figura 2.4.** ⁽¹⁾

Estos sistemas están diseñados para permitir que un proceso avance de una manera segura, cuando:

- Predeterminados puntos de calibración (set points) son excedidos.
- Las condiciones de operación seguras son violadas.
- Tomar medidas para mitigar las consecuencias de un riesgo industrial.

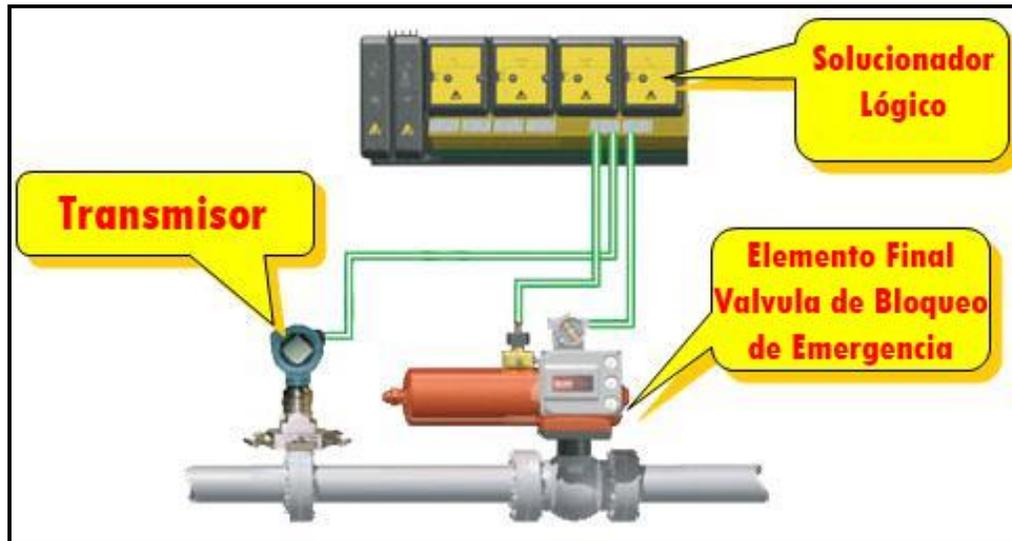


Figura 2.4. Definición de un sistema instrumentado de seguridad⁽⁷⁾

Por lo tanto, un sistema instrumentado de seguridad, puede proporcionar funciones permisivas, preventivas y/o de mitigación. Estos sistemas implementan funciones instrumentadas de seguridad (SIF), normalmente a variables críticas cuyo descontrol no puede ser atendido por el operador humano debido a su complejidad, rapidez de desarrollo, y que requieren detectarse de manera temprana y oportuna.

Para esto, la norma ANSI/ISA-91.00.01-2001 define la categoría, "Control de Seguridad Crítica", como un control cuyo fracaso para funcionar correctamente resultará directamente en una liberación catastrófica de tóxicos, reactivos químicos, inflamables o explosivos como lo demuestra la **figura 2.5.**⁽⁷⁾



Figura 2.5. SIS y su importancia en las capas de protección

2.4.4.1. Relación entre SIS y SIF

Es importante distinguir entre una función instrumentada de seguridad (SIF) y un Sistema Instrumentado de Seguridad (SIS). Una SIF se refiere a una sola función (por ejemplo, el apagado por alta presión, el apagado por bajo nivel, etc), con un nivel integral de seguridad (SIL) específico, mientras que un SIS se refiere a todas las funciones combinadas que componen el sistema en general, tal como se muestra en la **figura 2.6**.

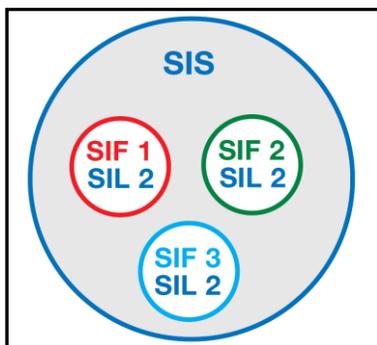


Figura 2.6. Relación entre SIS y SIL

Cada sistema instrumentado de seguridad tiene una o más funciones instrumentadas de seguridad y cada una detecta un peligro en específico para llevar el proceso a un estado seguro, ofreciendo una medida de reducción del riesgo indicada por su nivel de integridad de seguridad (SIL). El SIS no tiene un SIL asignado.

La norma IEC 61511 establece la ruta para la selección de las funciones instrumentadas de seguridad, proporcionando el diagrama de selección de las funciones de seguridad como se puede apreciar en la **figura 2.7.** ⁽⁷⁾

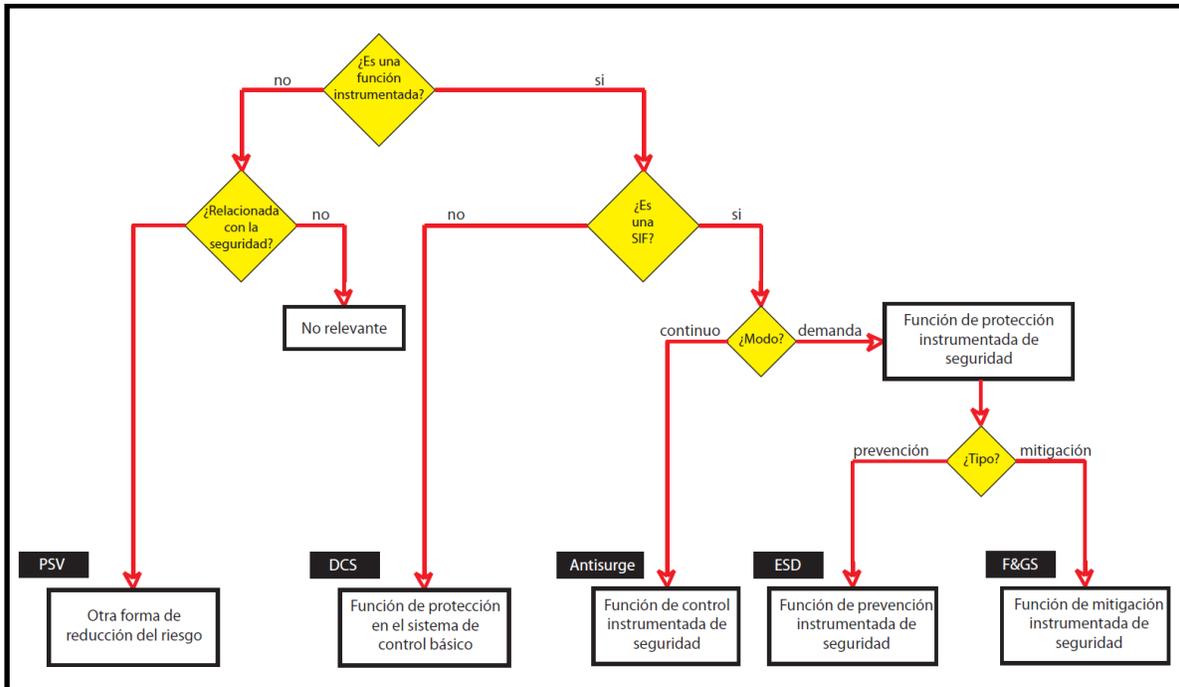


Figura 2.7. Selección de las funciones instrumentadas de seguridad ⁽⁷⁾

2.4.4.2. Sistemas de paro de emergencia

Los sistemas de paro de emergencia (Emergency Shutdown-ESD) son la expresión más común de las funciones instrumentadas de seguridad y son un conjunto de elementos que interactúan entre sí para llevar el proceso a una condición segura cuando se presentan condiciones peligrosas en los procesos, estos sistemas están normalmente vivos, es decir, se encuentran normalmente energizados o en posición 1. Una de las características de estos sistemas es la falla segura por lo que a falla de cualquier componente del sistema (sensores, controlador lógico, elementos finales) el sistema se coloca en una posición ó condición segura para el proceso, generalmente esta condición es la de paro del proceso ó de la función instrumentada de seguridad que se está protegiendo. ⁽⁸⁾



2.4.4.3. Sistemas de control de quemadores

Los sistemas de Control de Quemadores (Burner Management Systems- BMS) son una variante de los sistemas de paro por emergencia ya que en su primera función de operación tienen la función de ayudar a arrancar/parar una caldera o un horno de forma segura y su segunda función es la de mantener una operación segura, por su diseño estos sistemas requieren tanto confiabilidad como tolerancia a fallas, el diseño de estos sistemas es complejo ya que combinan funciones de protección y control. ⁽¹⁾

2.4.4.4. Sistemas de protección de presión de alta integridad

HIPPS es la abreviación de High Integrity Pressure Protection System, que es una aplicación de un sistema instrumentado de seguridad (SIS), diseñado de acuerdo con la norma IEC 61508. El propósito de un sistema HIPPS es el de proteger equipos e instalaciones corriente abajo contra una sobrepresión cerrando válvulas que lo aíslan de la fuente de esa sobrepresión. Generalmente esto se hace cerrando las válvulas de corte rápido dedicadas a prevenir la sobrepresión de las instalaciones. ⁽¹⁾

Debido a restricciones ambientales y control de costos, estos sistemas han ganado popularidad en los últimos años como la última línea de defensa, reemplazando a las válvulas de seguridad (PSV), válvulas “blow down” y flares.

2.4.4.5. Sistemas de gas y fuego

Los sistemas de monitoreo de gas y fuego (Fire and Gas-F&G) son sistemas pasivos, es decir, estos sistemas no actúan hasta que se detecta una fuga de gas combustible, alguna sustancia tóxica o bien la presencia de fuego. La función de estos sistemas es la de mitigación, actúan después de que se ha presentado una condición insegura, es decir, alertan a los operadores de presencia de fuego, gases tóxicos o humo en las áreas protegidas por este sistema, a su vez, se encargará de encender las bombas para presurizar líneas de agua contra incendio, hacer sonar alarmas audibles y visibles. Por su naturaleza, estos sistemas no requieren de tolerancia a fallas, dado que la falla de algún componente no genera disparos en falso, normalmente estos sistemas son diseñados con un alto nivel de diagnósticos capaces de detectar si algún sensor o elemento



final de control se encuentra fallando o bien si el cable que conduce la señal ha sido cortado o si se presenta un corto circuito que pueda inhabilitar al sensor o al elemento final. Cabe destacar que sigue el debate si el sistema de gas y fuego pertenece a los sistemas instrumentados de seguridad, ya que entre otras cosas, su función no es prevenir sino mitigar. ⁽¹⁾

2.4.4.6. Antisurge

El sistema antisurge o de control de flujo mínimo pertenece también a los sistemas instrumentados de seguridad. Su función es asegurar un flujo a través del compresor independientemente de la velocidad del compresor. El controlador de flujo mínimo debe ajustarse para impedir que el flujo de descarga baje hasta el punto de ocasionar el “disparo” (surge) del compresor. ⁽¹⁾

2.4.5. Dispositivos mecánicos activos de protección (Dispositivos de relevo)

Están diseñados para proteger la integridad mecánica de equipos, tuberías y recipientes a presión. Entre estos dispositivos encontramos las válvulas de seguridad y relevo por sobrepresión (PSV), los dispositivos de relevo térmico, discos de ruptura, válvulas rompedoras de vacío, etc. Si bien estos dispositivos pueden servir para evitar que un recipiente a presión explote, el desfogue del material puede resultar en un evento secundario peligroso (por ejemplo, la liberación de un material tóxico) o multas debido a una violación de normas medioambientales. ⁽⁸⁾

2.4.6. Dispositivos mecánicos pasivos de protección (Dispositivos de contención)

Son todos aquellos sistemas diseñados para la canalización de fugas, desfogues, derrames, siendo estos los diques de contención, torres lavadoras (scrubbers), quemadores elevados (flare), quemadores de piso, muros cortafuego, materiales de construcción no combustibles, barreras físicas, sistemas de drenaje aceitoso, drenajes químicos, fosas de captación y tratamiento, sistemas de quemado e incineración, sistemas de recolección y tratamiento de residuos peligrosos, etc. En la práctica son sistemas de protección al medio ambiente y de la salud de los trabajadores y de los habitantes en las comunidades aledañas ó regionales. ⁽⁸⁾



2.4.7. Sistemas de respuesta a emergencias de la planta

Lo conforman los cuerpos de bomberos, de rescate y de atención médica en planta, y de otros cuerpos especializados de contención de riesgos. Se consideran aquí también los sistemas contra incendio conformados por las redes de agua contra incendio y su equipamiento, así como la situación estratégica de equipos manuales de extinción de incendios (extinguidores fijos y portátiles). Se incluyen también los sistemas de aviso de evacuación del personal, métodos de aislamiento y avisos de trabajos peligrosos, establecimiento de vías de escape, puntos de reunión seguros, y todos aquellos planes y programas de salud y seguridad en el trabajo. ⁽¹⁾

2.4.8. Sistemas de respuesta a emergencias de la comunidad

Lo conforman los comités locales de ayuda mutua, sistemas de vías de escape, sistemas para la evacuación general de la población, intervención del ejército, policía, cuerpos de bomberos y de rescate de la comunidad, cuerpos especializados externos a la planta, y de todos aquellos planes y programas de salud general y de mantenimiento del entorno ambiental. ⁽¹⁾

2.5. SIS y la Administración de la Seguridad de los Procesos (PSM)

La industria química y de refinación del petróleo tiene un gran interés en la escritura de sus propias normas, directrices y prácticas recomendadas, sin embargo debido a grandes desastres en plantas químicas de proceso durante los años 80's y principios de los 90's, el temor por parte del gobierno estadounidense a una gran catástrofe obligo a intervenir y fue por eso que en 1992 la OSHA (Occupational Safety and Health Administration) publicó el estándar OSHA 29 CFR 1910.119 bajo el nombre de "Administración de la Seguridad de Procesos de Productos Altamente Peligrosos."

Se ha convertido en un estándar importante ya que las compañías aseguradoras internacionales recomiendan para todos sus asegurados (bajo pena de primas más altas) un desempeño mínimo acorde a lo que la OSHA establece para sus empresas en Estados Unidos.

En este estándar, se define en pocas palabras a la Administración de la Seguridad de los Procesos (PSM, por sus siglas en inglés) como el conjunto de elementos técnico-administrativos, interrelacionados y dispuestos, para asegurarse de que las diferentes protecciones, que evitan



accidentes e incidentes derivados de las fugas o liberaciones de sustancias químicas peligrosas, estén en su lugar y sean efectivas cuando se requieran. ⁽¹⁾

Los elementos que están cubiertos por la Administración de la Seguridad de los Procesos son la información de la seguridad del proceso, los análisis de riesgos de proceso, los procedimientos de operación, la participación de los trabajadores, la capacitación y entrenamiento, los contratistas, los permisos de trabajo, la administración al cambio, la investigación de incidentes, el plan de respuesta a emergencias, las auditorías de cumplimiento, la revisión previa a la puesta en marcha, los secretos comerciales y la integridad mecánica.

Sin embargo, esta tesis no pretende ahondar en cada uno de los elementos que componen a la Administración de la Seguridad de los Procesos, más bien lo que se quiere es ubicar la relación que existe entre los Sistemas Instrumentados de Seguridad (SIS) y la Administración de la Seguridad de los Procesos.

Pues bien, siguiendo con el estándar de OSHA 29 CFR Parte 1910.119 requiere que las organizaciones garanticen la integridad mecánica de todos sus sistemas de paro de emergencia y los controles de seguridad críticos.

Para asegurar la integridad mecánica de estos sistemas es necesario implementar un programa de actividades para garantizar que el equipo está diseñado, fabricado, adquirido, instalado, operado y mantenido de una manera apropiada para su aplicación prevista durante su tiempo de operación hasta su desmantelamiento, de manera segura, con esto se pretende asegurar la protección al personal, al medio ambiente y a las instalaciones. ⁽¹⁾

Ahora bien, el estándar de OSHA resulta una gran aportación en cuanto a la seguridad en las plantas químicas de proceso y de refinación de petróleo, pero no responde a las preguntas ¿Qué es una manera segura de operar? y sobre todo una pregunta que tiene un poco de connotación filosófica: ¿Qué tan seguro es lo suficientemente seguro?

Si bien, el estándar OSHA 29 CFR no es una receta, muchas normas y estándares de ingeniería se estaban convirtiendo en esto, pero hay un cambio en la manera en que las normas se están escribiendo. Se están alejando de ser normas prescriptivas y se están orientando más a la



ejecución de requisitos. Esto significa que cada organización tendrá que decidir por sí mismo lo que es seguro. Por desgracia, se trata de decisiones difíciles que pocos quieren hacer, y menos aún quieren poner por escrito. Lo que es seguro trasciende la ciencia pura y se ocupa de las cuestiones filosóficas, morales y legales.

Vale la pena señalar que OSHA dirigió una carta a ISA en el año 2000 donde indica que reconoce ANSI/ISA-84.01-1996 como una buena práctica de ingeniería reconocida y aceptada en general para los sistemas instrumentados de seguridad (SIS), y que si una empresa está en cumplimiento con la norma, el empleador será considerado en el cumplimiento de los requisitos de la administración de la seguridad de los procesos de la OSHA para los sistemas instrumentados de seguridad (SIS).

2.6. Seguridad funcional

Hasta este punto se han abordado los distintos tipos de sistemas de seguridad que se pueden implementar en una planta química para reducir los riesgos y con ellos hacerla más segura, sin embargo, no solo es diseñar el sistema de seguridad e implementarlo en la planta esperando que funcione correctamente, esta ha sido la forma de diseñar y construir plantas durante mucho tiempo. La automatización del equipamiento técnico para funciones relacionadas a seguridad en procesos a través de sistemas instrumentados de seguridad (SIS) implica ciertos riesgos ya que si este sistema de seguridad llegara a fallar las consecuencias podrían ser catastróficas.

Por lo tanto, surgen preguntas tan abrumadoras como: ¿Qué tan confiable es el funcionamiento del sistema de seguridad?, ¿Cómo se puede determinar y de qué forma se sabe que los sistemas de seguridad están funcionando de manera segura?⁽¹⁾

Uno de los indicadores para la evaluación de estos sistemas es la seguridad funcional. La seguridad funcional es la parte de la seguridad global que depende de que un sistema o equipo funcione correctamente en respuesta a sus entradas, es decir, la garantía de funcionamiento del sistema de seguridad con respecto a una posible demanda real de riesgo en las plantas de procesos.⁽¹⁰⁾



La evaluación de la seguridad funcional de los sistemas instrumentados de seguridad se lleva a cabo bajo la consideración de los siguientes parámetros:

- ¿Cuál es la función de seguridad? - ¿Qué hace la función de seguridad?
- ¿Cuál es el nivel de integridad de seguridad? – ¿Qué grado de certidumbre existe del desempeño de la función de seguridad?

La seguridad funcional es un concepto aplicable en todos los sectores de la industria, y aún más en la industria química de procesos y de refinación del petróleo. Es fundamental ya que asegura que los sistemas instrumentados de seguridad (SIS) ofrezcan la reducción del riesgo necesario para lograr la seguridad para el equipo.

2.7. Normatividad

Hasta hace unos años solo existían normas nacionales para la planificación, la construcción y la operación de las instalaciones de seguridad para la industria. Así por ejemplo, para el mercado alemán, los fabricantes y usuarios de dichas instalaciones se remitieron a las normas de seguridad DIN 19250, DIN 19251 y DIN 801. Con estas normas se describía el dimensionamiento de los dispositivos relevantes para la seguridad mediante las clases de seguridad AK (Clases AK 1-8).

Puesto que muchos países contaban con normas distintas, y con muy variadas nomenclaturas, para el correcto funcionamiento de dispositivos de seguridad, se emitió en el año de 1998 una norma de requisitos básicos con acreditación internacional a través de la Comisión Electrotécnica Internacional (IEC, International Electrotechnical Commission, por sus siglas en inglés) con sede en Génova, Suiza. Esta norma, válida para todo el mundo es la IEC 61508. ⁽¹⁾

A partir de la norma base IEC 61508 nacieron una serie de normas de aplicación para diferentes ramas y necesidades de la industria, en las que se definieron los requisitos organizacionales y técnicos exigidos a las instalaciones de seguridad y a su implementación.

2.7.1 IEC 61508

La norma industrial internacional IEC 61508 “Functional safety of Electrical/Electronic/Programmable Electronic safety-related systems” (Seguridad Funcional de los Sistemas

Eléctricos/Electrónicos/Electrónicos Programables relacionados a la Seguridad) fue desarrollada, durante varios años, mediante el consenso de expertos y representantes de las áreas de diseño y operación de sistemas críticos de seguridad y publicada en 1988.

IEC 61508 se aplica a sistemas relacionados con la seguridad cuando uno o más de tales sistemas incorporan dispositivos eléctricos y/o electrónicos y/o electrónicos programables (E/E/PE). Cubre los posibles riesgos causados por el fracaso de las funciones de seguridad que se deben realizar por los E/E/PE relacionadas con los sistemas de seguridad.⁽¹⁰⁾

La norma aplica al ciclo de vida entero del sistema de seguridad, desde su concepción, especificación, diseño, funcionamiento y uso, hasta su decomisionamiento. Consta de siete partes, las tres primeras partes de la norma proveen el manejo, desarrollo, despliegue y operación de los efectos del sistema de E/E/PES en hardware y software para seguridad. Las últimas cuatro partes de la norma tratan específicamente de las definiciones, aplicaciones y anexos informativos a la norma.

Esta norma se considera como una sombrilla que cubre distintas fallas de los sistemas de seguridad en diversas industrias como puede visualizarse en la **figura 2.8**. También es importante señalar que se considera actualmente como el estándar para los fabricantes y vendedores de equipos. Por ejemplo, cuando un vendedor recibe un producto certificado para su uso en un determinado nivel de integridad de seguridad (SIL), la agencia de certificación normalmente utiliza la norma IEC 61508 como base para la aprobación.

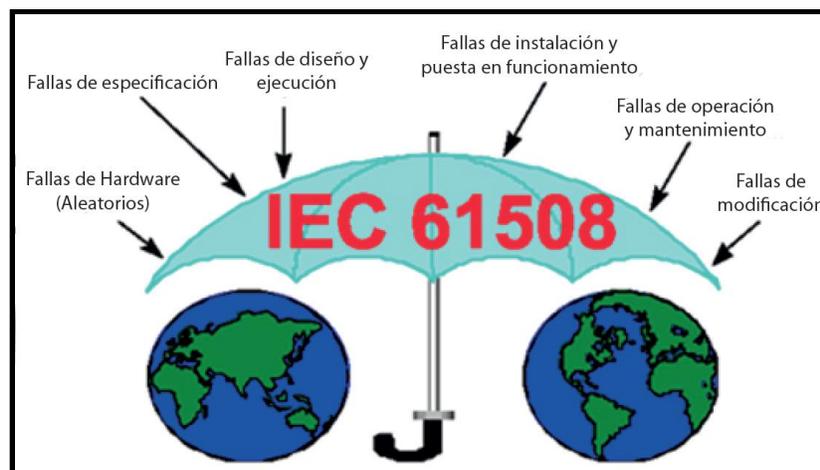


Figura 2.8. Fallas probables que pretende cubrir IEC 61508



2.7.2. ANSI/ISA-84.00.01-2004 (IEC 61511 Mod) y ANSI/ISA-84.01-1996

Haciendo un poco de historia, durante el desarrollo del estándar de la ISA SP84 el comité de la IEC comenzó con su norma general IEC 61508. El comité de ISA SP84 creyó que su estándar podría utilizarse como un estándar industrial específico para las industrias de procesos en el ámbito de la IEC. Con esto, la IEC desarrolló su estándar 61511 utilizando la norma ANSI/ISA-84.01-1996 como punto de partida. En lugar de reescribir el estándar SP84 ISA desde cero, el comité decidió aprobarla como la norma IEC 61511 con la adición de una "cláusula de abuelo" de la versión original de 1996 del estándar SP84 ISA. El nuevo estándar de tres partes es designado ANSI/ISA-84.00.01-2004, partes 1-3 (IEC 61511 Mod) y fue publicado en 2004.

La clausula de abuelo dice que: "Para los sistemas instrumentados de seguridad (SIS) existentes, diseñados y construidos de acuerdo con los códigos, normas o prácticas antes de la emisión de esta norma (por ejemplo, la norma ANSI / ISA 84.01-1996), el propietario/operador deberá determinar y documentar que el equipo está diseñado, inspeccionado, probado y hecho funcionar de una manera segura. " (7)

La norma IEC 61511 "Functional safety - Safety instrumented systems for the process industry sector" (Seguridad Funcional – Sistemas instrumentados de seguridad para el sector de la industria de procesos) fue dirigida a los diseñadores y usuarios finales, establece que éstos deben cumplir un ciclo de vida del SIS, el cual incluye el análisis actualizado del riesgo, diseño, instalación, comisionamiento, validación, operación, mantenimiento, modificaciones y desmantelamiento del SIS.

2.8. Ciclo de vida de seguridad

Tanto la norma IEC 61508 y IEC 61511 utiliza el ciclo de vida de seguridad como los requisitos relativos para la estructura de la especificación, diseño, integración, operación, mantenimiento, modificación y decomisionamiento de un sistema instrumentado de seguridad (SIS). Cada fase tiene un conjunto de entradas y salidas definidas, y hacia el final de cada fase, una verificación se llevará a cabo para confirmar que los resultados requeridos están según lo previsto. Mientras que el ciclo de vida de seguridad de la IEC 61508 está enfocado en la seguridad global de los E/E/EP, el ciclo de vida de seguridad de la IEC 61511 va dirigido en concreto a los sistemas

instrumentados de seguridad (SIS). La **figura 2.9** muestra los pasos del ciclo de vida como se describe en la norma IEC 61511.

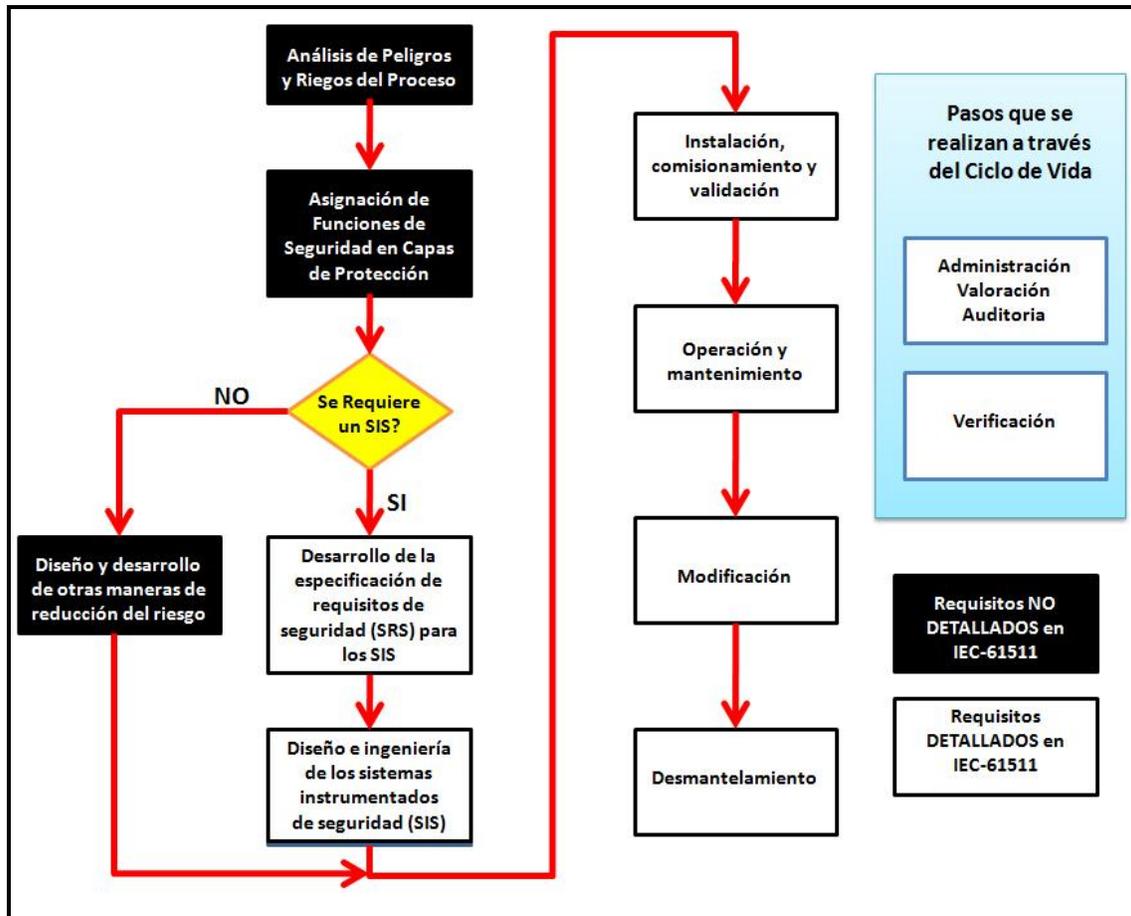


Figura 2.9. Ciclo de vida de diseño de un sistema instrumentado de seguridad (IEC-61511) ⁽⁷⁾

2.9. Modos de falla de un SIS

Debido a que un sistema instrumentado de seguridad (SIS) se compone de elementos eléctricos, electrónicos y electrónicos programables (E/E/PE) es muy común que estos fallen.

Una falla es cuando existe una diferencia entre la respuesta que genera un equipo y la respuesta que se espera. Su principal consecuencia es la pérdida de producción pero también puede tener un gran impacto en la seguridad.

La **figura 2.10** muestra el porcentaje de falla de los dispositivos que componen un sistema instrumentado de seguridad.

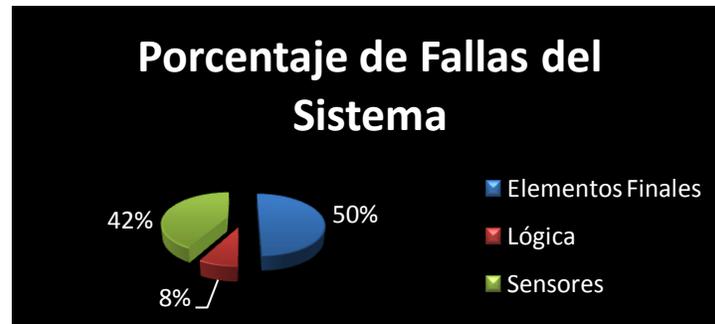


Figura 2.10. Porcentaje de fallas del sistema ⁽¹⁾

2.9.1. Falla segura

Una falla segura es la que ocurre cuando algún componente del SIS se daña y genera un paro de la instalación en falso, es decir, que nunca existió una condición potencialmente peligrosa que ameritara detener la operación, aunque ésta también puede darse en los sensores de campo, cuando reportan una falsa medición. ⁽¹⁾

2.9.2. Falla peligrosa

Falla peligrosa, es cuando el SIS no responde ante una señal de peligro pudiendo desencadenar una situación de peligro latente, esta se puede dar en los instrumentos sensores, actuadores o en el solucionador lógico. Es por ello que es importante contar con rutinas de diagnóstico que continuamente verifiquen el buen funcionamiento integral del sistema. ⁽¹⁾

2.10. Medida del Desempeño de los SIS

Para medir y comparar el desempeño de diferentes sistemas de seguridad, se necesita un marco común de referencia, un conjunto de términos comunes que sea comprensible. Durante años se han utilizado numerosos términos para el desempeño de estos sistemas, tales como la disponibilidad y confiabilidad. Lamentablemente, estos términos aparentemente triviales han causado problemas.

La razón principal se deriva de los dos modos de falla diferentes de los sistemas de seguridad analizados anteriormente (modo de falla segura y modo de falla peligrosa). Si hay dos modos de falla, debe haber dos términos de desempeño diferentes, uno para cada modo de fallo.

2.10.1. Disponibilidad

La disponibilidad de un sistema es la relación entre el tiempo que el sistema funciona como se conceptualizó y el tiempo total de vida del sistema, idealmente esta relación debe ser en porcentaje el 100%, aunque existen 3 posibles escenarios de disponibilidad tal como se muestra en la **figura 2.11** en donde no se representan porcentajes, solo es representativa.

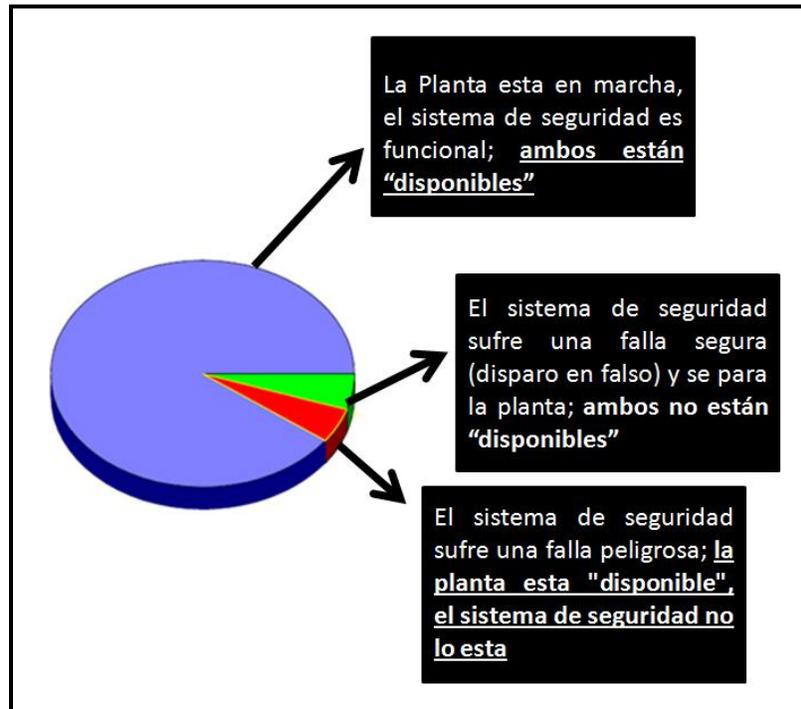


Figura 2.11. Confusión con el término "Disponibilidad" ⁽¹⁾

La figura anterior muestra claramente las diferencias entre cada uno de los escenarios posibles, sin embargo, en la mayoría de los casos las personas no son conscientes de lo que significa la parte donde el SIS no es funcional, por lo que el SIS no está disponible, pero la planta está todavía en marcha. En este tipo de falla, la planta no se para, la planta está disponible y aún produciendo, sin embargo, el SIS no funcionará cuando sea necesario. En este caso, la "disponibilidad" de los dos sistemas (el SIS y la planta) claramente no es la misma.

2.10.2. Confiabilidad

Confiabilidad se define como la probabilidad de que un sistema opere correctamente bajo condiciones predeterminadas durante un tiempo determinado. La confiabilidad es resultado de



muchos factores, tal como la calidad de sus componentes estos deben presentar una muy buena manufactura para que puedan garantizar un desempeño óptimo en su vida útil, esto se logra debido a los estándares de calidad con los que los fabricantes de equipo se apegan rigurosamente para sacar al mercado sus productos. También puede lograrse una alta confiabilidad mediante técnicas de redundancia, que es el hecho de poner a varios elementos del mismo tipo a desempeñar una función, así como que los dispositivos no trabajen al límite de sus capacidades para no estar propensos a daños por sobre rangos o situaciones extremas. ⁽¹⁾

2.10.3. Probabilidad de falla en demanda

La IEC-61508 define la Probabilidad de Falla en Demanda (PFD, por sus siglas en inglés, Probability of Failure on Demand), como la probabilidad estadística de que un sistema falle en forma peligrosa. Es el complemento de la disponibilidad de un sistema de seguridad y por esa misma razón también es conocido como la no disponibilidad (Unavailability). ⁽¹⁾

Es utilizada para evaluar la efectividad de las capas de protección independientes (IPL). La PFD es un número adimensional entre 0 y 1. Cuanto más pequeño es el valor de la PFD, más grande es la reducción en la frecuencia de la consecuencia para una frecuencia dada del evento iniciador. La reducción en la frecuencia alcanzada por un CPI también es conocida como el factor de reducción de riesgo.

Por ejemplo, la probabilidad de falla en demanda para cada una de las funciones de seguridad manejadas por un sistema de paro de emergencia (ESD), es la suma de las probabilidades promedio de cada elemento de la función de seguridad (sensor, actuador, controlador lógico programable). Las PFD son utilizadas para la fijación y determinación de los Niveles SIL.

2.10.4. Nivel Integral de Seguridad (SIL)

El nivel Integral de seguridad (SIL) es una representación estadística de la confiabilidad de los sistemas instrumentados de seguridad cuando una demanda en el proceso ocurre, es decir, cuando se presenta una situación de riesgo latente. ⁽¹⁾



Hay que recalcar que el SIL no es directamente una medida de riesgo de proceso, sino más bien una medida del desempeño del sistema de seguridad, necesaria para reducir los riesgos identificados anteriormente a un nivel aceptable como se muestra en la **figura 2.12**, con esto, sería incorrecto asignar un valor SIL a un proceso químico o a un equipo de proceso en específico. Cuanta más alta es la cifra del SIL, es mayor es la reducción del riesgo. ⁽¹¹⁾

Además, es incorrecto referirse al SIL de un componente individual de un sistema (por ejemplo, un sensor, un actuador, etc.). Cada componente individual podría ser evaluado para su uso en aplicaciones de un determinado SIL. Sería más apropiado referirse a la probabilidad de falla en demanda (PFD) de un componente individual.

Existen 2 tipos de SIL, el SIL requerido (target SIL) que es el valor para cada escenario de alto riesgo potencial que la empresa debe identificar, mientras que el SIL instalado (installed SIL) es el valor que el proveedor debe calcular para su propuesta y debe coincidir con el SIL requerido para el escenario de riesgo determinado.

La determinación del SIL aplica en instalaciones que deben cumplir condiciones técnicas de seguridad, las partes implicadas están afectadas por diferentes motivos:

- Operadores de instalaciones: Establecen los requisitos que han de cumplir los proveedores de componentes de seguridad. Éstos deben documentar el potencial de riesgo remanente.
- Constructores de instalaciones: Deben dimensionar adecuadamente la instalación.
- Proveedores: Confirman la clasificación de sus productos.
- Aseguradoras, autoridades: Exigen la demostración de que se ha realizado una reducción suficiente del riesgo remanente de la instalación.

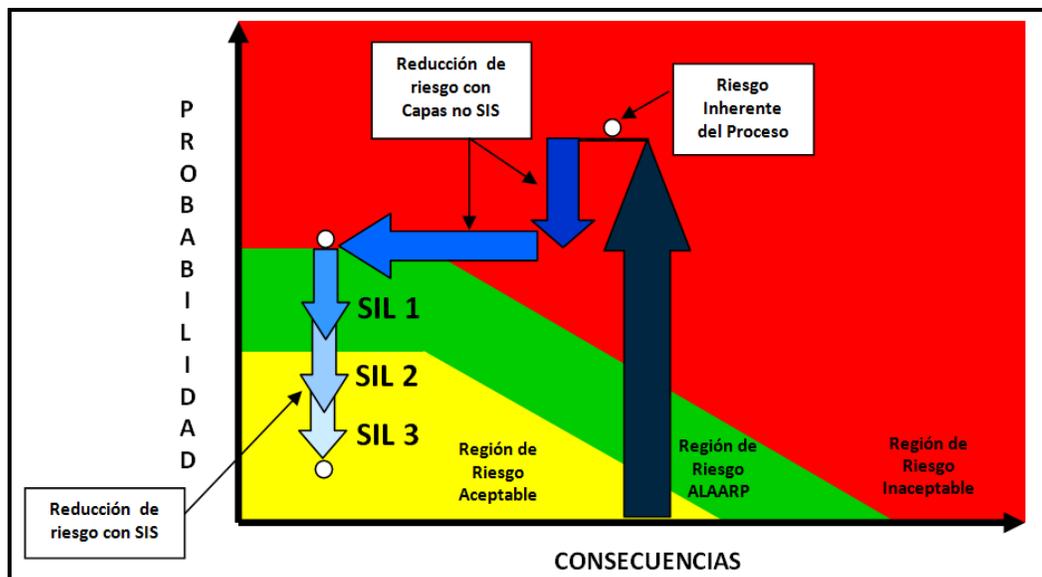


Figura 2.12. Efecto del SIL en la reducción de riesgos de proceso ⁽¹¹⁾

Las normas IEC 61508 y IEC 61511 definen cuatro niveles generales de integridad de seguridad con base al modo de operación del SIS.

2.11. Modos de operación del SIS

Las normas reconocen que los sistemas instrumentados de seguridad (SIS) pueden ser requeridos para operar de maneras muy diferentes. En particular, reconocen que muchas funciones son sólo requeridas con baja frecuencia, es decir, tienen una baja demanda. Por otro lado hay funciones que son de uso frecuente o continuo, es decir, de alta demanda.

La pregunta fundamental es ¿Con qué frecuencia conducirán a accidentes las fallas de cualquier tipo de función? La respuesta es diferente para los dos tipos.

2.11.1. Modo de demanda

Para las funciones con un bajo nivel de exigencia, la tasa de accidentes es una combinación de dos parámetros, la frecuencia de las demandas, y la probabilidad de falla en demanda (PFD) de la función. En este caso, la medida adecuada del desempeño de la función es la probabilidad de falla en demanda (PFD), o su factor recíproco, el factor de reducción del riesgo (RRF).

En la industria de procesos se utiliza típicamente el modo de baja demanda (on demand) y de los cuatro niveles SIL que marca la norma IEC-61511 solo se usan tres, el cuatro está asignado a la industria nuclear. Un ejemplo típico lo constituyen los sistemas de paro de emergencia (ESD) que sólo se activan cuando el proceso pasa a estar fuera de control. Normalmente, esto sucede menos de una vez al año. Por eso las consideraciones en esta tesis se refieren exclusivamente a este modo de operación.

Tabla 2.1. Niveles SIL para operación en modo demanda ⁽⁷⁾		
SIL	Probabilidad de falla en demanda promedio (PFD _{AVG})	Factor de reducción de riesgo (RRF)
3	$\geq 10^{-4}$ a $< 10^{-3}$	> 1000 a ≤ 10000
2	$\geq 10^{-3}$ a $< 10^{-2}$	> 100 a ≤ 1000
1	$\geq 10^{-2}$ a $< 10^{-1}$	> 10 a ≤ 100

2.11.2. Modo continuo

Para las funciones que tienen una tasa de alta demanda o que funcionan de manera continua, la frecuencia de fallas peligrosas por hora es la medida apropiada de rendimiento.

En manufactura se emplea en la mayoría de los casos el modo de alta demanda o demanda continua. Aquí es necesario a menudo un monitoreo continuo de los procesos de trabajo para poder garantizar la seguridad de las personas y del medio ambiente.

Tabla 2.2. Niveles SIL para operación en modo continuo ⁽⁷⁾	
SIL	Frecuencia de falla peligrosa (por hora)
3	$\geq 10^{-8}$ a $< 10^{-7}$
2	$\geq 10^{-7}$ a $< 10^{-6}$
1	$\geq 10^{-6}$ a $< 10^{-5}$

2.12. Métodos de cálculo del SIL

El ejercicio de determinación del SIL se produce durante las fases uno y dos del ciclo de vida de seguridad del SIS mostrado en la norma IEC 61511. En esta misma norma y en la IEC 61508 se indican diferentes métodos para calcular el índice SIL, unos cualitativos y otros cuantitativos.



Las técnicas cualitativas son fáciles y rápidas de aplicar, pero la experiencia ha demostrado que a menudo proporcionan respuestas con altos requisitos SIL. Esto se traduce en un sobrediseño de las funciones de seguridad, que trae como consecuencia gastos potencialmente innecesarios.

Las técnicas cuantitativas requieren un mayor esfuerzo en su desarrollo y uso, pero la experiencia ha demostrado que proporcionan a menudo menores requerimientos de SIL. La diferencia entre el costo de una sola función SIL 2 en comparación con un SIL 1 puede ser de decenas de miles de dólares. La diferencia entre SIL 2 y SIL 3 es aún mayor. Por lo tanto, puede haber ahorros significativos en los costos asociados con la utilización de las técnicas cuantitativas más detalladas.

Y es que, al menos dos estudios recientes, uno por una compañía de petróleo en todo el mundo, otro por una importante asociación, encontraron que una parte significativa de las funciones instrumentadas de seguridad (SIF) están sobrediseñadas (37-49%), así como bajodiseñadas (4-6%). De aquí la importancia por seleccionar un buen método para determinar el SIL. Ahora bien, la determinación del SIL también puede ayudar a saber si un SIS, o SIF especificados, son realmente necesarios. ⁽¹⁾

Por otra parte, la norma IEC 61508 sugiere que las personas o departamentos de las compañías que diseñan, implementan u operan equipamiento en el ámbito de la seguridad funcional, recurran a una organización independiente para realizar las evaluaciones de seguridad funcional.

A medida que aumenta el nivel de riesgo de una instalación o proceso industrial, más aconsejable es realizar la evaluación con un Organismo Independiente.

2.12.1. Método por matriz de riesgos

La matriz de riesgo se encuentra en muchas normas, métodos recomendados y procedimientos internos de las compañías, es uno de los más populares ya que es muy fácil de utilizar. Consiste en categorizar la frecuencia y severidad de un evento peligroso mediante varios niveles cualitativos.

La evaluación de la frecuencia

La frecuencia o probabilidad de un evento puede ser clasificado de bajo a alto, improbable a frecuente, o cualquier término que pueda ser apropiado. Esto puede ser para un solo elemento, o para un grupo de elementos, una unidad de proceso individual, o una planta entera. Los niveles se pueden clasificar tanto cualitativamente como cuantitativamente, como se muestra en la **tabla 2.3**. Si los valores cuantitativos se eligen, se sugiere que se diferencian por lo menos en un orden de magnitud, dado que los niveles de integridad de seguridad difieren por órdenes de magnitud individuales. ⁽¹⁾

Tabla 2.3. Frecuencia del riesgo (solo ejemplo)			
Nivel	Palabra Descriptiva	Frecuencia Cualitativa	Frecuencia Cuantitativa (Por año)
5	Frecuente	Una falla que se puede esperar razonablemente que se produzca más de una vez dentro de la vida útil de la planta.	$Freq > 1/10$
4	Probable	Una falla que se puede esperar razonablemente que se produzca durante la vida útil de la planta.	$1/100 < Freq < 1/10$
3	Ocasional	Una falla con una baja probabilidad de que ocurra dentro de la vida útil de la planta.	$1/1,000 < Freq < 1/100$
2	Lejano	Una serie de fallas, con una baja probabilidad de que ocurra dentro de la vida útil de la planta.	$1/10,000 < Freq < 1/1,000$
1	Improbable	Una serie de fallas, con una muy baja probabilidad de que ocurra dentro de la vida útil de la planta.	$Freq < 1/10,000$

La evaluación de la gravedad

La gravedad también puede ser categorizada de acuerdo a los diferentes factores de riesgo, las personas, los bienes capitales, el medio ambiente, la producción, etc. Los números que aparecen en las **tablas 2.3** y **2.4** son sólo ejemplos y no pretenden representar o implicar cualquier tipo de recomendación. Los valores monetarios se muestran en la **tabla 2.4** también son sólo ejemplos y deben ser calibrados para cada organización. Por ejemplo, lo que puede ser una pérdida catastrófica financiera a una organización puede ser una pérdida relativamente pequeña para otra. ⁽¹⁾

Tabla 2.4. Gravedad del riesgo (solo ejemplo)

Nivel	Palabra Descriptiva	Gravedad Potencial/Consecuencias		
		Personas	Medio Ambiente	Producción/Equipo
V	Catastrófico	Múltiples muertes	Liberación perjudicial fuera del sitio	Pérdida > 1.5M USD
IV	Severo	Una sola muerte	Liberación perjudicial dentro del sitio	Pérdida entre 1.5M y 500K USD
III	Grave	Accidente con tiempo perdido	En el sitio de la liberación: No inmediatamente contenida	Pérdida entre 500K USD y 100K USD
II	Menor	Tratamiento Médico	En el sitio de la liberación: inmediatamente contenida	Pérdida entre 100K y 2500 USD
I	Despreciable	Primeros Auxilios	Sin liberación perjudicial.	Pérdida < 2500 USD

Valoración del riesgo global

Los dos conjuntos de números a continuación, se pueden combinar en un gráfico XY tal como se muestra en la **tabla 2.5**. La esquina inferior izquierda representa un bajo riesgo (es decir, de baja probabilidad y baja frecuencia), la esquina superior derecha representa un alto riesgo (es decir, de alta probabilidad y alta frecuencia). Para esto se ha de tener en cuenta, que la definición de las fronteras entre las categorías es bastante subjetiva. También se pueden usar más de tres categorías generales. ⁽¹⁾

Tabla 2.5. Riesgo total (solo ejemplo)

		Frecuencia				
		1	2	3	4	5
Gravedad	V	1-V	2-V	3-V	4-V	5-V
	IV	1-IV	2-IV	3-IV	4-IV	5-IV
	III	1-III	2-III	3-III	4-III	5-III
	II	1-II	2-II	3-II	4-II	5-II
	I	1-I	2-I	3-1	4-I	5-I

El problema con las matrices de riesgo es que la selección del SIL Objetivo está basada en términos de una evaluación cualitativa. Algunas empresas han calibrado sus matrices de acuerdo a su experiencia y tipo de aplicación y pueden proveer una guía rápida en la evaluación del nivel SIL objetivo, sin embargo dejar a criterio de personas la selección del SIL objetivo podría no ser una buena idea ya que pueden perderse de vista factores externos o experiencias externas en procesos similares que puedan representar un potencial problema de presentarse combinaciones de eventos no previstas por el analista.

2.12.2. Matriz de capas de seguridad

La matriz de capas de seguridad es una matriz de seguridad a la cual se le adiciona un tercer eje (Z) para tener en cuenta las capas adicionales de seguridad. Esto se refiere a las capas externas del sistema instrumentado de seguridad y se muestra en el diagrama de cebolla (ver figura 2.3).⁽¹⁾

A modo de ejemplo, supongamos que el evento peligroso en cuestión es una condición de sobrepresión que resulta en una explosión de un recipiente. Si el área opera con normalidad, puede haber múltiples víctimas mortales. Esto podría dar lugar a la más alta calificación de gravedad. Los registros históricos de explosiones de recipientes podrían indicar una frecuencia muy baja, de nuevo se recalca que, esto no es más que un ejemplo hipotético. Si no hay capas de seguridad adicionales más allá del sistema de seguridad instrumentado, el eje Z no puede ser utilizado. Esto daría como resultado un requisito SIL 3 como se muestra en la figura 2.13. Sin embargo, si hay capas adicionales, tales como una válvula de alivio, se podría utilizar el eje Z y bajar los requisitos de diseño del sistema de seguridad estudiado, de SIL 3 a SIL 2.⁽¹⁾

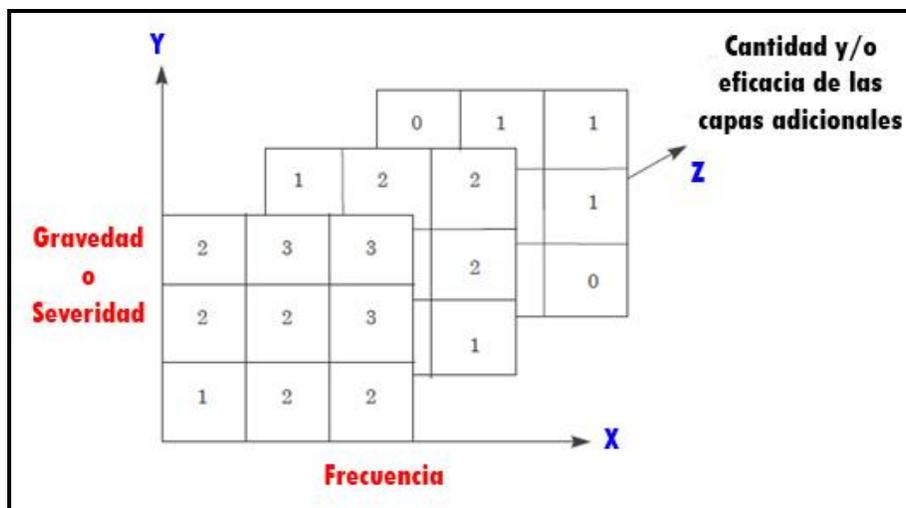


Figura 2.13. Matriz de riesgo tridimensional para seleccionar el SIL

2.12.3. Gráfica de riesgo

El método de gráficos de riesgo fue desarrollado con la publicación de la norma Alemana DIN 19250 en 1994, y es un método muy popular en la determinación del nivel de SIL objetivo.



Este método cualitativo se basa en categorías. Las categorías utilizadas son las consecuencias y frecuencias de un evento peligroso, pero también la probabilidad de que una persona se encuentre en el área afectada y la posibilidad de que esta pueda evadir el peligro. Se muestra en la **figura 2.14** la representación de un gráfico de riesgos. Los términos utilizados en la figura son intencionalmente vagos y abiertos a la interpretación, únicamente para ejemplificar. ⁽¹⁾

La **figura 2.14** fue pensada para un riesgo al personal, pero se pueden desarrollar gráficos similares para los riesgos asociados con el equipo, las pérdidas de producción, impacto ambiental, etc. Estos parámetros de riesgo pueden ser tomados de la norma IEC 61511. ⁽¹⁾

El parámetro de consecuencias (C) describe el resultado probable del evento peligroso, y está compuesto por cuatro categorías, Ca es el valor menos severo y el rango de afectación está dado por la lesión de una persona, Cb representa lesiones serias para una o varias personas, incluso con una muerte, Cc representa muerte de varias personas y Cd fatalidad de múltiples personas.

El parámetro de tiempo de exposición (F) nos indica la fracción de tiempo que la persona expuesta al peligro se encuentra en el área del evento, Fb indica un riesgo mayor que Fa y generalmente se selecciona Fa cuando el tiempo de ocupación es aproximadamente de 10% o menor.

La posibilidad de que el personal evite el peligro es incorporado en el parámetro (P). Este refleja la logística y los métodos implementados para que el personal pueda escapar del área peligrosa, Pb representa un riesgo mayor que Pa.

El parámetro final es la relación de demandas (W), la cual es la frecuencia por año en que se presenta la consecuencia no deseada sin la función instrumentada de seguridad (SIF). W1 indica una frecuencia baja, menor a W2 que indica una frecuencia media menor a W3 que significa una frecuencia relativamente alta ($W1 < W2 < W3$).

A simple vista se puede ver que todo esto es muy subjetivo. También se puede cuestionar la calibración de la **figura 2.14**. Cada organización debe definir los límites o clasificaciones con

mayor precisión. Las normas simplemente tratan de mostrar la metodología, no un ejemplo de trabajo que pueda ser mal utilizado.

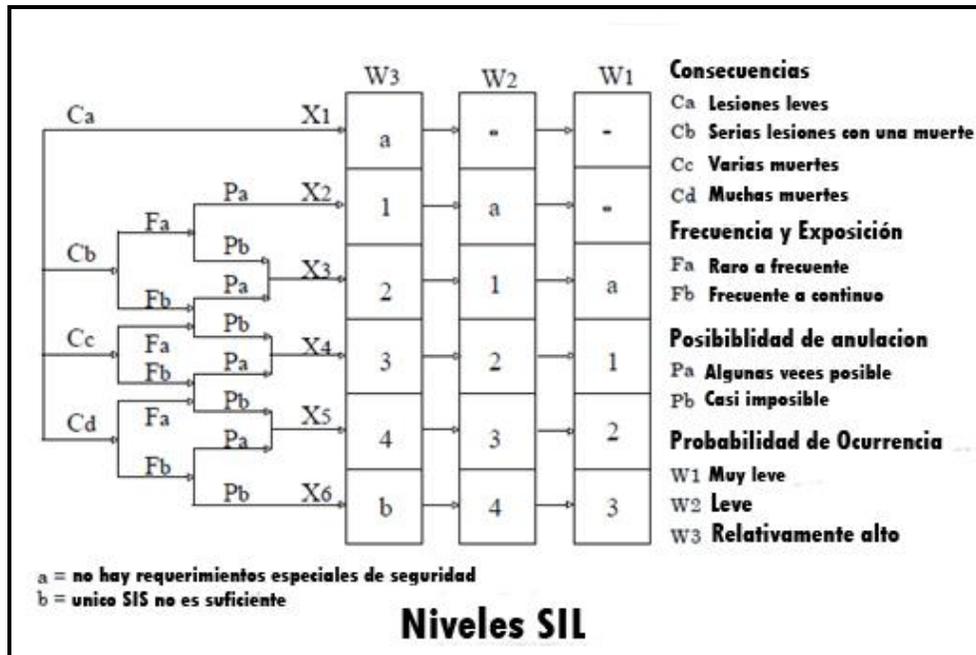


Figura 2.14. Gráfico de riesgo⁽¹⁾

2.12.4. Método LOPA

Debido a que los métodos anteriores son cualitativos, muchos ingenieros no se sienten convencidos debido a que la repetibilidad de los resultados es muy cuestionable. Por ello, la metodología de LOPA (Layer of Protection Analysis) fue introducida a principios de los años 90's, y ha ganado popularidad en los últimos años como técnica semi-cuantitativa para la determinación del SIL. LOPA obtiene la información del análisis de peligros y operación (HAZOP)⁽¹⁾

El método de LOPA tiene como principales características:

- Utiliza como punto de partida el establecimiento del criterio de riesgo tolerable, puede utilizarse el riesgo individual, social o corporativo.
- La frecuencia del evento iniciador, este valor puede ser tomado de tablas o valores publicados en bases de datos, de valores corporativos o bien de análisis y simulaciones por medio de arboles de fallas o diagramas de bloques de confiabilidad.



- Calcula la frecuencia de las consecuencias no mitigadas y de las consecuencias mitigadas.
- Considera eventos o condiciones que permiten que un evento iniciador se propague, este término es particularmente importante en procesos por lotes (batch) o procesos que requieren interacción con el operador.
- Utiliza modificadores condicionales, que son circunstancias o eventos que pueden suceder a la par del evento iniciador y que pueden amplificar, modificar o exponenciar el evento iniciador.
- Considera todas las capas independientes de protecciones existentes y potencialmente existentes para determinar cuando el criterio de riesgo se cumple utilizando los valores de probabilidad de falla en demanda (PFD), esto permite de forma fácil evaluar las modificaciones y adiciones requeridas para reducir el riesgo a un valor de riesgo necesario.
- Proporciona información de los requerimientos o modificaciones que hay que realizar en el proceso para cumplir con el criterio de riesgo.

LOPA es cuantitativo por que se basa en: ⁽¹²⁾

- Calcular la frecuencia del evento iniciador.
- Calcular la frecuencia de las consecuencias mitigadas y no mitigadas.
- Calcular la probabilidad de falla en demanda (PFD) de cada capa independiente de protección (IPL).

LOPA es semi-cuantitativo por que se basa: ⁽¹²⁾

- En valores de criterios de riesgo tolerable que pueden ser generados por leyes y normas para estimar el riesgo social, individual o corporativo.
- En poder utilizar valores publicados en tablas o bases de datos para estimar la frecuencia del evento iniciador.

- En poder utilizar valores publicados para estimar los eventos condicionales y modificadores condicionales.

LOPA es cualitativo por que se basa en: ⁽¹²⁾

- Criterios basados en experiencia para seleccionar las capas de protección necesarias y más eficientes.
- Criterios para asignar eventos condicionales y modificadores condicionales.
- Criterios para seleccionar el concepto de riesgo tolerable.

Transferir de HAZOP a LOPA.

Normalmente el software comercial proporciona herramientas para transferir los estudios HAZOP a LOPA, como se muestra en la **figura 2.15**.

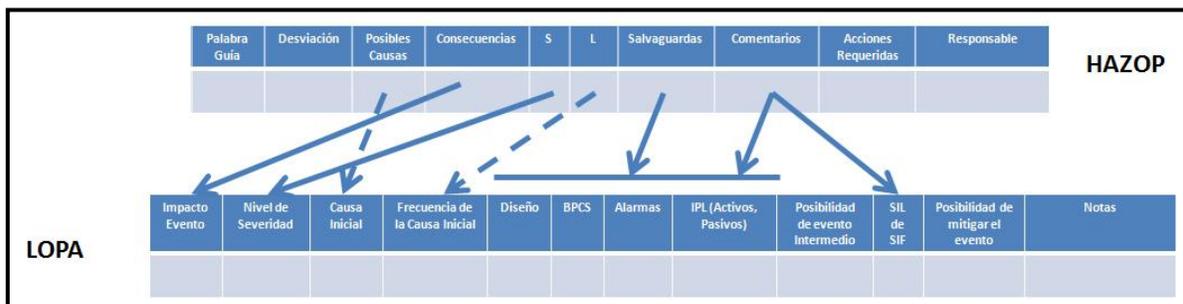


Figura 2.15. Transformación de HAZOP a LOPA ⁽¹²⁾

La metodología de LOPA ha sido interpretada y desarrollada por varios autores y compañías de forma diferente, sin embargo se sigue una metodología común.

El primer paso consiste en determinar un nivel de riesgo tolerable. Algunos gobiernos alrededor del mundo han documentado un número de valores para usar en la industria, para ellos elaboran tablas de probabilidades anuales tolerables de mortalidad, impacto de medio ambiente, pérdida de producción, bienes capitales y de otra índole.

El siguiente paso consiste en determinar las frecuencias de inicio del evento o probabilidades. Estos pueden ser los acontecimientos externos, por ejemplo, un rayo o el incumplimiento de una de las capas como el que una válvula de control falle en posición abierta, lo



que conduciría a un evento peligroso. Los números deben ser determinados para cualquier evento que se trate. Los números se pueden determinar sobre la base de registros históricos o datos de tasa de fracaso (que es una forma de registro histórico).

A continuación, la **figura 2.16** representa el método de cálculo que se sigue para determinar el SIL por este método. La metodología que se empleará en esta tesis es una variante del método LOPA y será descrita en el capítulo 4.

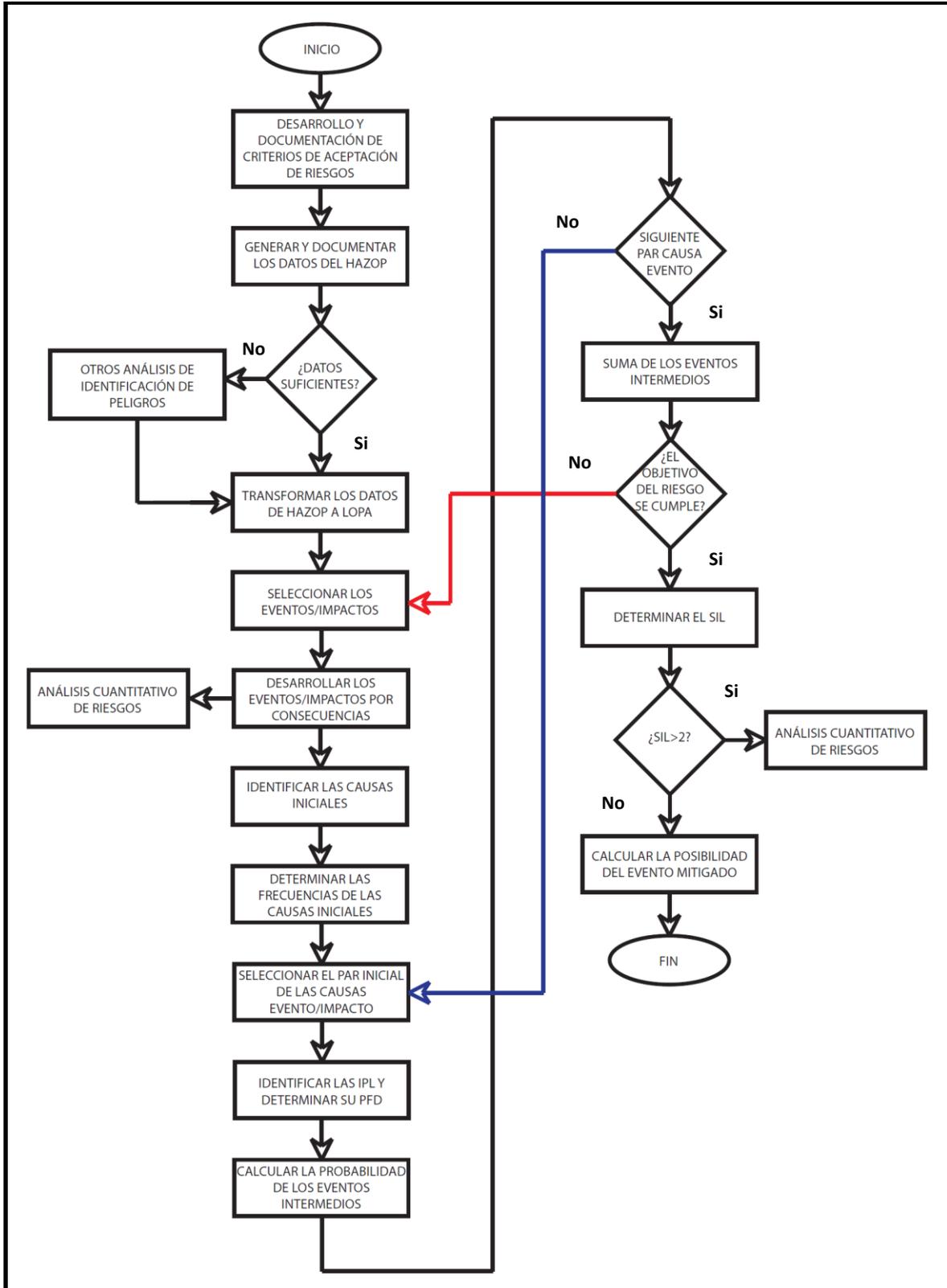


Figura 2.16. Diagrama de flujo de cálculo del SIL usando el método LOPA ⁽¹²⁾

2.13. Redundancia

Si la falla de un único sensor no puede ser tolerada o si un solo sensor no puede cumplir con los requisitos de rendimiento, a continuación, los sensores redundantes o múltiples pueden ser utilizados. La redundancia es el uso de múltiples elementos o sistemas para desempeñar la misma función y es usada para mejorar la confiabilidad y la disponibilidad. ⁽¹⁾

Existe la redundancia diversa como se puede apreciar en la **figura 2.17** para evitar las fallas de causa común que se generan por el uso de dos o más dispositivos iguales en tecnología.



Figura 2.17. Redundancia diversificada

También existe la redundancia diversificada para evitar fallas sistemáticas que se generan por el uso de dispositivos de igual fabricante y que algún error de diseño de este puede estar impreso en todos los demás dispositivos de ese fabricante.

La redundancia por votación que pueda ser requerida depende de una serie de factores (por ejemplo, los requisitos de SIL, la tasa deseada de paros en falso, etc.). La **tabla 2.6** muestra las configuraciones de uso común con los sensores y elementos finales.

Las **figuras 2.18 a 2.20** muestran la configuración típica de los elementos en cada determinado caso de nivel SIL.



Tabla 2.6. Redundancia por votación ⁽¹⁾

SENSORES	
1oo1	1 de 1 (es decir, un solo sensor). Se utiliza si el componente cumple con los requisitos de desempeño.
1oo1D	1 de 1 con diagnósticos. Los diagnósticos pueden ser proporcionados por un monitor de alarma adicional o integrado en el sensor (es decir, un sensor de seguridad certificado).
1oo2	1 de 2. Dos sensores instalados, pero sólo uno es necesaria para la activación del paro de planta. Esta configuración es más segura que 1oo1, pero muchos disparos en falso.
1oo2D	1 de 2 con diagnósticos. Los diagnósticos pueden ser proporcionados por un monitor de alarma adicional o integrado en el sensor. Esta configuración es "tolerante a fallas" y puede sobrevivir a las fallas seguras y peligrosas y continuar funcionando correctamente.
2oo2	2 de 2. Dos sensores instalados y ambos son necesarios para la activación del paro de planta. Este esquema es menos seguro que 1oo1, sin embargo, tiene un menor número de disparos en falso.
2oo3	2 de cada 3. Tres sensores instalados y dos son necesarios para la activación del paro de planta. Al igual que con 1oo2D, esta configuración es "tolerante a fallas" y puede sobrevivir a las fallas seguras o fallas peligrosas y continuar funcionando correctamente.
ELEMENTOS FINALES	
1oo1	Una sola válvula. Se utiliza si el dispositivo cumple con los requisitos de rendimiento.
1oo2	1 de 2. Dos válvulas instaladas, pero sólo una es necesaria para el paro de emergencia. Al igual que con los sensores, este sistema es más seguro que el 1oo1, pero es susceptible a muchos disparos en falso.
2oo2	2 de 2. Dos válvulas instaladas y ambos son necesarios para el paro de emergencia. Al igual que con los sensores, este sistema es menos seguro que el 1oo1, sin embargo, tiene un menor número de disparos en falso.

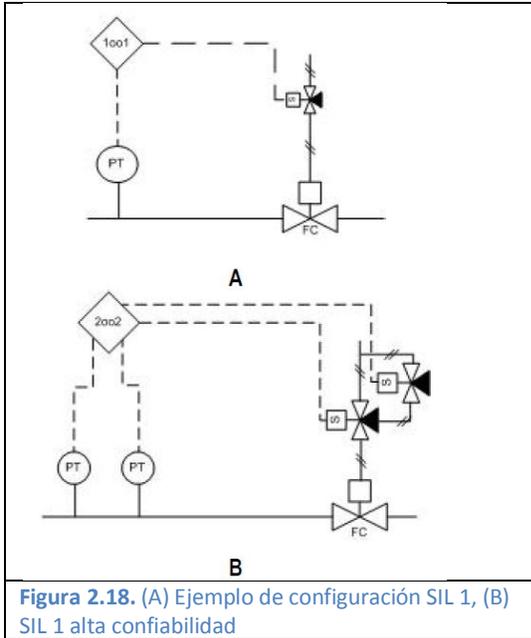


Figura 2.18. (A) Ejemplo de configuración SIL 1, (B) SIL 1 alta confiabilidad

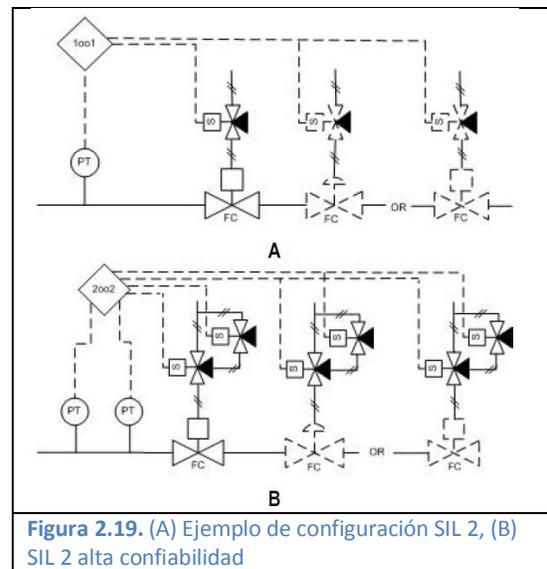


Figura 2.19. (A) Ejemplo de configuración SIL 2, (B) SIL 2 alta confiabilidad

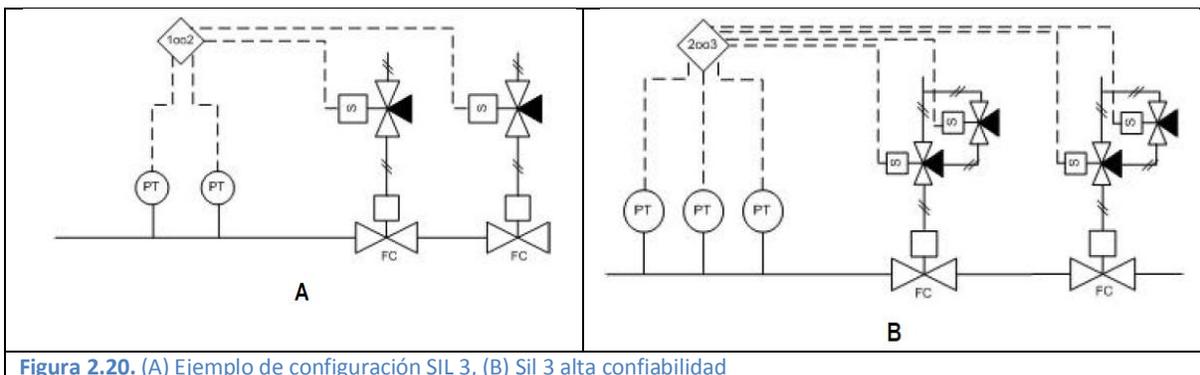


Figura 2.20. (A) Ejemplo de configuración SIL 3, (B) Sil 3 alta confiabilidad

2.14. SIS vs BPCS

Es importante darse cuenta y comprender las diferencias fundamentales entre el control de procesos y el control de seguridad. El sistema de control de proceso está activo o dinámico. Tienen entradas analógicas, salidas analógicas, permite realizar operaciones matemáticas y cálculos numéricos, y tienen lazos de retroalimentación. Por lo tanto, la mayoría de las fallas en los sistemas de control se revelan a sí mismas. ⁽¹⁾

Los sistemas de control son lo suficientemente flexible como para permitir los cambios frecuentes. Por ejemplo, los parámetros del proceso como los puntos de calibración (set points), la configuración del PID. Además, una porción del sistema también puede ser colocado en bypass y el proceso puede ser controlado manualmente. Todo esto es normal para los sistemas de control.

Los sistemas de seguridad, sin embargo, son justo lo contrario. Están durmientes, o pasivos. Ellos operan por largos períodos de tiempo sin hacer prácticamente nada y se espera que nunca se les llame a la acción. El sistema de seguridad no debe cambiar durante su operación, además de que algunas funciones no deben estar accesibles al operador precisamente para que esto no ocurra. El sistema de control debe ser totalmente independiente del sistema de seguridad en todos sus elementos tal como lo muestra la **figura 2.21.** ⁽¹⁾

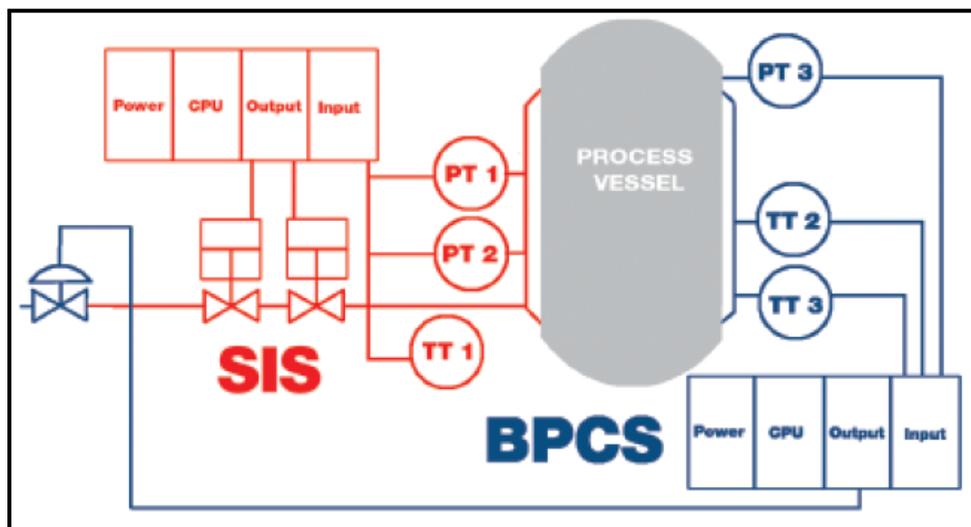
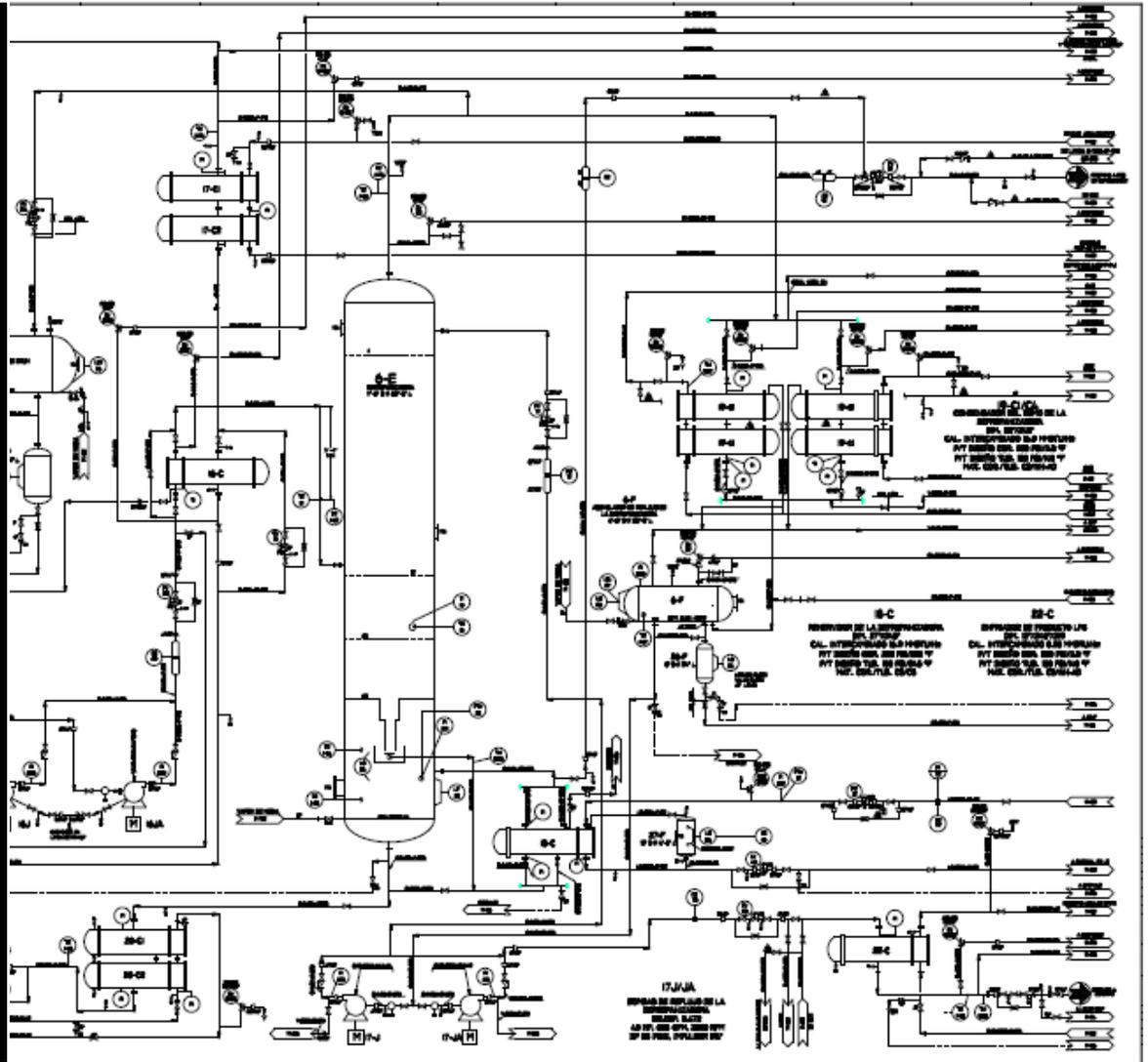


Figura 2.21. Independencia del SIS y el BPCS

CAPÍTULO 3: DESCRIPCIÓN DEL PROCESO DE LA PLANTA BAJO ESTUDIO



3.1. Introducción

Este proceso fue desarrollado e industrializado en la década de 1940 y ha sufrido, a lo largo del tiempo, diferentes modificaciones y mejoras en cuanto a su tecnología y al catalizador empleado, incrementando su eficiencia, los beneficios económicos del proceso y atendiendo las demandas específicas de cada refinería.

3.2. Química del proceso FCC

Al ser un proceso extremadamente complejo desde el punto de vista químico, con múltiples reacciones que ocurren en forma paralela y secuencial, no puede darse una descripción completa y satisfactoria de la totalidad de las reacciones que tienen lugar. La **figura 3.1** muestra algunos ejemplos de las reacciones que se llevan a cabo en el proceso FCC. ⁽¹³⁾

La alimentación empleada en refinerías generalmente es gasóleo de vacío, que comprende diferentes familias de hidrocarburos, siendo los principales componentes hidrocarburos aromáticos o nafténicos de alrededor de 20 a 50 átomos de carbono que equivalen a moléculas con pesos moleculares de más 500 g/gmol. ⁽¹³⁾

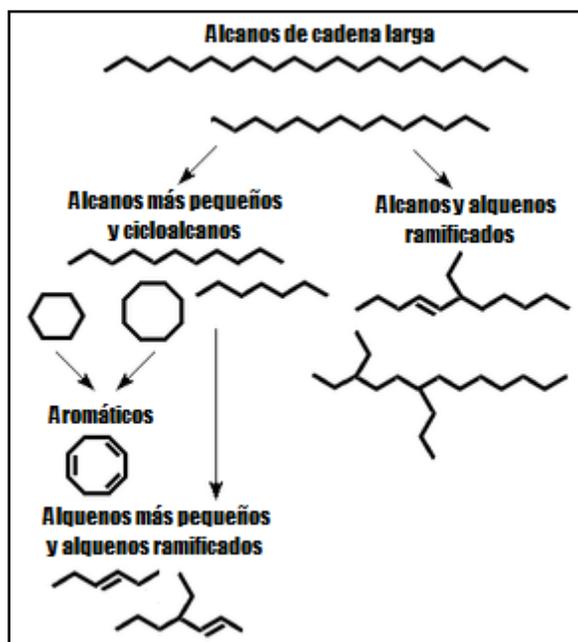


Figura 3.1. Un ejemplo de craqueo catalítico fluidizado de hidrocarburos

Las reacciones se llevan a cabo sobre la superficie de un catalizador del tipo adsorbente que libera los productos craqueados livianos y retiene los productos asfálticos transformándolos en coque. El coque se elimina luego del catalizador en la etapa de regeneración y el catalizador se retorna al proceso. El proceso FCC genera, a partir del craqueo de la alimentación, una gran cantidad de productos con una distribución de pesos moleculares amplia.

3.3. La planta FCC en la refinería

Actualmente, el proceso de craqueo catalítico de hidrocarburos en lecho fluidizado, conocido como FCC (por sus siglas en inglés, fluid catalytic craking), es considerado el más importante dentro de la refinería. Este proceso es el principal productor de naftas de alto número de octano (RON) a partir de corrientes de petróleo pesadas y de bajo valor económico, como el gasóleo pesado de vacío. El proceso genera, además de gasolina, diesel, gas LP y olefinas livianas. Las olefinas pueden ser utilizadas en la planta de alquilación de la refinería y también en la producción de MTBE (metil terbutil éter). De hecho, algunas unidades FCC pueden estar dedicadas a la producción de petroquímicos, como el proceso petro-FCC de UOP.

En la **figura 3.2** se muestra la posición del proceso FCC en una refinería comercial de proporciones considerables y la **tabla 3.1** muestra los productos que genera la planta FCC, su proporción aproximada y su destino dentro de la refinería. ⁽¹³⁾

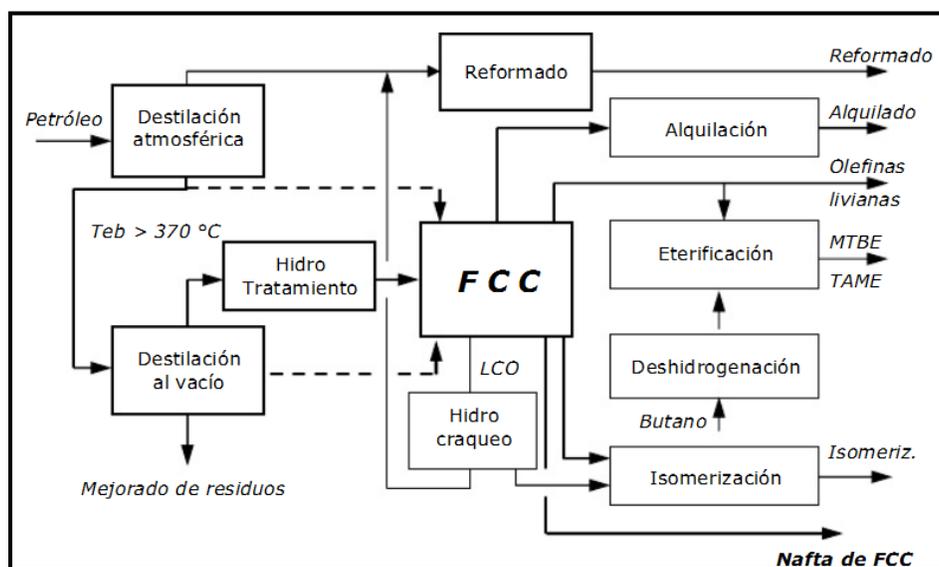


Figura 3.2. El proceso FCC dentro de la refinería



A pesar de la importancia de todos los subproductos que genera la planta FCC mostrados en la **tabla 3.1**, el objetivo principal del proceso de FCC es la generación de combustibles líquidos (gasolina, querosina y diesel). En este sentido, este proceso es central dentro de la refinería, ya que su aporte al total de gasolina producida en la misma es del orden del 40%, contribuyendo directamente a través de la nafta de FCC e, indirectamente, mediante el aporte de materias primas a los procesos de isomerización, alquilación y producción de compuestos oxigenados que también contribuyen al acumulado de gasolina. ⁽¹³⁾

Producto	Característica	Porcentaje	Destino
Gas Seco	Metano-Etano-Etileno	2%	Sistema de gas combustible de la refinería.
Propano	Propano-Propileno	15%	Procesado en petroquímica
Butano	Butano-Buteno	21%	Procesado en Planta MTBE, Planta Alquilación y Planta Isomerización.
Gasolina	RON 90 a 94	41%	Procesada en Plantas HDS
Diesel	Aceite cíclico ligero (Cetano 47)	10%	Procesada en Planta HDD
Gasóleo Pesado	Insaturado	5%	Procesado en Planta FCC
Coque	Insaturado	6%	Se quema en Planta FCC

3.4. Descripción del flujo de la planta catalítica (FCC)

El FCC, es un proceso muy versátil y las unidades comerciales pueden ser operadas en diferentes modos, en función de las necesidades de la planta y las demandas actuales del mercado. Se puede operar el sistema de tres modos principales: para maximizar la producción de gasolina, para maximizar la generación de olefinas livianas, o para la producción únicamente de destilados medios. En esta sección se describirá el proceso para una producción máxima de gasolina, información recopilada por el IMP ⁽¹⁴⁾. Con la ayuda de los DFP's **P-4169-D** y **P-4170-D** que se encuentran en el anexo C se podrá dar seguimiento a la descripción de este proceso.

3.4.1. Sección de carga y reacción

La carga a la planta es una mezcla de gasóleos que se producen en la planta de alto vacío. Estos gasóleos se reciben en el tanque de balance de carga 12-F a control de nivel (LIC-5). Por un



lado, a través de la válvula de control de nivel LV-5B se reciben gasóleos calientes (90° C) provenientes de la planta de alto vacío y por otro lado se recibe carga de tanques de almacenamiento que viene un poco más fría (66° C) y que es impulsada por las bombas 22-J/JA pasando a través de la válvula de control de nivel LV-5A. Para conocer la cantidad de carga proveniente de almacenamiento se tiene el registrador FR-32 y para el total de carga fresca que está entrando al proceso se tiene el FR-33 a la descarga de las bombas de carga.

Del tanque de carga, ésta es bombeada con las bombas 3-J(M) o 3-JA(T) a través de cambiadores de calor y un calentador a fuego directo para proporcionarle la temperatura que requiere al entrar al reactor.

La carga se divide en dos corrientes controladas por las válvulas de control de flujo FV-35 y FV-36, que corresponden a cada uno de los serpentines del calentador a fuego directo 2-B. El calor que se suministra a la carga en el calentador 2-B es proporcionado por gas combustible controlado por el PIC-12 o por diesel controlado con PIC-42. A la salida del calentador 2-B se unen las corrientes de los dos serpentines y se controla la temperatura en este punto con el TIC-14 (350° C) que puede actuar en cascada con el PIC-12 o el PIC-42 según el combustible que se esté utilizando. Se tiene indicación de temperaturas en la consola multipunto para la salida de cada uno de los serpentines TI-1-6 y TI-1-7 y para la corriente total TI-1-8.

De aquí la carga se va hacia el peine de carga pasando por una válvula de compuerta, en donde adelante se le incorpora la recirculación de lodos que manda la bomba 11-J. Ese líquido recirculado es una corriente pequeña, equivalente a un 5% en volumen de la carga, el cual tiene como finalidad retornar el catalizador del asentador de lodos al convertidor, y es una mezcla de lodos de la fraccionadora con algo de aceite cíclico pesado inyectado con la válvula de control de flujo FV-44 para diluir la concentración de catalizador. Toda esta corriente se controla mediante la válvula de control de flujo FV-39.

En la parte inferior del elevador de desintegración (Riser) la carga se mezcla con vapor de dispersión controlado con el FIC-5 y todo esto se alimenta al elevador a través de un juego de seis boquillas localizadas perimetralmente. Se dispone de dos sistemas de inyección de carga (coronas de carga). El superior será utilizado normalmente. El inferior está diseñado para bajas cargas y será usado cuando la carga sea inferior al 80% de la de diseño.



En el Riser la carga se reúne con catalizador regenerado y con los vapores de fluidización lateral y vertical que pasan a través del indicador de flujo FI-27. El catalizador caliente vaporiza la carga, la calienta a la temperatura de reacción y proporciona el calor necesario para la desintegración. La temperatura de salida del Riser es indicada en el TI-1-28 y controlada con el TRC-2 mediante la admisión de catalizador, abriendo o cerrando la válvula tapón PV-2. Esta temperatura deberá ser de 527° C para operación de máxima gasolina.

La mezcla de catalizador y vapores fluye en forma ascendente en el elevador y la reacción se efectúa. Tomando en cuenta que la reacción de desintegración procede con mucha rapidez, el diámetro del elevador aumenta en forma ascendente para manejar el volumen creciente y proporcionar el tiempo de reacción deseado. La mezcla fluye en el tramo vertical restante del elevador, pasa por la línea horizontal de transferencia y finalmente desciende por la bajante vertical hasta la parte inferior de la cámara de separación.

El elevador termina en la parte inferior de la cámara de separación. En este lugar ocurre una separación burda del catalizador y de los vapores, mediante un separador ranurado (separador burdo). La mayor parte de los vapores fluyen horizontalmente por las ventanas laterales del separador, en tanto que la mayor parte del catalizador fluye hacia abajo por el fondo abierto del elevador sumergido en catalizador.

Los vapores de los hidrocarburos formados durante la desintegración, los inertes, el vapor de dispersión y el vapor de agotamiento de catalizador, fluyen hacia arriba en la cámara de separación y salen a través de cuatro juegos de ciclones de dos pasos. El catalizador arrastrado por los vapores es separado de éstos en los ciclones y se retorna al fondo de la cámara de separación, descargándose a través de las válvulas que tienen los ciclones al final de sus piernas. Los vapores fluyen de la cámara de separación hacia la fraccionadora 1-E.

Se tiene un anillo de vapor (FI-100) instalado en el domo de la cámara de separación para evitar la acumulación de vapores de hidrocarburos en esta zona.

El catalizador gastado que contiene el carbón formado durante la reacción de desintegración, pasa hacia abajo a través de un cono dentro del agotador de catalizador gastado. El agotador se localiza directamente debajo de la cámara de separación y cuenta con mamparas



atornilladas tipo disco y dona para asegurar el contacto eficiente del catalizador descendente con el vapor de agotamiento controlado por FIC-4 que fluye hacia arriba. El propósito del agotamiento es el de eliminar los hidrocarburos que han quedado atrapados en el catalizador descendente.

Del agotador, el catalizador fluye en fase densa descendente por un tubo (stand pipe) a través de la válvula tapón PV-1 y cae dentro del pozo de distribución de catalizador agotado. La PV-1 controla el nivel de la cama de catalizador arriba del agotador (nivel del separador LIC-1). Distribuidas a lo largo de la bajante, hay ocho boquillas de aireación con vapor para asegurar un flujo uniforme del catalizador descendente (FI-21 y FI-84).

El catalizador agotado sube a través del pozo y es distribuido por tres brazos (en forma de cornetas) a la primera etapa de regeneración. En el regenerador, el carbón depositado durante la desintegración se quema para eliminarlo del catalizador. Se usan dos etapas de regeneración para alcanzar un contenido muy bajo de carbón en el catalizador regenerado.

En la primera etapa se quema aproximadamente el 80% del carbón. Dependiendo de la operación, se esperan temperaturas de 607 a 641 °C. El aire llega a la primera etapa controlado por el FIC-1 y el MIC-2 a través de un anillo que lo distribuye eficientemente. El catalizador de la primera etapa fluye a través de ranuras en la placa de contención hacia la segunda etapa.

El resto del carbón se quema en la segunda etapa, a temperaturas más elevadas, de 627 a 677 °C, dependiendo de la operación. Se inyecta aire a la segunda etapa con el FIC-3 y el MIC-3 a través de un distribuidor tubular (en forma de araña) que se ha diseñado para proporcionar distribución uniforme de aire y permitir el ajuste a bajos flujos.

El gas efluente de la combustión de carbón atraviesa la fase densa de la cama y asciende a la fase diluida, donde con seis juegos de ciclones de dos pasos, se retorna a la cama el catalizador que arrastraron los gases. Sólo los ciclones secundarios cuentan con válvulas en sus piernas. El efluente de los ciclones fluye a la cámara plena y a la línea de salida. En esta línea dos válvulas deslizantes (SLV Ote y SLV Pte) restringen el paso del gas efluente y controlan la presión del regenerador con el PIC-6. De las válvulas deslizantes el gas fluye a la cámara de orificios en donde la presión se reduce al valor requerido por la caldera de monóxido de carbono.



El soplador de aire 1-J para la combustión del catalizador, es accionado por una turbina de vapor. El calentador de aire 1-B, parte integral de la línea de entrada al anillo de distribución de la primera etapa, se usa durante la puesta en operación de la planta para dar el calor requerido para elevar la temperatura de la cama hasta el punto en que se inicia la combustión del aceite antorcha, después de lo cual el quemado del aceite antorcha eleva la temperatura de la cama a su valor normal.

Para mantener un grado razonable de fluidización de la cama y evitar un flujo inverso del catalizador hacia los anillos de aire y las líneas, en caso de falla del soplador de aire, se dispone de vapor de emergencia para cada anillo de aire (MIC-8 y MIC-9). Para mantener la circulación de catalizador durante los arranques o en las fallas de carga, se cuenta asimismo con vapor de emergencia al riser (MIC-6).

3.4.2. Sección de fraccionamiento

Los vapores que salen del convertidor, son una mezcla de hidrocarburos producto de la reacción de desintegración catalítica, vapor de agua e inertes. Entran por el fondo de la fraccionadora 1-E y fluyen a través de cinco mamparas y un plato de lavado (plato 15). La corriente de circulación de fondos entra a la torre en flujo descendente sobre las mamparas enfriando los vapores para condensar la producción neta de aceite decantado y la recirculación de fondos.

Estos fondos se extraen con las turbo-bombas 9-J/JA. A la descarga se tiene el registrador de flujo FR-41. Una corriente se va hacia los intercambiadores de calor 8-C1/C4 a precalentar la carga fresca; este flujo se controla mediante el FIC-92. Otra corriente se va hacia los intercambiadores 14-C1/C2 para darle temperatura al fondo de la debutanizadora 5-E; este flujo se controla mediante el FIC-67 que actúa en cascada con el TIC-17. Una tercera corriente va a la caldera 2-C donde se enfría generando vapor de media presión (19.5 kg/cm^2); para esta corriente el control es con el PIC-13. De esta manera, los fondos que se extraen calientes (354° C) se retornan a la fraccionadora 1-E un poco más fríos (195° C) y con ello se establece el equilibrio térmico de esta torre.

En el fondo de la torre hay un anillo de vapor (FI-37A) que sirve para prevenir un asentamiento de catalizador y para agotar los hidrocarburos ligeros del residuo. En la base de la



fraccionadora se ha incorporado un asentador de lodos (cónico). El residuo (lodos) del fondo de la fraccionadora escurre al asentador por un tubo sumergido. El catalizador se asienta en el fondo de la sección cónica y de aquí se le extrae como un residuo espeso diluido con ACP inyectado con la válvula de control de flujo FV-44 y es recirculado a la carga de alimentación al reactor utilizando las bombas 11-J/JA a través de la válvula de control de flujo FV-39.

El aceite decantado se extrae de la parte superior del asentador de lodos y se bombea con las bombas 10-J/JA al límite de batería a través de la válvula de control de flujo FV-51, después que precalienta a la carga fresca en el intercambiador de calor 6-C y que se enfría en los solo-aíres 7-C1/C2. Una parte del aceite decantado puede recircularse a la fase líquida arriba del asentador para controlar la gravedad del aceite decantado y la temperatura del asentador. La temperatura del aceite decantado debe mantenerse por arriba de los 50° C que es su punto de congelación (TI-1-43). El sistema del aceite decantado está diseñado para manejar el doble del flujo normal y el sistema de recirculación de lodos para un 50% arriba del flujo normal para agregar flexibilidad.

El plato de lavado (15) que se localiza entre la mampara superior y la cubeta de extracción de ACP sirve para eliminar arrastres de residuo o catalizador provenientes de las mamparas inferiores. El líquido para lavar el plato consiste del retorno de aceite de sellos a las bombas y una parte de la recirculación de aceite cíclico pesado controlada mediante el FIC-43.

La cubeta de extracción del aceite cíclico pesado es una placa cóncava con dos chimeneas rectangulares y está localizada abajo del plato 14 de la torre. Las bombas de aceite cíclico pesado 7-J/JB (M) y 7-JA (T) distribuyen su descarga para aceite de lavado para las bombas, válvulas e instrumentos; el reflujo circulante controlado con el FIC-45 cambia calor con la carga fresca en los intercambiadores de calor 29-C1/C2. Una parte del ACP se usa para dilución de la recirculación de los lodos al convertidor y se controla con FIC-44. Proporciona el aceite de sellos para las bombas de recirculación de fondos y proporciona el aceite de lavado (flushing) para las bombas, instrumentos y válvulas en servicio de residuo. Del circuito de aceite cíclico pesado hay un disparo hacia la válvula de control de flujo FV-6 que se utiliza como aceite antorcha (torch oil) para elevar la temperatura de las camas de catalizador en el regenerador de catalizador.

El aceite cíclico ligero que sale como producto, el aceite de sellos para las bombas y el aceite esponja, se extraen del plato 9 de la torre 1-E. El aceite cíclico ligero y el aceite de sellos se



agotan con vapor (indicado por el FI-47A) en la torre agotadora 2-E y los vapores del domo de ésta se retornan a la fraccionadora arriba del plato de extracción, en tanto que el producto del fondo lo bombean las bombas 5-J/JA/JB (M) a enfriarse a los solo-aíres 4-C1/C2 controlado con el FIC-49, posteriormente sale a límite de batería donde hay un disparo hacia el tanque de carga 12-F que se utiliza en arranques y emergencias para establecer la recirculación larga. El aceite de sellos se toma del producto enfriado para hacerlo circular a través de los sellos de las bombas y tiene una línea para tomarlo de la carga fresca en los arranques y emergencias. El aceite esponja (aceite cíclico ligero sin desflemar) se bombea con las bombas 6-J/JA a la sección de recuperación de vapores, donde absorbe algunos componentes ligeros en el absorbedor secundario 4-E y se enfría un poco. El aceite esponja rico retorna a la fraccionadora principal 1-E, dos platos arriba del de extracción, eliminando algo de calor de la fraccionadora.

Los vapores del domo de la fraccionadora fluyen a los condensadores 1-C1/C8 enfriados por agua y al acumulador 3-F donde se tienen tres fases: una fase gas, una de hidrocarburos líquidos y otra de agua amarga. La corriente de gases va al turbocompresor 2-J en la sección de recuperación de vapores. Los hidrocarburos líquidos (gasolina) se bombean a control de nivel LIC-9 en cascada con FIC-46 al absorbedor 3-E con las bombas 4-J/JA y el agua amarga se bombea también a control de nivel LIC-8 con las 8-J/JA a la sección de tratamiento de aguas amargas.

Parte de los hidrocarburos líquidos se mandan con las bombas 29-J/JA como reflujo al plato 1 de la fraccionadora para controlar la temperatura del domo a través de la válvula de control de flujo FV-42 que actúa en cascada con el controlador de temperatura TIC-15.

3.4.3. Sección de recuperación de vapores

Los vapores del acumulador 3-F de destilado ligero de la fraccionadora van al separador de succión 16-F y de allí al primer paso del compresor centrífugo 2-J movido por una turbina de vapor. Se dispone de dos pasos de compresión para alcanzar la presión de descarga requerida con un mínimo de potencia. Los vapores de la descarga del primer paso del 2-J fluyen hacia los enfriadores de entrepasos 27-C1/C2. Se inyecta agua de lavado (indicada por el FI-64) a la entrada de los enfriadores pasando al acumulador de entrepasos 15-F en donde se separan los vapores condensados. El agua amarga se envía a tratamiento a control de nivel (LC-18). Los hidrocarburos condensados se bombean con las bombas 14 J/JA a control de nivel con el LIC-17 para juntarlos



con la descarga del segundo paso del compresor 2-J. Los vapores del acumulador 15-F se van al separador de succión 17-F, luego se comprimen en el segundo paso de compresión. Se inyecta agua de lavado (indicada con el FI-59) a la corriente de descarga del segundo paso del compresor, con el fin de eliminar sales solubles mediante el lavado. Esta agua se inyecta con las bombas 27-J/JA.

Los vapores del domo del agotador 3-E y la gasolina rica en LPG del absorbedor primario 3-E que pasa por la válvula de control de nivel LV-21, se juntan con los vapores de la descarga del segundo paso del compresor y fluyen a través de los condensadores de alta presión 9-C1/C4 al separador de alta presión 4-F. Esta condensación a alta presión, constituye una etapa de equilibrio con enfriamiento y aumenta la eficiencia de recuperación del sistema absorbedor-agotador.

La recirculación de gasolina desbutanizada previamente sub-enfriada que bombean las 26-J/JA a control de flujo con el FIC-70, sirve como gasolina de absorción y se inyecta al plato uno del absorbedor primario 3-E. La gasolina del agotador 3-F fluye como aceite de absorción al plato cuatro del agotador 3-E a través de la válvula de control de flujo FV-46 y controlando el nivel en cascada con el LIC-9. El absorbedor primario está sentado directamente encima del agotador, con una placa sólida que separa las dos secciones. Este absorbedor recupera la mayor parte del propano y los butanos de los vapores que salen del separador de alta presión 4-F.

El gas residual del absorbedor primario 3-E se alimenta al absorbedor secundario 4-E, en el que se recuperan cantidades adicionales de hidrocarburos ligeros (principalmente propano), incluyendo arrastres de gasolina de absorción controlado por el FIC-50, después de enfriarse por intercambio de calor en los condensadores 11-C1/C2 con el aceite esponja rico se retorna a la fraccionadora a control del nivel con LIC-23, donde los gases absorbidos se desorben.

El gas seco del absorbedor secundario fluye al sistema de gas combustible (TH-1201) a control de presión mediante el PIC-30, después de eliminar ácido sulfhídrico, como se describe en la sección de tratamiento con amina.

Los hidrocarburos líquidos del separador de alta presión 4-F (gasolina rica en LPG) se bombean con las bombas 13 J/JA a control de nivel con el LIC-20 al plato superior del agotador 3-E (plato 25). Esta torre, equipada con el recalentador 10-C, sirve para controlar el contenido de



etano en el producto propano LPG y su flujo de fondos representa el total de líquidos recuperados del sistema incluyendo la gasolina desbutanizada recirculada como aceite de absorción. El recalentador 10-C del agotador se calienta con vapor de media controlado con el PIC-16 que actúa en cascada con el TIC-16 para la temperatura del fondo del agotador 3-E.

La gasolina rica del fondo del agotador 3-E se alimenta a control del nivel del agotador con el LIC-22 en cascada con el FIC-52 a la torre desbutanizadora 5-E después de calentarse contra el líquido del fondo de la desbutanizadora 5-E en el intercambiador de calor 13-C. La torre desbutanizadora 5-E sirve para separarle a la gasolina los propanos, y los butanos que salen por el domo dándole a la vez una estabilización al regularle la presión de vapor con la temperatura del fondo. La debutanizadora se recalienta con la circulación de fondos de la fraccionadora en los intercambiadores 14-C1/C2 controlada por el FIC-67 en cascada con el TIC-17. El reflujo controlado por el FIC-68 y la corriente neta de vapores del domo se condensan totalmente en los condensadores 15-C1/C4 y se acumulan en el acumulador 5-F de donde se bombean a tratamiento (Amina y Merox). Los fondos (gasolina desbutanizada) se enfrían por intercambio de calor contra la carga, primero en el 13-C, precalentando la carga a la despropanizadora; después en el 16-C y finalmente en los enfriadores con agua 17-C1/C2.

La gasolina desbutanizada que sirve como aceite de absorción en el absorbedor primario 3-E se recircula con las bombas 26- J/JA que la succionan a la salida de los intercambiadores 17-C1/C2 antes de mandarla a endulzamiento de Merox. Esta se enfría con una corriente circulante de agua helada del sistema de refrigeración "Chiller" hasta unos 14° C (TI-1-77) en el 28-C.

El producto propano –butano LPG del domo de la 5-E con las 15 J/JA a control de presión con PIC-17 a través de la sección de tratamiento con amina para eliminarle el ácido sulfhídrico y luego pasa a la sección de tratamiento Merox para eliminarle mercaptanos. De la sección Merox, la corriente de LPG va a control de presión con el PIC-18 al tanque de balance 13-F, que se mantiene a una presión constante de 11.3 Kg/cm² con el PIC-19, que es de unos 2 Kg/cm² mayor que la presión a la cual hierve la mezcla a la temperatura que se tiene. Esta condición es necesaria para evitar la vaporización. El control de la presión en el acumulador 13-F se consigue mediante un sistema de rango dividido con el PIC-19, que introduce vapores calientes del domo de la



despropanizadora con la válvula PV-19A ó ventea la presión sobrante al acumulador de entrepasos 15-F con la válvula PV-19B.

La corriente butano-propano del tanque de balance 13-F se bombea con las bombas 16 J/JA controlando el nivel de éste con el FIC-69 en cascada con el LIC-26 a precalentamiento con la gasolina desbutanizada en el precalentador 16-C y se alimenta a la torre despropanizadora 6-E arriba del plato 17. En la despropanizadora se efectúa la separación del propano-propileno por el domo y el butano-butileno por el fondo, de acuerdo a las especificaciones de estos productos. El reflujo al domo controlado con el FIC-71 y el producto neto del domo, se condensan totalmente en los condensadores 19-C1/C4 y se acumulan en el 6-F. Con las bombas 17 J/JA se envía al propano-propileno de reflujo a la torre y la cantidad restante a esferas de almacenamiento a control de presión de la torre con el PIC-20 y a través de un enfriador con agua 22-C. Antes de los condensadores 19-C hay una línea que sirve para enviar propano-propileno a la red de gas combustible (TH-1400) controlado mediante el FIC-91. A través de esta misma salida se puede mandar butano-butileno a gas combustible por un disparo que viene de la salida del recalentador 18-C. Se usa vapor de baja presión como medio de calentamiento al fondo de la despropanizadora en el 18-C controlado por el PIC-21 en cascada con el TIC-19. El butano-butileno producto del fondo, fluye a esferas de almacenamiento a través de dos enfriadores 20-C1/C2 a control del nivel de la torre con el LIC-28.

3.4.4. Sección de tratamiento con amina

En esta sección se les elimina el gas ácido (H_2S y CO_2) a las corrientes de gas residual que viene del absorbedor secundario 4-E y de propano-butano-LPG proveniente del sistema del domo de la debutanizadora 5-E, utilizando una solución acuosa de dietanol-amina (DEA) al 20% en peso.

Para esto, se tiene un contactor gas residual-amina (9-E) para el gas residual y un contactor LPG líquido-amina (7-E) para la corriente de propano-butano. Para regenerar la DEA y poder utilizarla nuevamente, se cuenta con la torre regeneradora de DEA 8-E.



3.4.4.1. Flujo del gas residual

El gas residual que sale por el domo del absorbedor secundario 4-E fluye al separador de arrastre 14-F para eliminar cualquier cantidad de aceite de absorción que pudiera arrastrarse. El líquido arrastrado puede retornarse hacia la fraccionadora.

El gas que sale por el domo del separador 14-F y entra al fondo del contactor 9-E, que es una columna empacada con anillos rasching y en donde la DEA a contracorriente la absorbe el gas ácido a los hidrocarburos ascendentes. Para conocer la caída de presión a través de la torre se tiene un registrador de presión diferencial PDR-53.

El gas endulzado sale por el domo del contactor 9-E a control de presión con PIC-30 que a la vez es el control de la presión de los absorbedores 4-E, 3-E y de la descarga del compresor 2-J en el separador 4-F. De aquí el gas libre de H_2S y CO_2 se envía hacia el tanque TH-2000 y de ahí a la red de gas combustible de la refinería.

3.4.4.2. Flujo de propano-butano LPG.

El LPG que sale del sistema de la desbutanizadora a control de presión a través de la PV-17, entra al fondo del contactor LPG-amina 7-E, que es una columna empacada con anillos rasching en donde se encuentra con un nivel de DEA para absorberle el gas ácido que lleva. Sale por el domo del contactor 7-E y se manda al recipiente 7-F donde los arrastres de DEA se le separan y por la parte superior de este recipiente sale para enviarse a la sección de tratamiento Merox.

3.4.4.3. Circulación de DEA

DEA rica

A control de nivel con el LC-33 sale la DEA rica en gas ácido del contactor 9-E, con el LRC-34 la DEA del contactor 7-E y con LC-36 la DEA arrastrada al separador 7-F y de ahí se van hacia el tanque separador de hidrocarburos 11-F donde la presión se regula a unos 7 Kg/cm^2 con el controlador de rango dividido PIC-31; los hidrocarburos ligeros vaporizan y se van hacia la red de gas combustible.



La DEA rica del separador 11-F se pasa por el filtro 5-L para eliminar cascarilla y otros contaminantes. La corriente filtrada fluye a precalentarse en los 23-C1/C2 contra amina pobre caliente, para entrar a la torre regeneradora 8-E a control de nivel del 11-F con el LC-37.

Torre regeneradora 8-E

En esta torre, se liberará el dióxido de carbono CO_2 y el ácido sulfhídrico H_2S de la amina quedando en condiciones de usarse nuevamente. Para calentar el fondo de esta torre a unos 120°C se tiene los rehervidores 25-C1/C2 y de ahí al acumulador 8-F, en donde se colectan y se bombean con las bombas 19-J/JA al plato superior de la torre como reflujo para recuperar los arrastres formados durante la vaporización instantánea de la solución de DEA rica al entrar en el plato tres.

Los gases que llegan al acumulador 8-F constituyen el gas ácido y a control de presión con el PIC-32 (0.8 Kg/cm^2), salen para mandarse como parte de la carga a la planta de azufre.

DEA pobre

Por el fondo de la torre regeneradora 8-E sale DEA pobre caliente (120°C) y precalienta la carga de la torre (DEA rica) en los intercambiadores 23-C1/C2 y luego se enfría con agua en los enfriadores 124-C1/C2 y llega a la succión de las bombas 18-J/JA. Estas bombas descargan la DEA pobre a control de flujo al contactor 9-E con el FIC-76 y hacia el contactor 7-E con el FIC-77.

3.4.5. Sección de tratamiento de Merox

3.4.5.1. Extracción de mercaptanos al LPG

Flujo de propano-butano LPG

La corriente de propano-butano que sale por la parte superior del separador de amina-LPG 7-F en la sección de amina lleva una cierta cantidad de mercaptanos, que son compuestos de azufre de la fórmula general R-S-H los cuales van a serle removidos en el sistema Merox que aquí se describe.



Primero se hace pasar la corriente de LPG a través del prelavador cáustico 12-E, en donde se mantiene un nivel de sosa cáustica en solución acuosa, con la finalidad de asegurar la completa eliminación de H_2S .

Sale el LPG por arriba del prelavador 12-E y entra por la parte inferior al extractor de mercaptanos 13-E, donde se encuentra a contracorriente con una solución de sosa cáustica con una concentración al 8% aproximadamente que va a reaccionar con los mercaptanos formando mercapturos de sodio dejando de esta forma al LPG más o menos libre de mercaptanos. El LPG libre de mercaptanos sale por la parte superior del extractor 13-E y se va hacia el lavador 14-E entrando por abajo y en donde se va a lavar con agua para eliminar cualquier arrastre de sosa. Una parte del LPG que sale del extractor 13-E se recircula hacia la entrada con la bomba 52-J controlado por el FIC-209.

De la parte superior de lavador 14-E sale el LPG lavado y se envía hacia el tanque de balance de carga a la despropanizadora 13-F a control de presión mediante el PIC-18.

Regeneración de la sosa

La solución de sosa rica en mercaptanos que sale por el fondo del extractor 13-F se calienta en el calentador 50-C con vapor de baja presión hasta unos $45^\circ C$, posteriormente se manda a regenerar en el oxidador 15-E, pasando por la válvula LV-231 que controla el nivel del 46-F.

Se inyecta aire para proporcionar la cantidad necesaria de oxígeno para la regeneración a través de la válvula FV-217. Este aire es proporcionado por los compresores recíprocos 44-J/JA y se acumula en el recipiente 37-F.

Para disolver los disulfuros que se forman durante la regeneración de la sosa, existe una inyección de gasolina dulce proveniente de la salida de gasolina del reactor Merox 11-E a través de la válvula FV-218. Esta gasolina se incorpora a la sosa rica en mercapturos antes de entrar al oxidador 15-E y va a ayudar a hacer la separación de la sosa regenerada de los disulfuros.

Por la parte superior del oxidador 15-E sale una corriente de sosa con gasolina y disulfuros que se van a separar en el separador 46-F controlados por el MIC-223.



La gasolina con disulfuros del separador 46-F es succionada con las bombas 51-J/JA a control de nivel con el LC-228 y se envía a la salida de gasolina dulce del reactor merox 11-E antes de la válvula PV-109.

La sosa regenerada sale por el fondo del oxidador 15-E y del acumulador 46-F se succiona con las bombas 49-J/JA, mismas que la descargan hacia el extractor de mercaptanos 13-E controlada mediante el FC-210 para que vuelva a cumplir con su cometido.

La regeneración de la sosa se lleva a cabo con el oxígeno del aire y en presencia de un catalizador que está disperso en la circulación de sosa. Para adiciones de catalizador se prepara una solución de catalizador con sosa y condensado en el recipiente 45-F y presionando el recipiente con aire se hace fluir hacia la entrada de sosa rica en mercapturos antes del intercambiador 50-C.

El exceso de aire y otros vapores, salen por la parte superior de la chimenea del separador 46-F a control de presión con la válvula PV-230. Se pueden mandar hacia la chimenea del calentador 2-B o hacia el tanque de venteo 47-F de donde salen hacia la atmósfera.

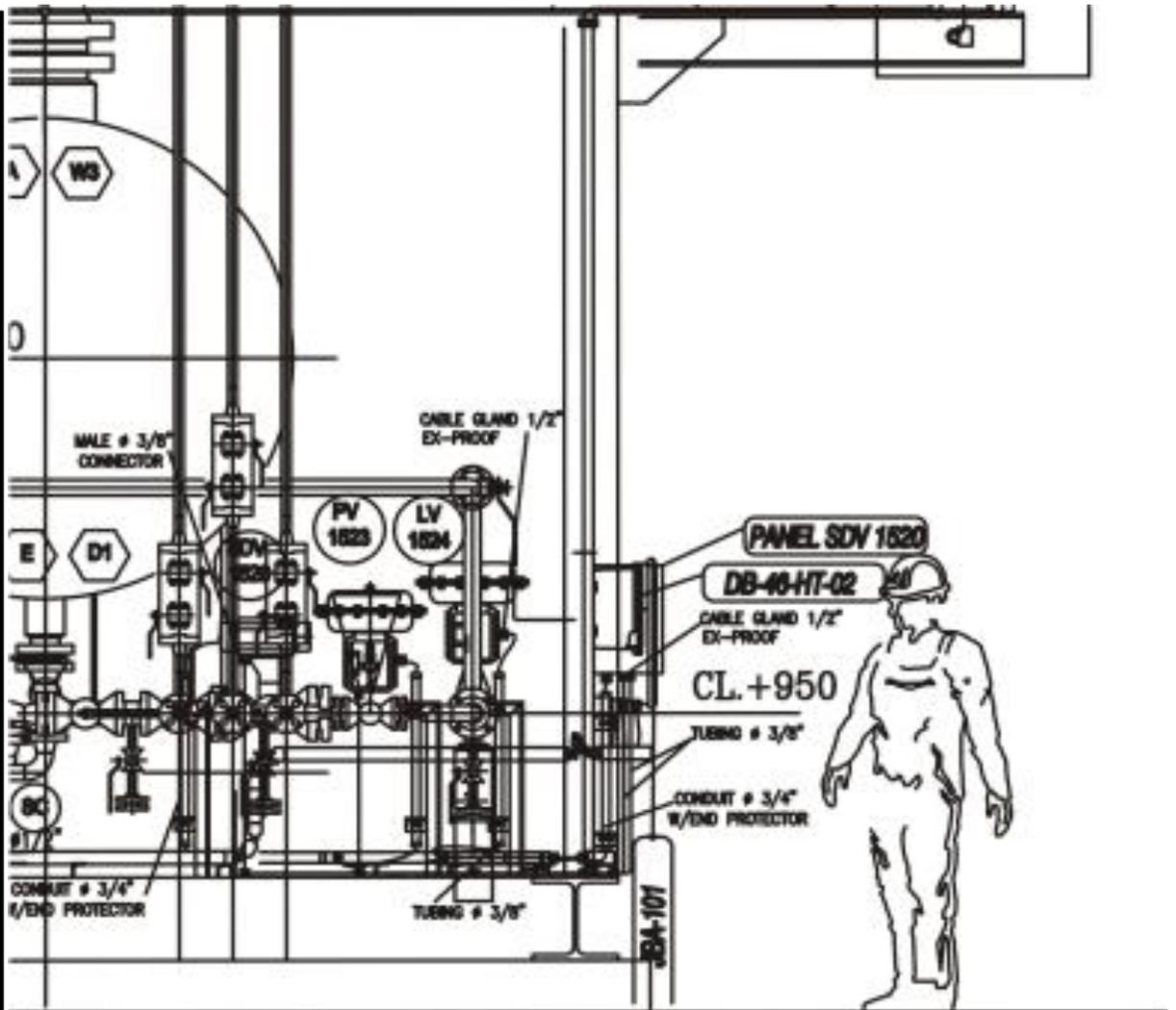
3.4.5.2 Endulzamiento Merox de gasolina

El endulzamiento de la gasolina se lleva a cabo con el reactor de cama sólida 11-E. El reactor merox está empacado con carbón activado y tiene impregnado el catalizador (Merox1) que consiste principalmente en quelatos de hierro y se satura con solución de sosa cáustica.

La gasolina amarga que llega por la válvula FV-103 se mezcla con aire y sosa en el mezclador 22-L y entran al reactor merox, 11-E. La sosa cáustica se introduce con ayuda de las bombas 46-J/JA.

El aire es suministrado por los compresores 44-J/JA y se alimenta través de la válvula FV-102 que actúa de acuerdo al relacionador RS-102 para controlar únicamente la cantidad de aire necesaria para la reacción. La gasolina dulce sale a control de presión del reactor mediante el PC-109. La sosa sale por el fondo del reactor 11-E a control de nivel a través de la válvula LV-107.

CAPÍTULO 4: DETERMINACIÓN DEL NIVEL INTEGRAL DE SEGURIDAD (SIL)





A continuación se detalla una metodología de análisis semicuantitativo para la determinación de los sistemas instrumentados de seguridad (SIS) requeridos y su SIL objetivo asociados y es la que se utilizara en el caso de estudio de esta tesis.

El método fue desarrollado por Cruz-Campa y Cruz-Gómez ⁽¹⁵⁾ en el Departamento de Ingeniería Química de la Facultad de Química en la Universidad Nacional Autónoma de México y publicado en 2010 en el Process Safety Progress de la AIChE.

La metodología como tal está basada en el método LOPA, sin embargo, en el clásico LOPA, los datos de la probabilidad y la frecuencia se utilizan tal como están. En esta metodología, las matemáticas se han simplificado mediante el uso de sólo el orden de magnitud de los datos de frecuencia y probabilidad, así que la multiplicación de las probabilidades y las frecuencias pasan a ser simples adiciones de números enteros.

Además, el LOPA clásico utiliza varios factores que afectan la frecuencia resultante para el evento no deseado: principalmente el factor de uso, la probabilidad de ignición, la probabilidad de explosión, y la ocupación. En esta metodología, el factor de uso, que es la fracción de tiempo en el que el proceso peligroso está en operación o el peligro está presente en el sistema, se supone que es uno, lo que implica un proceso continuo. Además, la ocupación, es decir, la probabilidad de que la zona de efecto de un accidente tenga un impacto en uno o más trabajadores, y las probabilidades de ignición y explosión, ya son tomadas en cuenta a la hora de seleccionar una categoría de la gravedad de las consecuencias.

4.1. Información necesaria para la aplicación de la metodología LOPA

La información que se necesita para la determinación del SIL requerido es la siguiente:

- Estudio de análisis HAZOP de la planta bajo estudio actualizado al momento de la realización del estudio del SIL requerido (los estudios se centrarán en los eventos con riesgo nivel A y nivel B, sin protecciones).
- Diagramas de tubería e instrumentación actualizados de los casos seleccionados.
- Manuales de operación de las plantas de los casos seleccionados.



4.2 Descripción de la metodología

En la teoría del LOPA, los accidentes ocurren cuando se combina un evento iniciador con la falla de las capas de protección del proceso, siendo la frecuencia de dichos accidentes igual a la frecuencia de los eventos iniciales (los cuales presentan demandas a los sistemas de protección) por la probabilidad de que éstos fallen simultáneamente ante estas demandas. Dependiendo de la gravedad de las consecuencias potenciales del accidente se establece un criterio de aceptabilidad de riesgos con base en una frecuencia máxima aceptable.

Al evaluar semi-cuantitativamente la frecuencia de las demandas y la probabilidad de falla bajo demanda de las capas de protección se puede determinar si las protecciones son suficientes de acuerdo a los criterios establecidos. Si las protecciones para un escenario de riesgo no son suficientes se deben evaluar capas de protección adicionales entre las cuales se puede utilizar una Función Instrumentado de Seguridad (SIF), en cuyo caso el método permite determinar fácilmente el SIL requerido.

Los pasos que se siguieron para la determinación del SIL fueron los siguientes:

1. Definición de los criterios de aceptabilidad de riesgos.
2. Identificación de los eventos peligrosos y evaluación de su gravedad.
3. Identificación de los eventos iniciales y evaluación de su frecuencia.
4. Identificación de las capas de protección independientes aplicables y evaluación de su efectividad.
5. Determinación de la efectividad mínima requerida del evento peligroso considerando las capas de protección independientes.
6. Determinación de la necesidad de capas adicionales de protección y determinación del SIL requerido si un SIS es recomendado, comparando la efectividad total de las capas y la efectividad mínima requerida.
7. En caso de requerir un SIS, proponer el diseño conceptual del SIS.

4.2.1 Definición de los criterios de aceptabilidad de riesgos

Es de gran importancia que este paso se realice con cuidado. Los criterios de aceptabilidad de riesgos tienen que responder a las necesidades de la empresa, autoridades y clientes. Los criterios de aceptación deben ser establecidos para los diferentes tipos de consecuencias en las personas, el ambiente y los activos de la empresa.

Para este trabajo, se usaron datos publicados por el AIChE ^{(2) (6) (16)} sobre criterios de aceptabilidad de riesgos como se observa en la **tabla 4.1**. Se usaron estos datos ya que aplican apropiadamente para refinerías y empresas petroquímicas.

Tabla 4.1. Frecuencia límite en la zona de criterio variable para cada categoría de consecuencia		
Gravedad de las consecuencias	Frecuencia límite inferior (eventos/año)	Frecuencia límite superior (eventos/año)
Categoría 5 - Catastróficas	1/100,000,000	1/1,000
Categoría 4 - Mayores	1/10,000,000	1/100
Categoría 3 - Críticas	1/1,000,000	1/10
Categoría 2 - Menores	1/100,000	1
Categoría 1 - Despreciables	1/10,000	10

Con base en esta información se procede a construir un diagrama frecuencia-gravedad para así obtener las tres zonas de los niveles de riesgo como se observa en la **figura 4.1**.

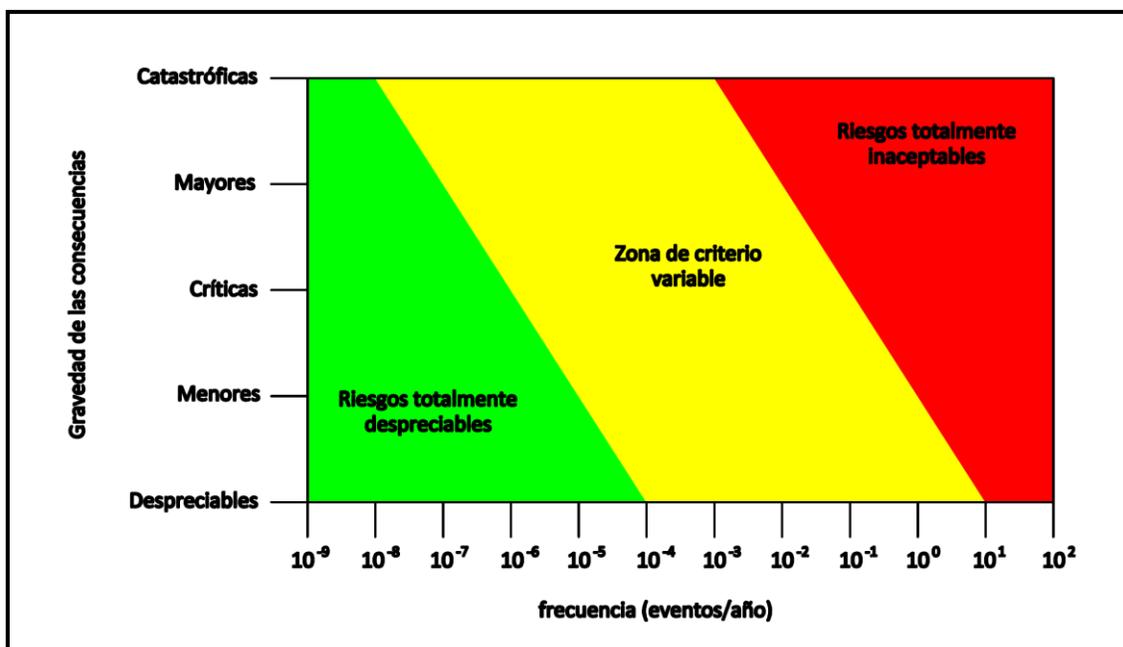


Figura 4.1. Representación de los criterios de aceptabilidad de riesgos en un diagrama frecuencia – gravedad ⁽¹⁵⁾



Para los efectos de este trabajo, el establecimiento de una política de aceptabilidad de riesgos significa la elección de una frecuencia máxima tolerable para cada categoría de gravedad de las consecuencias, entre los dos límites establecidos en la **tabla 4.1**. Por lo tanto se ha elegido el primer criterio para un máximo de frecuencias tolerables, representados la en segunda columna de la **tabla 4.2**.

Tabla 4.2. Criterios de frecuencia meta asociada a cada categoría de gravedad (G) de las consecuencias ⁽¹⁵⁾

Gravedad de las consecuencias	Frecuencia máxima tolerable (criterio utilizado en el análisis) (eventos/año)	Frecuencia (FQ) con protecciones (Frecuencia meta para cada escenario)	$CF_{meta} = \log_{10}(FQ)$
Categoría 1 Catastrófico	1/3,000	1/30,000 (0.1% de probabilidad de ocurrir en la vida útil de una planta)	-4.5
Categoría 2 Mayor	1/300	1/3000 (1% de probabilidad de ocurrir en la vida útil de una planta)	-3.5
Categoría 3 Crítico	1/30	1/300 (10% de probabilidad de ocurrir en la vida útil de una planta)	-2.5
Categoría 4 Menor	1/3	1/30 (Alta probabilidad de por lo menos una ocurrencia en la vida de la planta)	-1.5
Categoría 5 Despreciable	3	1/3	-0.5

Se utilizo este criterio de aceptabilidad de riesgo ya que es el que recomienda AIChE para muchas refinerías y plantas petroquímicas durante su tiempo de vida. Como se muestra en la **figura 4.2**, se ha delimitado perfectamente el criterio de aceptación de riesgos que será usado en este trabajo.

Otras compañías sin duda pueden elegir objetivos de rendimiento más altos utilizando una frecuencia de magnitud menor lo que significaría que la empresa desea el funcionamiento de la instalación de proceso de forma más segura que el promedio, pero se debe ser consciente que esto implicaría grandes costes para reducir el riesgo.

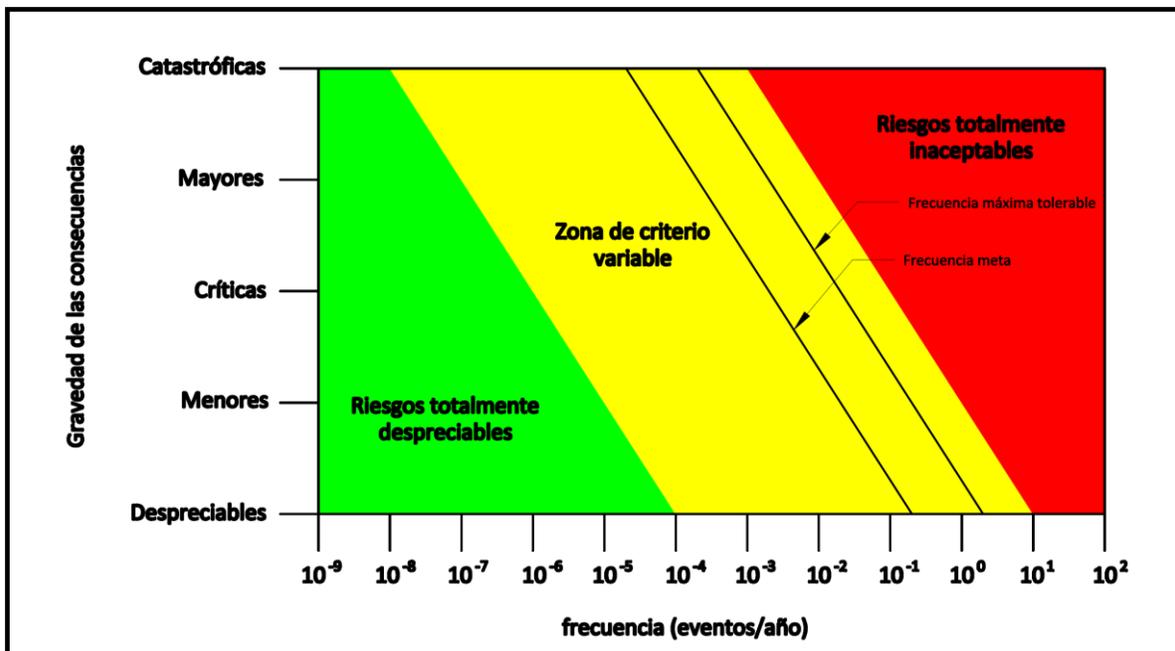


Figura 4.2. Representación de los criterios de aceptación de riesgos para este trabajo

4.2.2 Identificación de los eventos peligrosos y evaluación de su gravedad

La base para la identificación de los eventos peligrosos es el estudio HAZOP que se tenga de la planta bajo estudio; de él se seleccionarán los escenarios de mayor riesgo potencial. El riesgo potencial es el riesgo de un escenario, sin considerar las capas de protección existentes, evaluado cualitativamente mediante una matriz de riesgos; por lo que los escenarios a ser considerados serán los que tengan un nivel de riesgo tipo A y tipo B sin protecciones, de acuerdo a la matriz de riesgos de PEMEX que se muestra en la **figura 4.3**.

Clase		Gravedad			
		1	2	3	4
Frecuencia	1	A	A	B	C
	2	A	B	C	D
	3	B	C	D	D
	4	C	D	D	D

A – Inaceptable –
Mitigarlo hasta tener un riesgo C o menor dentro de un periodo máximo de 6 meses.

B – Indeseable –
Mitigarlo hasta tener un riesgo C o menor dentro de un periodo máximo de 12 meses.

C – Aceptable con controles –
Verificar que los controles estén en uso y sean efectivos.

D – Aceptable como está –
No se requiere mitigar el riesgo.

Figura 4.3. Matriz de riesgos de Pemex refinación utilizada en el análisis



Con la información disponible en las consecuencias señaladas en el estudio HAZOP, se debe categorizar la gravedad de las consecuencias para poder asignar una frecuencia umbral al escenario estudiado. El valor de gravedad será una calificación de frecuencia meta (CF_{meta}) asociada para cuya asignación se utilizará la **tabla 4.2**, donde la última columna nos muestra las CF_{meta} asociadas a los valores de gravedad de las consecuencias.

Los criterios que se utilizarán para calificar de forma adecuada la gravedad de las consecuencias de un escenario de riesgo, dependiendo ya sea del receptor del daño, de las características de la sustancia derramada, del tipo de planta o del costo total del evento se muestran a continuación en las **tablas 4.3, 4.4, 4.5, 4.6**.

La descripción de los efectos potenciales en estas tablas se usa en este trabajo ya que es aplicable a todos los tamaños de empresa, a excepción de los costos estimados implicados. Los importes monetarios utilizados además de las cantidades de sustancias manejadas son apropiados para refinerías, y empresas petroquímicas.

Tabla 4.3. Guía para evaluar la gravedad (G) de las consecuencias en función de la cantidad de sustancia derramada y sus características ⁽¹⁵⁾

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

Las siglas PE se refieren al punto de ebullición de la sustancia toxica



Tabla 4.4. Guía para evaluar la gravedad (G) de las consecuencias en función del receptor ⁽¹⁵⁾		
Gravedad	Receptor	Descripción de los efectos potenciales
Categoría 5 Catastrófico	Personal	Muerte o lesiones que producen discapacidad permanente.
	Comunidad	Uno o más heridos graves.
	Medio ambiente	Descargas significativas con impacto severo hacia el exterior de las instalaciones y con probabilidades de causar efectos a la salud inmediatos o de largo plazo.
	Producción	Destrucción mayor o total de una o varias áreas de proceso con un costo estimado mayor a 10 millones de dólares o pérdidas significativas de producción.
Categoría 4 Mayor	Personal	Uno o más heridos graves.
	Comunidad	Uno o más heridos leves.
	Medio ambiente	Descargas significativas con impacto severo al medio ambiente
	Producción	Daño mayor a una o varias áreas de proceso con un costo estimado mayor a 1 millón de dólares o algo de pérdida de producción.
Categoría 3 Crítico	Personal	Lesiones leves con posible suspensión de labores.
	Comunidad	Quejas de la población cercana por olores o ruido.
	Medio ambiente	Notificación de o a las autoridades ambientales o violación de permisos como resultado de emisiones.
	Producción	Varios equipos dañados con un costo estimado mayor a 100,000 dólares y con pérdidas mínimas de producción.
Categoría 2 Menor	Personal	Lesiones leves sin suspensión de labores.
	Comunidad	Sin daños, peligros o molestias en la población.
	Medio ambiente	Evento intrascendente, sin notificaciones o violación de permisos.
	Producción	Daños menores a algún equipo, con un costo menor de 100,000 dólares y sin pérdida de producción.
Categoría 1 Despreciable	Personal	Sin lesiones o suspensión de labores
	Comunidad	Sin daños, peligros o molestias a la población
	Medio ambiente	Evento intrascendente, sin notificaciones o violación de permisos
	Producción	Daños menores a algún equipo, con un costo menor de 10,000 dólares y sin pérdida de producción

Tabla 4.5. Guía para evaluar la gravedad (G) de las consecuencias en función del costo del evento ⁽¹⁵⁾					
Costo total del evento	0 a 10,000 USD	10,000 a 100,000 USD	100,000 a 1,000,000 USD	1 a 10 millones de USD	Más de 10 millones de USD
Categoría de las consecuencias	Despreciable Categoría 1	Menor Categoría 2	Crítico Categoría 3	Mayor Categoría 4	Catastrófico Categoría 5



Tabla 4.6. Guía para evaluar la gravedad (G) de las consecuencias en función de la afectación a la producción y a las instalaciones ⁽¹⁵⁾

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

Un aspecto importante que se lleva a cabo en este paso es la selección de los escenarios de riesgo del HazOp realizado a la planta. Para ellos se siguieron los siguientes criterios en el orden que se muestran a continuación:

- En una primera etapa de selección, de los escenarios totales del análisis HAZOP, se tomarán solamente aquellos que tengan un nivel de riesgo tipo A y B, de acuerdo a la clasificación del nivel de riesgo usado en los análisis HAZOP.
- En una segunda etapa de selección, de los escenarios obtenidos de la etapa anterior, se eliminarán aquellos donde no hay una relación directa con las capas de protección independientes tomadas en cuenta para la realización de este estudio.
- En una tercera etapa de selección, de los escenarios resultantes de la etapa anterior se procede se toman aquellos que tuvieran las mismas protecciones y se escogerían solo los que tuvieran mayor nivel de riesgo de acuerdo a la lista jerárquica de recomendaciones generada por el HAZOP. Este criterio se aplicó independientemente de que variaran la causa y/o la desviación del escenario analizado.

4.2.3 Identificación de los eventos iniciales y evaluación de su frecuencia

Los eventos iniciales están señalados en las causas de un escenario de un análisis HAZOP. La determinación de la frecuencia para el estudio del SIL requerido se puede hacer a partir de la frecuencia cualitativa, sin considerar protecciones, utilizada en la matriz de evaluación de riesgos



de PEMEX Refinación. Este dato se debe cotejar con los rangos presentados en la literatura concerniente para validarlo. Una buena fuente de información son datos de confiabilidad de equipos de proceso publicados por la AIChE. Lo recomendable es que los datos que se tomen para calificar la frecuencia de los eventos iniciales sean generados por la propia Refinería para tener una mayor certeza en la obtención de resultados de los estudios del SIL.

El valor de frecuencia será una calificación de frecuencia (CF) de los eventos iniciales asociada para cuya asignación se utilizará la **tabla 4.7**, donde la primera columna nos muestra los CF asociados a los valores de frecuencia.

Tabla 4.7. Calificación de frecuencia (F) para los eventos iniciales ⁽¹⁵⁾

CF = log ₁₀ (F)	Equivalencia en frecuencia (F) con la matriz de riesgos de PEMEX Refinación.	Orden de magnitud Frecuencia o Posibilidad.	Descripción cualitativa.
+1		Una vez por mes	Ocurre frecuente o regularmente
0	1	Una vez por año	Probable que ocurra ocasionalmente/varias veces durante la vida de la planta
-1	2	10% de probabilidad en un año	Probablemente sucederá más de una vez en la vida de la planta
-2	3	1% de probabilidad en un año	No se espera que ocurra, pero podría ocurrir durante la vida de la
-3	4	1 en 1000 de probabilidad en un año	Sería una sorpresa que ocurriera durante la vida de la planta
-4		1 en 10,000 de probabilidad en un año	Extremadamente remota, no se espera que sea posible

4.3.4 Identificación de las capas de protección independientes (IPL's) aplicables

En este punto es recomendable tener en cuenta la distinción entre una IPL (que ya se ha tratado en el capítulo 2 de esta tesis) y una protección o salvaguarda como las que se listan en un análisis HAZOP. Una protección o salvaguarda es cualquier dispositivo, sistema o acción que probablemente interrumpiría la cadena de eventos que siguen a un evento iniciador. Sin embargo, la eficacia de algunas protecciones o salvaguardas no puede ser cuantificada debido a la carencia de datos, a la incertidumbre en cuanto a su independencia o eficacia, o a otros factores.



- La **tabla 4.8** indica que protecciones o salvaguardas no se consideran de inicio como IPL's. Además.

Tabla 4.8. Protecciones o salvaguardas que usualmente no se consideran IPL's ⁽¹⁵⁾

Protecciones o salvaguardas que no se consideran IPL's.	Comentarios
Entrenamiento y certificación	Estos factores pueden ser considerados en la evaluación de la PFD para la acción del operador, pero no son por si solos IPL's.
Procedimientos y programas	Estos factores pueden ser considerados en la evaluación de la PFD para la acción del operador, pero no son por si solos IPL's.
Inspección y pruebas normales	Estas actividades se asumen que existen para todos los análisis de riesgos y forman la base de juicio para determinar la PFD. La prueba y la inspección normal afectan la PFD de ciertas IPL's. Alargar los intervalos de prueba e inspección puede incrementar la PFD de una IPL.
Mantenimiento	Esta actividad se asume que existe para todos los análisis de riesgos y forma la base de juicio para determinar la PFD. El mantenimiento afecta la PFD de ciertas IPL's.
Comunicaciones	Es una suposición básica que existen comunicaciones adecuadas en una instalación. Comunicaciones pobres afectan la PFD de ciertas IPL's.
Señalizaciones	Las señalizaciones por si mismas no son IPL's. Las señalizaciones pueden no ser claras, oscurecidas, ignoradas, etc. Las señalizaciones pueden afectar la PFD de ciertas IPL's.
Protección contra incendio	La protección contra incendios activa no se considera a menudo como una IPL pues es un evento posterior para la mayoría de los escenarios y su disponibilidad y efectividad puede ser afectada por el fuego y/o explosión la cual se pretende contener. Sin embargo, si una compañía puede demostrar que cumple con los requisitos de una IPL para un escenario dado puede ser utilizada como IPL. Nota: La protección contra incendios es una IPL de mitigación pues procura prevenir una consecuencia más grande posterior a un evento que ha ocurrido ya. El aislamiento a prueba de fuego se puede utilizar como una IPL para algunos escenarios a condición de que cumpla los requisitos de la normatividad API y de estándares corporativos.

Nota: La deficiente ejecución en las áreas discutidas en esta tabla pueden afectar la seguridad del proceso de la planta entera y de este modo pueden afectar algunas de las suposiciones hechas en la aplicación de la metodología propuesta.

Las capas de protección independiente (IPL) posteriores a los sistemas de relevo ya no se consideraron en esta metodología, pues la meta principal de este estudio es asegurar que los



incidentes se queden dentro de los límites de las plantas de proceso y no tener la necesidad de usar esas IPL's.

4.3.5 Evaluación de la efectividad de las IPL's

El valor de la efectividad de cada capa identificada de acuerdo al punto 4.3.6 será una calificación de efectividad (CE) asociada para cuya asignación se utilizará la **tabla 4.9**, donde la primera columna nos muestra los CE asociados a los valores de efectividad.

Tabla 4.9. Calificación de la efectividad (E) de las IPL's ⁽¹⁵⁾

CE= $-\log_{10}(\text{PFD})$	Confiabilidad	Probabilidad de falla bajo demanda (PFD)	SIL equivalente	Ejemplos típicos
0	0%	100%		Sin salvaguardas o salvaguardas no diseñadas para el escenario analizado. Operación compleja y con muy poco tiempo para responder.
1	90%	10%		Operación simple, respuesta con tiempo adecuado (confiabilidad normal del ser humano).
2	99%	1%	1	Lazo de control automático sencillo con pruebas funcionales periódicas.
3	99.9%	0.1%	2	Protección pasiva (válvula de relevo) o una combinación de protecciones con calificaciones 1 y 2.
4	99.99%	0.01%	3	Dos lazos de control automáticos sencillos independientes en el mismo equipo o sección con pruebas funcionales periódicas.

Para la asignación de los valores de CE a cada una de las IPL's se relacionará la PDF de las publicaciones de la AIChE, muchas de ellas se muestran en el anexo A de este trabajo.

4.3.6 Obtención de la efectividad total de las capas de protección independientes

Para comenzar se necesita explicar de dónde salen los términos que se utilizaran en esta metodología. En la teoría del LOPA, los accidentes ocurren cuando se combina un evento iniciador con la falla de las capas de protección del proceso, siendo la frecuencia de dichos accidentes ($F_{\text{consecuencia}}$) igual a la frecuencia de los eventos iniciales (F_{causa}) por la probabilidad de que éstos fallen simultáneamente ante estas demandas (PFD_i).



$$F_{consecuencia} = F_{causa} \cdot \prod_{i=1}^n PFD_i$$

Si reescribimos la ecuación anterior con logaritmos para facilitar el manejo de los números se obtiene:

$$\log(F_{consecuencia}) = \log(F_{causa}) + \sum_{i=1}^n \log(PFD_i)$$

Como la PFD es un número entre 0 y 1, el logaritmo siempre es menor que 0 o negativo, entonces se obtiene:

$$\log(F_{consecuencia}) = \log(F_{causa}) - \sum_{i=1}^n (-\log(PFD_i))$$

Si llamamos a:

$$CF = \log(F)$$

$$CE = -\log(PFD)$$

Donde

CF: Calificación de Frecuencia

CE: Calificación de Efectividad

F: Frecuencia (eventos por año)

PFD: Probabilidad de Falla bajo Demanda

Entonces la ecuación anterior se puede reescribir de manera simplificada como:

$$CF_{consecuencia} = CF_{causa} - \sum_{i=1}^n CE_i$$

Una vez identificado cada termino e identificada las capas de protección independiente y evaluadas en cuanto a su efectividad, se deberán sumar los valores **CE** individuales para obtener la efectividad total de las protecciones (**E_{tot}**), donde:

$$E_{tot} = \sum CE$$

4.3.7. Determinación de la efectividad mínima requerida del evento peligroso considerando las capas de protección independientes

Ya que se cuenta con la calificación de frecuencia de los eventos iniciales **CF** y con el valor de la efectividad total de las protecciones **E_{tot}** se calcula la calificación de frecuencia de los eventos iniciales tomando en cuenta las protecciones **CF_{consecuencia}** mediante la siguiente ecuación:



$$CF_{consecuencia} = CF - E_{tot}$$

Con el valor de $CF_{consecuencia}$ calculado y el valor asignado de CF_{meta} asociado a la gravedad de las consecuencias del punto 4.2.2, se calcular el valor de la efectividad mínima requerida (E_{min}) del escenario de riesgo considerando las capas de protección independientes mediante la siguiente ecuación:

$$E_{min} = CF_{consecuencia} - CF_{meta}$$

4.3.8. Determinación de las capas adicionales de protección y determinación del SIL

Se procede a calcular el SIL requerido si una SIF es recomendada, comparando la efectividad total de las capas y la efectividad mínima requerida.

Ya obtenida la efectividad mínima requerida del escenario de riesgo (E_{min}) se siguen los siguientes criterios:

- $E_{min} \leq 0$, entonces las protecciones son suficientes para el escenario de riesgo en cuestión.
- $E_{min} \ll 0$, entonces hay un exceso de protecciones, por lo tanto se recomienda la relocalización de las protecciones no indispensables.
- $E_{min} > 0$, entonces las protecciones son insuficientes para el escenario de riesgo en cuestión (la efectividad de las protecciones no alcanza para reducir la frecuencia del evento inicial hasta el valor de frecuencia meta del escenario), por lo tanto es necesario agregar protecciones adicionales.

En el supuesto de que se tenga un $E_{min} > 0$, se tienen los siguientes tres casos de acuerdo al valor de E_{min} que se haya obtenido:

Caso 1: $E_{min} \leq 1.5$

En caso de que ya haya capas de protección aplicables al escenario (normalmente este es el caso), es prudente recomendar mejorar la efectividad de éstas capas (por ejemplo: los programas de mantenimiento más frecuentes y sistematizados pueden mejorar la confiabilidad de las protecciones ya existentes; la respuesta de los operadores puede ser razonablemente



mejorada con capacitación y entrenamiento). En caso de no haber capas de protección aplicables al escenario, tratar de implementar alguna capa de protección que no sea un SIS.

Caso 2: $1.5 < E_{min} \leq 4$

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

Caso3: $E_{min} > 4$

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

En caso de resultar conveniente el uso de un Sistema Instrumentado de Seguridad (SIS), el SIL requerido se determinará reevaluando el valor de E_{min} después de considerar las otras alternativas no-SIS y utilizando la **tabla 4.10**.

Tabla 4.10. Determinación del SIL requerido a partir del valor de E_{min} .		
E_{min} .	PFD correspondiente	SIL requerido
1.5 - 2	$10^{-1} - 10^{-2}$	1
2.5 - 3	$10^{-2} - 10^{-3}$	2
3.5 - 4	$10^{-3} - 10^{-4}$	3

Para la correcta aplicación de la metodología del SIL requerido, se recomienda utilizar el formato guía que se muestra en la **figura 4.2**. En este mismo se da a conocer la información que se obtiene del análisis HAZOP y que sirve para calcular el SIL.

4.3.9. En caso de requerir un SIS, proponer el diseño conceptual del SIS

La propuesta del diseño conceptual del SIS será de acuerdo al escenario de riesgo en el que haya resultado un SIS y bajo el amparo de las normas ANSI/ISA 84.01, IEC 61508, IEC 61511 y NRF-045-PEMEX-2002.



CAPÍTULO 4: DETERMINACIÓN DEL NIVEL INTEGRAL DE SEGURIDAD (SIL)



 UNAM	HOJA DE DETERMINACIÓN DE LOS SISTEMAS INSTRUMENTADOS DE SEGURIDAD (SIS) REQUERIDOS Y DE SU NIVEL DE INTEGRIDAD DE SEGURIDAD (SIL) OBJETIVO.		
Planta:		Número de estudio SIL:	
Circuito:	Información de HAZOP	Fecha de revisión:	
Nodo No. Información de HAZOP			
Descripción del nodo:	Información de HAZOP		
Diagramas:			
Productos:			
Desviación No. Información de HAZOP			
Palabra Guía:	Información de HAZOP		
Parámetro:	Información de HAZOP		
Desviación:	Información de HAZOP		
Escenario No. Información de HAZOP			
Descripción del Escenario:	Información de HAZOP		
Evento Inicial			CF
Información de HAZOP			Información de HAZOP
Consecuencias		Categoría	CF_{META}
Información de HAZOP			
Capas de Protección Independientes (IPL)			CE
Información de HAZOP			
Efectividad total ($E_{tot} = \sum CE_i$):			
Calificación de frecuencia del evento inicial tomando en cuenta las protecciones ($CF_{consecuencia} = CF - E_{tot}$):			
Efectividad mínima requerida: ($E_{min} = CF_{consecuencia} - CF_{meta}$):			
Aplicación de los criterios de E_{min}		Interpretación de los Criterios	
$E_{min} \leq 0$	<input type="checkbox"/>	Las protecciones son suficientes para el escenario de riesgo en cuestión.	
$E_{min} < 0$	<input type="checkbox"/>	Hay un exceso de protecciones, por lo tanto se recomienda la relocalización de las protecciones no indispensables.	
$E_{min} > 0$	<input type="checkbox"/>	Las protecciones son insuficientes para el escenario de riesgo en cuestión (la efectividad de las protecciones no alcanza para reducir la frecuencia del evento inicial hasta el valor de frecuencia meta del escenario), por lo tanto es necesario agregar protecciones adicionales.	
En caso de que $E_{min} > 0$, aplicar los siguientes criterios:			
$E_{min} \leq 1.5$	<input type="checkbox"/>	$1.5 < E_{min} \leq 4$	<input type="checkbox"/>
		$E_{min} > 4$	<input type="checkbox"/>
Alternativas aplicables			
No.	Alternativa		CE
¿Se recomienda un SIS?		SI <input type="checkbox"/> NO <input type="checkbox"/>	En caso de requerirse un SIS, ¿Qué SIL Debe Cumplir?
Recomendaciones, acciones, o comentarios adicionales.			
1			

Figura 4.4. Formato para la aplicación de la metodología del SIL requerido



4.4. Resultados

Una vez definidos los criterios de aceptabilidad de riesgos en la **tabla 4.2** del punto **4.2.1** se procede a aplicar la metodología planteada en este trabajo, por lo que, derivado del HAZOP de la planta FCC realizado con anterioridad, se tuvieron en cuenta los escenarios con niveles de riesgo tipo A y tipo B, sin embargo no todas eran candidatas a un estudio SIL ya que la gran mayoría de ellas no se relacionaban con algún tipo de capa de protección independiente. Además de ello se dejó fuera todos aquellos donde la recomendación fuera instalar un sistema de detección de gas y fuego por lo anteriormente establecido en el alcance de este trabajo.

A continuación se exponen en la **tabla 4.11**. Cada una de ellas será analizada y se le realizara el cálculo de su nivel de integridad de seguridad.

Tabla 4.11. Emergencias en el convertidor 1-D de una planta FCC

Caso	Variable	Desviación	Evento inicial	Calificación HAZOP
1.1	Diferencial de presión de la válvula de catalizador agotado (PV1)	bajo-bajo	Falla de transmisor de presión diferencial PDT-7	B
1.2	Diferencial de presión de la válvula de catalizador regenerado (PV2)	bajo-bajo	Falla de transmisor de presión diferencial PDT-8	B
1.3	Temperatura de reacción en el RISER	bajo	Falla de controlador de temperatura de reacción TRC-2	B
1.5	Nivel de catalizador en el agotador	alto-alto	Falla de controlador de nivel en el separador LRC-1	B
1.6	Flujo de aire de combustión a regenerador	bajo-bajo	Falla de aire soplador 1-J	B
1.7	Diferencial de presión separador-regenerador	bajo-bajo	Falla de controlador de presión diferencial separador-regenerador PDRC-4	B
2	Presión en el separador del convertidor 1-D	alto-alto	Falla del compresor de gas húmedo 2-J	B

Caso 1.

Este caso se refiere al convertidor. Los controles primarios de suma importancia en un convertidor FCC sin duda son para variables como la temperatura, la presión y el nivel de catalizador. Para comprender a plenitud los riesgos que pueden existir en este convertidor se



debe comprender a fondo la filosofía de operación del control automático de procesos y analizar los lazos de control que son críticos.

Se les llama lazos críticos ya que son tan importantes para la correcta y segura operación del convertidor, que una falla en uno de ellos podría ocasionar un descontrol en toda la unidad y que si no se toma una adecuada respuesta ante un problema en uno de ellos podría tener consecuencias negativas en los trabajadores, el medio ambiente y las mismas instalaciones.

En una unidad como esta, aun existen 4 modos de control: el manual, el automático, en cascada y el avanzado. Es por ello que se dificulta el análisis de la filosofía de control.

A continuación una descripción general de los lazos de control críticos que se encontraron en el convertidor.

Lazos de control críticos del convertidor.

El primer lazo de control crítico es el que controla la cantidad de catalizador existente en el separador/agotador. Este nivel está controlado por el LRC-1 como se puede apreciar en la figura 4.4 que acciona la válvula tapón de catalizador agotado PV-1, localizado a la salida del tubo bajante del agotador. Se dispone de alarmas por alto y bajo nivel (LAH-1 y LAL-1) asociadas al control de nivel, para avisar cuando se presente cualquiera de estas condiciones. Hay un registrador de densidad (DR-1) colocado a través de la cama catalítica del agotador.

El segundo lazo de control crítico es el flujo de catalizador regenerado al reactor elevador que está controlado por un controlador registrador de temperatura TRC-2 que posiciona el tapón de la válvula PV-2 como se puede ver en la figura 4.4, de manera que permite mantener la temperatura adecuada en la salida del reactor, regulando el flujo de catalizador caliente que entra al reactor. La válvula tapón de catalizador agotado PV-1 es posicionada por el controlador registrador de nivel del agotador de catalizador LRC-1. Un cambio en la abertura de la válvula tapón provoca un cambio en la circulación de catalizador y mantiene las condiciones de operación en la posición de ajuste que se le indique. Se dispone de indicadores de posición de las válvulas (VPI-5 para la de catalizador agotado (PV-1) y VPI-6 para la del regenerador (PV-2)).

Parte de este lazo de control lo conforma también el registrador de nivel LR-3, que registra el nivel de catalizador en la primera etapa del regenerador, mientras que el LRC-2 lo hace



con el de la segunda etapa. El control de la válvula tapón PV-2 lo tendrá el LRC-2 en vez del TRC-2 a través de un relevador RL-2 en caso de haber bajo nivel de catalizador en la segunda etapa. Asociadas al LRC-2 están una alarma por alto y otra por bajo nivel (LAH-2y LAL-2). Se cuenta con registradores de densidad en ambas etapas de regeneración, DR-2 para la primera y DR-3 para la segunda. En ambas etapas de regeneración se cuenta con registradores de diferenciales de temperatura entre las fases densa y diluida (TDR-4 para la primera etapa y TDR-5 para la segunda). Se incluyen alarmas por alta diferencial de temperatura asociadas con el TDR-5 de la segunda etapa.

El tercer control crítico asegura una circulación de catalizador ininterrumpida y uniforme, manteniendo una adecuada caída de presión a través de las válvulas de control de catalizador agotado y regenerado PV-1 y PV-2.

Para ellos se dispone de un sistema controlador de presión diferencial (PDRC-4) entre el separador y el regenerador. Este controlador posicionará una de las válvulas deslizantes que controlan la salida de los gases de combustión del regenerador para mantener una presión diferencial prefijada. Sin embargo, se incluye un relevador selector (RL-1) para prevenir sobrepresionamiento en el regenerador. Este consiste en un relevador selector de señal baja. Las señales de aire de instrumentos de la salida del controlador de presión del regenerador PRC-6 y la salida del PDRC- 4 se alimentan al relevador selector RL-1. Entonces el relevador selecciona la señal de aire de instrumentos más baja y pasa esta señal hacia la válvula deslizante (la que tenga alineado el aire motriz) para hacer los ajustes necesarios. Adicionalmente los diferenciales de presión de las válvulas tapón se indican por las PDR-7 y PDR-8 con alarmas de baja diferencial PDAL-7 y PDAL 8.

Una vez analizados los lazos críticos del sistema, y con base en los escenarios de riesgo potencial arrojados por el HAZOP mostrados en la tabla **4.11**, indican que el mayor riesgo que existe en un convertidor de una planta FCC es la inversión de las diferenciales de las válvulas tapón (baja presión diferencial), ya que provocaría condiciones de emergencia extremas. A continuación se analizan cada uno de estos casos con la metodología que se empleara en este trabajo mediante el llenado de la hoja para la determinación del SIL.

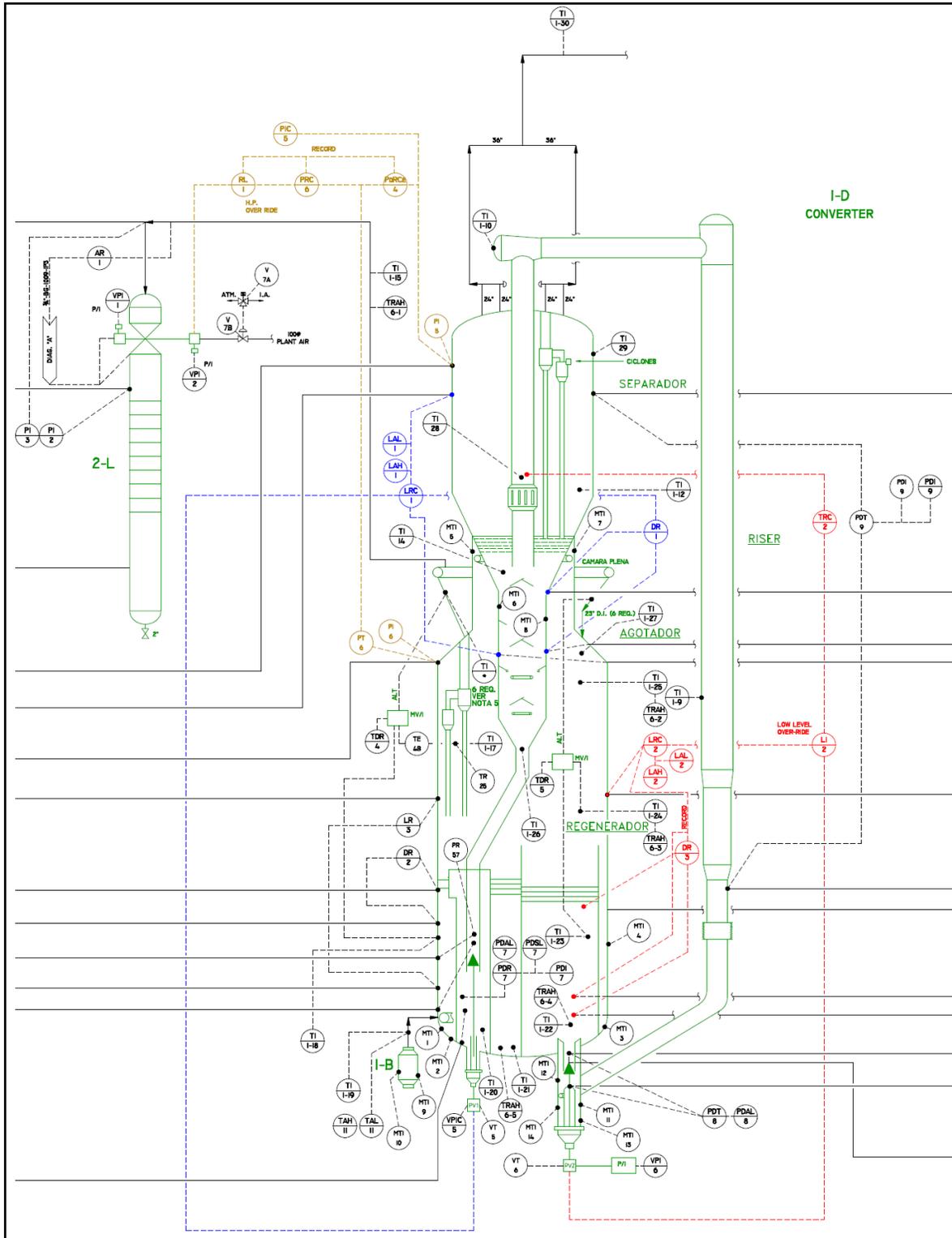


Figura 4.5. Lazos de control críticos del convertidor 1-D

CASO 1.1.

 UNAM	HOJA DE DETERMINACIÓN DE LOS SISTEMAS INSTRUMENTADOS DE SEGURIDAD (SIS) REQUERIDOS Y DE SU NIVEL DE INTEGRIDAD DE SEGURIDAD (SIL) OBJETIVO.		
	Planta:	Catalítica FCC No. 1	Número de estudio SIL:
Circuito:	De Reacción.	Fecha de revisión:	01/03/2012

Nodo No. 4	
Descripción del nodo:	Recibo de carga fresca precalentada al convertidor 1-D y reacción.
Diagramas:	62-D3 y 62-D4
Productos:	Gasóleo, Gasolina, LPG, H ₂ S y Gas combustible

Desviación No. 9	
Palabra Guía:	Inverso
Parámetro:	Flujo
Desviación:	Flujo inverso

Escenario No. 1		
Descripción del Escenario:	Flujo inverso de catalizador	
Evento Inicial		CF
Falla de transmisor de presión diferencial PDAL-7		0
Consecuencias	Categoría	CF_{META}
1. Pérdida del diferencial de presión al ser falsa la medición. En caso de una inversión del diferencial de presión este no se detecta a tiempo. 2. El diferencial de presión regenerador-separador disminuye y esta ocasiona falla en la circulación del catalizador e inversión del diferencial de presión de las válvulas PV-1. 3. Inversión de la diferencial en la PV-1, que permitiría el paso de aire al agotador de catalizador, lo que ocasionaría una combustión en esa zona con el consecuente aumento de temperatura en todo el separador. 4. También permitiría que el gas de combustión caliente fluya en reversa al riser y el fraccionador principal, dañando la integridad mecánica de estos recipientes con peligro de explosión. 5. Disminución de la temperatura en el riser. 6. Paro de Planta.	Catastrófico	-4.5
Capas de Protección Independientes (IPL)		CE
1. Lazo de control PDRC-4 que controla la presión del regenerador.		2.0
Efectividad total ($E_{tot} = \sum CE_i$):		2.0
Calificación de frecuencia del evento inicial tomando en cuenta las protecciones ($CF_{consecuencia} = CF - E_{tot}$):		-2.0
Efectividad mínima requerida: ($E_{min} = CF_{consecuencia} - CF_{meta}$):		2.5
Aplicación de los criterios de E_{min}	Interpretación de los Criterios	
$E_{min} \leq 0$	<input type="checkbox"/>	Las protecciones son suficientes para el escenario de riesgo en cuestión.
$E_{min} << 0$	<input type="checkbox"/>	Hay un exceso de protecciones, por lo tanto se recomienda la relocalización de las protecciones no indispensables.



CAPÍTULO 4: DETERMINACIÓN DEL NIVEL INTEGRAL DE SEGURIDAD (SIL)



$E_{min} > 0$	<input checked="" type="checkbox"/>	Las protecciones son insuficientes para el escenario de riesgo en cuestión (la efectividad de las protecciones no alcanza para reducir la frecuencia del evento inicial hasta el valor de frecuencia meta del escenario), por lo tanto es necesario agregar protecciones adicionales.
---------------	-------------------------------------	---

En caso de que $E_{min} > 0$, aplicar los siguientes criterios:

$E_{min} \leq 1.5$	<input type="checkbox"/>	$1.5 < E_{min} \leq 4$	<input checked="" type="checkbox"/>	$E_{min} > 4$	<input type="checkbox"/>
Alternativas aplicables					
No.	Alternativa	CE	$SIL_{equivalente}$		
1	Instalar Función Instrumentada de Seguridad (SIF) con la propuesta de configuración SIL 1 muy baja presión diferencial en la válvula de catalizador gastado PV-1 en el convertidor 1-D. La señal se alimentara al sistema de paro de emergencia por baja presión diferencial del convertidor 1-D.	2.0	1		
¿Se recomienda un SIS?	SI <input checked="" type="checkbox"/>	NO <input type="checkbox"/>	En caso de requerirse un SIS, ¿Qué SIL Debe Cumplir?		1

Recomendaciones, acciones, o comentarios adicionales.

1

Caso 1.2

 UNAM		HOJA DE DETERMINACIÓN DE LOS SISTEMAS INSTRUMENTADOS DE SEGURIDAD (SIS) REQUERIDOS Y DE SU NIVEL DE INTEGRIDAD DE SEGURIDAD (SIL) OBJETIVO.	
Planta:	Catalítica FCC No. 1	Número de estudio SIL:	3
Circuito:	De Reacción.	Fecha de revisión:	01/03/2012

Nodo No. 4	
Descripción del nodo:	Recibo de carga fresca precalentada al convertidor 1-D y reacción.
Diagramas:	62-D3 y 62-D4
Productos:	Gasóleo, Gasolina, LPG, H ₂ S y Gas combustible

Desviación No. 9	
Palabra Guía:	Inverso
Parámetro:	Flujo
Desviación:	Flujo inverso

Escenario No. 2		
Descripción del Escenario:	Flujo inverso de catalizador	
Evento Inicial		CF
Falla de transmisor de presión diferencial PDAL-8		0
Consecuencias		CF_{META}
1. Pérdida del diferencial de presión al ser falsa la medición. En caso de una inversión del diferencial de presión este no se detecta a tiempo. 2. El diferencial de presión regenerador-separador disminuye y esta ocasiona falla en la circulación del catalizador e inversión del diferencial de presión de las válvulas PV-2. 3. La inversión de la caída de presión en la PV-2 permitiría el paso de catalizador embebido de hidrocarburos; así como vapores de hidrocarburos al regenerador lo cual provocaría temperaturas extremas, superando ampliamente los límites mecánicos de los recipientes. 4. Flujo inverso del catalizador del regenerador al soplador 1-J 5. Disminución de la temperatura en el riser. 6. Paro de Planta.		Catastrófico -4.5
Capas de Protección Independientes (IPL)		CE
1. Lazo de control PDRC-4 que controla la presión del regenerador.		2.0
Efectividad total ($E_{tot} = \sum CE_i$):		2.0
Calificación de frecuencia del evento inicial tomando en cuenta las protecciones ($CF_{consecuencia} = CF - E_{tot}$):		-2.0
Efectividad mínima requerida: ($E_{min} = CF_{consecuencia} - CF_{meta}$):		2.5
Aplicación de los criterios de E_{min}	Interpretación de los Criterios	
$E_{min} \leq 0$	<input type="checkbox"/>	Las protecciones son suficientes para el escenario de riesgo en cuestión.



CAPÍTULO 4: DETERMINACIÓN DEL NIVEL INTEGRAL DE SEGURIDAD (SIL)



$E_{min} < 0$	<input type="checkbox"/>	Hay un exceso de protecciones, por lo tanto se recomienda la relocalización de las protecciones no indispensables.
$E_{min} > 0$	<input checked="" type="checkbox"/>	Las protecciones son insuficientes para el escenario de riesgo en cuestión (la efectividad de las protecciones no alcanza para reducir la frecuencia del evento inicial hasta el valor de frecuencia meta del escenario), por lo tanto es necesario agregar protecciones adicionales.

En caso de que $E_{min} > 0$, aplicar los siguientes criterios:

$E_{min} \leq 1.5$	<input type="checkbox"/>	$1.5 < E_{min} \leq 4$	<input checked="" type="checkbox"/>	$E_{min} > 4$	<input type="checkbox"/>
--------------------	--------------------------	------------------------	-------------------------------------	---------------	--------------------------

Alternativas aplicables

No.	Alternativa	CE	$SIL_{equivalente}$
1	Instalar Función Instrumentada de Seguridad (SIF) con la propuesta de configuración SIL 1 muy baja presión diferencial en la válvula de catalizador regenerado PV-2 en el convertidor 1-D. La señal se alimentara al sistema de paro de emergencia por baja presión diferencial del convertidor 1-D.	2.0	1
¿Se recomienda un SIS?		SI <input checked="" type="checkbox"/>	NO <input type="checkbox"/>
En caso de requerirse un SIS, ¿Qué SIL Debe Cumplir?			1

Recomendaciones, acciones, o comentarios adicionales.

1

CASO 1.3.

 UNAM	HOJA DE DETERMINACIÓN DE LOS SISTEMAS INSTRUMENTADOS DE SEGURIDAD (SIS) REQUERIDOS Y DE SU NIVEL DE INTEGRIDAD DE SEGURIDAD (SIL) OBJETIVO.		
	Planta:	Catalítica FCC No. 1	Número de estudio SIL:
Circuito:	De Reacción.	Fecha de revisión:	01/03/2012

Nodo No. 4	
Descripción del nodo:	Recibo de carga fresca precalentada al convertidor 1-D y reacción.
Diagramas:	62-D3 y 62-D4
Productos:	Gasóleo, Gasolina, LPG, H ₂ S y Gas combustible

Desviación No. 5	
Palabra Guía:	También como
Parámetro:	Presión
Desviación:	Baja presión diferencial

Escenario No. 4		
Descripción del Escenario:	Baja presión diferencial	
Evento Inicial		CF
Falla del controlador TRC-2 con una posición más cerrada en la válvula PV-2		0
Consecuencias	Categoría	CF_{META}
1. Falla la circulación del catalizador y se invierte el diferencial de presión de las válvulas PV-2. 2. La inversión de la caída de presión en la PV-2 permitiría el paso de catalizador embebido de hidrocarburos; así como vapores de hidrocarburos al regenerador lo cual provocaría temperaturas extremas por un quemado descontrolado, superando ampliamente los límites mecánicos de los recipientes con riesgo alto de explosión. 3. Disminución de la temperatura en el riser, que ocasiona la formación de coque en las paredes del riser y en la fraccionadora principal. 4. Paro de Planta.	Catastrófico	-4.5
Capas de Protección Independientes (IPL)		CE
1. Lazo de control PDRC-4 de control de presión diferencial separador-regenerador.		2
2. Respuesta humana a una alarma de proceso (Baja presión diferencial en las válvulas PV1 o PV2 (PDAL-7 o PDAL-8 respectivamente)		0.5
Efectividad total ($E_{tot} = \sum CE_i$):		2.5
Calificación de frecuencia del evento inicial tomando en cuenta las protecciones ($CF_{consecuencia} = CF - E_{tot}$):		-2.5
Efectividad mínima requerida: ($E_{min} = CF_{consecuencia} - CF_{meta}$):		2.0
Aplicación de los criterios de E_{min}	Interpretación de los Criterios	
$E_{min} \leq 0$	<input type="checkbox"/>	Las protecciones son suficientes para el escenario de riesgo en cuestión.
$E_{min} < 0$	<input type="checkbox"/>	Hay un exceso de protecciones, por lo tanto se recomienda la relocalización de las protecciones no indispensables.



CAPÍTULO 4: DETERMINACIÓN DEL NIVEL INTEGRAL DE SEGURIDAD (SIL)



$E_{min} > 0$	<input checked="" type="checkbox"/>	Las protecciones son insuficientes para el escenario de riesgo en cuestión (la efectividad de las protecciones no alcanza para reducir la frecuencia del evento inicial hasta el valor de frecuencia meta del escenario), por lo tanto es necesario agregar protecciones adicionales.
---------------	-------------------------------------	---

En caso de que $E_{min} > 0$, aplicar los siguientes criterios:

$E_{min} \leq 1.5$ <input type="checkbox"/>	$1.5 < E_{min} \leq 4$ <input checked="" type="checkbox"/>	$E_{min} > 4$ <input type="checkbox"/>
---	--	--

Alternativas aplicables

No.	Alternativa	CE	SIL _{equivalente}
1	Instalar Función Instrumentada de Seguridad (SIF) con la propuesta de configuración SIL 1 por y baja temperatura de reacción a la salida del RISER del convertidor 1-D. La señal se alimentara al sistema de paro de emergencia por baja presión diferencial del convertidor 1-D.	2.0	1
¿Se recomienda un SIS?		SI <input checked="" type="checkbox"/> NO <input type="checkbox"/>	En caso de requerirse un SIS, ¿Qué SIL Debe Cumplir?
			1

Recomendaciones, acciones, o comentarios adicionales.

1



CASO 1.4

 UNAM	HOJA DE DETERMINACIÓN DE LOS SISTEMAS INSTRUMENTADOS DE SEGURIDAD (SIS) REQUERIDOS Y DE SU NIVEL DE INTEGRIDAD DE SEGURIDAD (SIL) OBJETIVO.		
	Planta: Catalítica FCC No. 1	Número de estudio SIL: 5	
Circuito: De Reacción.	Fecha de revisión: 01/03/2012		

Nodo No. 4	
Descripción del nodo:	Recibo de carga fresca precalentada al convertidor 1-D y reacción.
Diagramas:	62-D3 y 62-D4
Productos:	Gasóleo, Gasolina, LPG, H ₂ S y Gas combustible

Desviación No. 5	
Palabra Guía:	También como
Parámetro:	Presión
Desviación:	Baja presión diferencial

Escenario No. 5		
Descripción del Escenario:	Baja presión diferencial	
Evento Inicial		CF
Falla del controlador LIC-1 con una posición más cerrada en la válvula PV-1		0
Consecuencias	Categoría	CF_{META}
1. El nivel de catalizador en el separador aumenta dramáticamente, con ello aumenta la presión en el separador provocando una inversión en la presión diferencial. 2. Inversión de la diferencial en la PV-1, que permitiría el paso de aire al agotador de catalizador, lo que ocasionaría una combustión en esa zona con el consecuente aumento de temperatura en todo el separador. 3. También permitiría que el gas de combustión caliente fluya en reversa al riser y el fraccionador principal, dañando la integridad mecánica de estos recipientes con peligro de explosión. 4. La inversión de la caída de presión en la PV-2 permitiría el paso de catalizador embebido de hidrocarburos; así como vapores de hidrocarburos al regenerador lo cual provocaría temperaturas extremas por un quemado descontrolado, superando ampliamente los límites mecánicos de los recipientes con riesgo alto de explosión. 5. Disminución de la temperatura en el riser, que ocasiona la formación de coque en las paredes del riser y en la fraccionadora principal. 6. Mayor arrastre de catalizador a la fraccionadora principal 1-E. 7. Paro de Planta.	Catastrófico	-4.5
Capas de Protección Independientes (IPL)		CE
1. Lazo de control PDRC-4 de control de presión diferencial separador-regenerador.		2
2. Respuesta humana a una alarma de proceso (Baja presión diferencial en las válvulas PV1 o PV2; PDAL-7 o PDAL-8 respectivamente).		0.5
Efectividad total ($E_{tot} = \sum CE_i$):		2.5



CAPÍTULO 4: DETERMINACIÓN DEL NIVEL INTEGRAL DE SEGURIDAD (SIL)



Calificación de frecuencia del evento inicial tomando en cuenta las protecciones ($CF_{consecuencia} = CF - E_{tot}$):		-2.5
Efectividad mínima requerida: ($E_{min} = CF_{consecuencia} - CF_{meta}$):		2.0
Aplicación de los criterios de E_{min}	Interpretación de los Criterios	
$E_{min} \leq 0$	<input type="checkbox"/>	Las protecciones son suficientes para el escenario de riesgo en cuestión.
$E_{min} << 0$	<input type="checkbox"/>	Hay un exceso de protecciones, por lo tanto se recomienda la relocalización de las protecciones no indispensables.
$E_{min} > 0$	<input checked="" type="checkbox"/>	Las protecciones son insuficientes para el escenario de riesgo en cuestión (la efectividad de las protecciones no alcanza para reducir la frecuencia del evento inicial hasta el valor de frecuencia meta del escenario), por lo tanto es necesario agregar protecciones adicionales.

En caso de que $E_{min} > 0$, aplicar los siguientes criterios:			
$E_{min} \leq 1.5$	<input type="checkbox"/>	$1.5 < E_{min} \leq 4$	<input checked="" type="checkbox"/>
		$E_{min} > 4$	<input type="checkbox"/>
Alternativas aplicables			
No.	Alternativa	CE	$SIL_{equivalente}$
1	Instalar Función Instrumentada de Seguridad (SIF) con la propuesta de configuración SIL 1 por muy alto nivel en el separador de catalizador del convertidor 1-D. La señal se alimentara al sistema de paro de emergencia por baja presión diferencial del convertidor 1-D.	2.0	1
¿Se recomienda un SIS?	SI <input checked="" type="checkbox"/>	NO <input type="checkbox"/>	En caso de requerirse un SIS, ¿Qué SIL Debe Cumplir?
			1

Recomendaciones, acciones, o comentarios adicionales.
1

CASO 1.5

 UNAM	HOJA DE DETERMINACIÓN DE LOS SISTEMAS INSTRUMENTADOS DE SEGURIDAD (SIS) REQUERIDOS Y DE SU NIVEL DE INTEGRIDAD DE SEGURIDAD (SIL) OBJETIVO.		
	Planta: Catalítica FCC No. 1	Número de estudio SIL: 6	
Circuito: De reacción	Fecha de revisión: 01/03/2012		

Nodo No. 4	
Descripción del nodo:	Recibo de carga fresca precalentada al convertidor 1-D y reacción.
Diagramas:	62-D3 y 62-D4
Productos:	Gasóleo, Gasolina, LPG, H ₂ S y Gas combustible

Desviación No. 5	
Palabra Guía:	También como
Parámetro:	Presión
Desviación:	Baja presión diferencial

Escenario No. 1		
Descripción del Escenario:	Baja presión diferencial	
Evento Inicial		CF
Falla del soplador 1-J		0
Consecuencias	Categoría	CF_{META}
1. El regenerador se queda sin alimentación de aire y no será posible continuar la regeneración de catalizador ni mantener el balance térmico del convertidor. 2. El diferencial de presión regenerador-separador disminuye y esta ocasiona falla en la circulación del catalizador e inversión del diferencial de presión de las válvulas PV-1 y PV-2. 3. Inversión de la diferencial en la PV-1, que permitiría el paso de aire al agotador de catalizador, lo que ocasionaría una combustión en esa zona con el consecuente aumento de temperatura en todo el separador. 4. Igualmente, puede permitir que el gas de combustión caliente fluya en reversa al riser y el fraccionador principal, dañando la integridad mecánica de estos recipientes con peligro de explosión. 7. La inversión de la caída de presión en la PV-2 permitiría el paso de catalizador embebido de hidrocarburos; así como vapores de hidrocarburos al regenerador lo cual provocaría temperaturas extremas, superando ampliamente los límites mecánicos de los recipientes. 5. Disminución de la temperatura en el riser. 6. Paro de Planta.	Catastrófico	-4.5
Capas de Protección Independientes (IPL)		CE
1. Lazo de control PDRC-4 de control de presión diferencial separador-regenerador.		2.0
2. Respuesta humana a una alarma de proceso (Baja presión diferencial en las válvulas PV1 o PV2; PDAL-7 o PDAL-8 respectivamente).		0.5
Efectividad total ($E_{tot} = \sum CE_i$):		2.5



CAPÍTULO 4: DETERMINACIÓN DEL NIVEL INTEGRAL DE SEGURIDAD (SIL)



Calificación de frecuencia del evento inicial tomando en cuenta las protecciones ($CF_{consecuencia} = CF - E_{tot}$):		-2.5
Efectividad mínima requerida: ($E_{min} = CF_{consecuencia} - CF_{meta}$):		2.0
Aplicación de los criterios de E_{min}	Interpretación de los Criterios	
$E_{min} \leq 0$	<input type="checkbox"/>	Las protecciones son suficientes para el escenario de riesgo en cuestión.
$E_{min} << 0$	<input type="checkbox"/>	Hay un exceso de protecciones, por lo tanto se recomienda la relocalización de las protecciones no indispensables.
$E_{min} > 0$	<input checked="" type="checkbox"/>	Las protecciones son insuficientes para el escenario de riesgo en cuestión (la efectividad de las protecciones no alcanza para reducir la frecuencia del evento inicial hasta el valor de frecuencia meta del escenario), por lo tanto es necesario agregar protecciones adicionales.

En caso de que $E_{min} > 0$, aplicar los siguientes criterios:			
$E_{min} \leq 1.5$	<input type="checkbox"/>	$1.5 < E_{min} \leq 4$	<input checked="" type="checkbox"/>
		$E_{min} > 4$	<input type="checkbox"/>
Alternativas aplicables			
No.	Alternativa	CE	$SIL_{equivalente}$
1	Instalar Función Instrumentada de Seguridad (SIF) con la propuesta de configuración SIL 1 por muy bajo flujo de aire al regenerador de catalizador del convertidor 1-D. La señal se alimentara al sistema de paro de emergencia por baja presión diferencial del convertidor 1-D.	2.0	1
¿Se recomienda un SIS?		SI <input checked="" type="checkbox"/>	NO <input type="checkbox"/>
En caso de requerirse un SIS, ¿Qué SIL Debe Cumplir?			1

Recomendaciones, acciones, o comentarios adicionales.
1



CASO 1.6

 UNAM	HOJA DE DETERMINACIÓN DE LOS SISTEMAS INSTRUMENTADOS DE SEGURIDAD (SIS) REQUERIDOS Y DE SU NIVEL DE INTEGRIDAD DE SEGURIDAD (SIL) OBJETIVO.		
	Planta:	Catalítica FCC No. 1	Número de estudio SIL:
Circuito:	De Reacción.	Fecha de revisión:	01/03/2012

Nodo No. 4	
Descripción del nodo:	Recibo de carga fresca precalentada al convertidor 1-D y reacción.
Diagramas:	62-D3 y 62-D4
Productos:	Gasóleo, Gasolina, LPG, H ₂ S y Gas combustible

Desviación No. 5	
Palabra Guía:	También como
Parámetro:	Presión
Desviación:	Baja presión diferencial

Escenario No. 2		
Descripción del Escenario:	Baja Presión diferencial	
Evento Inicial		CF
Falla del controlador PDIC-4 por apertura de SLV-OTE, o SLV-PTE.		0
Consecuencias	Categoría	CF_{META}
1. El diferencial de presión regenerador-separador disminuye y esta ocasiona falla en la circulación del catalizador e inversión del diferencial de presión de las válvulas PV-1 y PV-2. 2. Inversión de la diferencial en la PV-1, que permitiría el paso de aire al agotador de catalizador, lo que ocasionaría una combustión en esa zona con el consecuente aumento de temperatura en todo el separador. 3. También permitiría que el gas de combustión caliente fluya en reversa al riser y el fraccionador principal, dañando la integridad mecánica de estos recipientes con peligro de explosión. 4. La inversión de la caída de presión en la PV-2 permitiría el paso de catalizador embebido de hidrocarburos; así como vapores de hidrocarburos al regenerador lo cual provocaría temperaturas extremas, superando ampliamente los límites mecánicos de los recipientes. 5. Flujo inverso del catalizador del regenerador al soplador 1-J. 6. Disminución de la temperatura en el riser. 7. Paro de Planta.	Catastrófico	-4.5
Capas de Protección Independientes (IPL)		CE
1. Respuesta humana a una alarma de proceso (Baja presión diferencial en las válvulas PV-1 y/o PV-2; PDAL-7 o PDAL-8 respectivamente)		0.5
2. Lazo de control PIC-6 que controla la presión del regenerador.		2
Efectividad total ($E_{tot} = \sum CE_i$):		2.5



Calificación de frecuencia del evento inicial tomando en cuenta las protecciones ($CF_{consecuencia} = CF - E_{tot}$):		-2.5
Efectividad mínima requerida: ($E_{min} = CF_{consecuencia} - CF_{meta}$):		2.0
Aplicación de los criterios de E_{min}	Interpretación de los Criterios	
$E_{min} \leq 0$	<input type="checkbox"/>	Las protecciones son suficientes para el escenario de riesgo en cuestión.
$E_{min} \ll 0$	<input type="checkbox"/>	Hay un exceso de protecciones, por lo tanto se recomienda la relocalización de las protecciones no indispensables.
$E_{min} > 0$	<input checked="" type="checkbox"/>	Las protecciones son insuficientes para el escenario de riesgo en cuestión (la efectividad de las protecciones no alcanza para reducir la frecuencia del evento inicial hasta el valor de frecuencia meta del escenario), por lo tanto es necesario agregar protecciones adicionales.

En caso de que $E_{min} > 0$, aplicar los siguientes criterios:			
$E_{min} \leq 1.5$	<input type="checkbox"/>	$1.5 < E_{min} \leq 4$	<input checked="" type="checkbox"/>
Alternativas aplicables			
No.	Alternativa	CE	SIL _{equivalente}
1	Instalar Función Instrumentada de Seguridad (SIF) con la propuesta de configuración SIL 1 por muy baja presión diferencial entre separador-regenerador del convertidor 1-D. La señal se alimentara al sistema de paro de emergencia por baja presión diferencial del convertidor 1-D.	2.0	1
¿Se recomienda un SIS?	SI <input checked="" type="checkbox"/>	NO <input type="checkbox"/>	En caso de requerirse un SIS, ¿Qué SIL Debe Cumplir?
			1

Recomendaciones, acciones, o comentarios adicionales.
1

Descripción del Sistema Instrumentado de Seguridad (SIS) del convertidor 1-D propuesto.

El Sistema Instrumentado de Seguridad (SIS) del convertidor 1-D propuesto como se muestra en la **figura 4.6** es denominado Sistema de Paro de Emergencia (ESD) por baja presión diferencial y es un conjunto de funciones instrumentadas de seguridad (SIF's), que tiene como objeto llevar al convertidor a un estado seguro en caso de que se invierta el diferencial de presión a través de las válvulas de catalizador gastado (PV-1) y catalizador regenerado (PV-2), ya que si esto llegara a suceder las consecuencias serian catastróficas.

El sistema realiza el paro de la unidad de manera automática y segura respondiendo ante los siguientes iniciadores mostrados en la **tabla 4.12**:

Tabla 4.12. Entradas del sistema de paro de emergencia del convertidor 1-D de la planta FCC

	Señal de muy bajo (low-low) diferencial de presión en la válvula de catalizador gastado PV-1.
	Señal de muy bajo (low-low) diferencial de presión en la válvula de catalizador regenerado PV-2.
	Señal de baja temperatura de reacción a la salida del RISER.
	Señal de muy alto (high-high) nivel de catalizador en el separador-agotador del convertidor 1-D.
	Señal de muy bajo (low-low) flujo de aire al primer paso del regenerador (FSSL-01A) y muy bajo flujo al segundo paso del regenerador (FSSL-02B). Se realiza una votación 2 de 2. Si las dos son positivas de procede a enviar la señal al ESD.
	Señal de muy bajo (low-low) diferencial de presión entre separador-regenerador.

Se propone que la unidad cuente con un Controlador de Procesos Críticos (CPC) de arquitectura Triple Modular Redundante (TMR) lo cual le permite mantener el control confiable del proceso aún en la presencia de fallas en el controlador. Este sistema supera fallas permanentes y transitorias desde las entradas de los sensores hasta las salidas de los actuadores. Tres tarjetas electrónicas supervisan independientemente los sensores de campo (variables inicializadoras), realizan el cálculo o lógica de control y proporcionan salida a los actuadores como se puede apreciar en la **figura 4.6**.

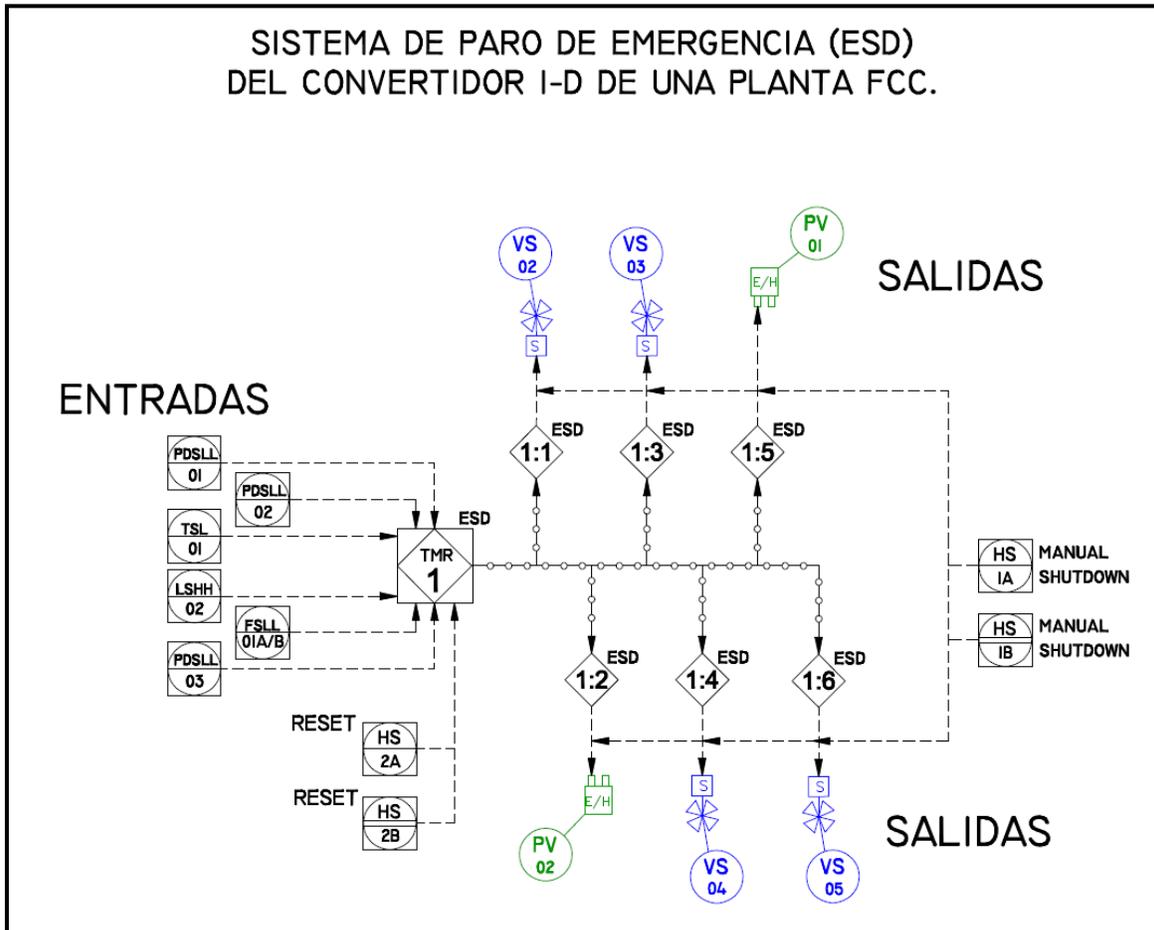


Figura 4.6. Sistema de paro de emergencia del convertidor

Si el resultado de por lo menos uno de los eventos iniciadores en la votación es positivo se inicia un período de validación de 20 segundos para el iniciador respectivo, antes de proceder con la secuencia de paro de emergencia del convertidor 1-D. Al iniciarse esta secuencia de paro de emergencia se des-energizan simultáneamente las salidas a campo, lo cual se traduce en los efectos de la **tabla 4.13**.



Tabla 4.13. Salidas del sistema de paro de emergencia del convertidor

Lógica.	Solenoides Des-energizada	Acción	Elemento Final	Descripción.
ESD 1:1	VS-02	CIERRA	VAAR-02	Corte de la admisión de carga al RISER del convertidor 1-D.
ESD 1:2	VS-03	ABRE	XV-01	Máxima admisión de vapor de levantamiento al RISER del convertidor 1-D.
ESD 1:3	--	CIERRA	PV-1	Corte de catalizador gastado hacia el regenerador del convertidor 1-D.
ESD 1:4	--	CIERRA	PV-2	Corte de catalizador regenerado al RISER del convertidor 1-D.
ESD 1:5	VS-04	ABRE	XV-02	Desvío de la carga hacia la fraccionadora principal 1-E.
ESD 1:6	VS-05	ABRE	XV-03	Admisión del vapor de levantamiento de emergencia al RISER del convertidor 1-D

Para las funciones instrumentadas de seguridad que tienen el objetivo de cortar la circulación de catalizador de manera momentánea, es recomendable cambiar los actuadores de las válvulas de catalizador gastado y regenerado (PV-1 y PV-2) de neumático a electro-hidráulico.

Debido a que no se puede lograr independencia del elemento final de control en este caso específico, entre los sistemas instrumentados de seguridad y el control básico de procesos se propone usar un controlador redundante en el actuador de la válvula.



Los controladores redundantes constan de 2 nodos. Cada nodo puede controlar el actuador independientemente del otro. Un software en el controlador no sólo controla la posición de la válvula, sino que también controla el estado del otro nodo y los componentes individuales del nodo. Cuando el fallo de un componente o nodo se detecta, se producirán las conmutaciones adecuadas para garantizar que la unidad siga funcionando sin ninguna interrupción del servicio y sin necesidad de intervención humana.

HS-1A y HS-2A son botones ubicados en el cuarto de control dedicados al paro manual y al “reseteo” del SIS respectivamente. HS-1B y HS-2B cumplen la misma función solo que están localizados en panel o botonera 15 metros alejados de la VAAR.

En lo que respecta al desvío de la carga a la torre fraccionadora, esta debe ser lenta, para ello se puede usar un orificio de restricción (RO-01) o también se puede controlar con el tamaño de la válvula.

Con esta filosofía de paro de emergencia del convertidor, el regenerador puede seguir funcionando, aunque a tasas reducidas. Con el flujo de aire principal todavía viable, el regenerador puede mantenerse en funcionamiento y en la temperatura, ya sea con aceite de antorcha o un calentador de aire directo.

Este enfoque de mantener el regenerador en operación permite una rápida puesta en marcha del convertidor una vez que el problema de la presión diferencial se resuelve. En el **ANEXO B** se agregan los diagramas de tubería e instrumentación que se generaron al realizar los estudios SIL del convertidor.



Caso 3.

 UNAM	HOJA DE DETERMINACIÓN DE LOS SISTEMAS INSTRUMENTADOS DE SEGURIDAD (SIS) REQUERIDOS Y DE SU NIVEL DE INTEGRIDAD DE SEGURIDAD (SIL) OBJETIVO.		
	Planta:	Catalítica FCC No. 1	Número de estudio SIL:
Circuito:	De carga fresca.	Fecha de revisión:	01/03/2012

Nodo No. 1	
Descripción del nodo:	Recibo de carga fresca precalentada al convertidor 1-D y reacción.
Diagramas:	62-D3 y 62-D4
Productos:	Gasóleo, Gasolina, LPG, H ₂ S y Gas combustible

Desviación No. 10	
Palabra Guía:	Más/Alto
Parámetro:	Presión
Desviación:	Alta Presión

Escenario No. 1		
Descripción del Escenario:	Alta presión en separador del convertidor 1-D	
Evento Inicial		CF
Falla del compresor de gas húmedo 2-J		0
Consecuencias	Categoría	CF_{META}
1. El diferencial de presión regenerador-separador disminuye y esto ocasiona falla en la circulación del catalizador e inversión del diferencial de presión de las válvulas PV-1 y PV-2. 2. Inversión de la diferencial en la PV-1, que permitiría el paso de aire al agotador de catalizador, lo que ocasionaría una combustión en esa zona con el consecuente aumento de temperatura en todo el separador. 3. También permitiría que el gas de combustión caliente fluya en reversa al Riser y el fraccionador principal, dañando la integridad mecánica de estos recipientes con peligro de explosión. 4. La inversión de la caída de presión en la PV-2 permitiría el paso de catalizador embebido de hidrocarburos; así como vapores de hidrocarburos al regenerador lo cual provocaría temperaturas extremas, superando ampliamente los límites mecánicos de los recipientes. 5. Flujo inverso del catalizador del regenerador al soplador 1-J 6. Disminución de la temperatura en el Riser. 7. Paro de Planta.	Catastrófico	-4.5
Capas de Protección Independientes (IPL)		CE
1. Respuesta humana a una alarma de proceso PAH-15 (Baja presión diferencial en tanque de succión de 1er paso.		0.5
2. Lazo de control PIC-6 que controla la presión del regenerador.		2
Calificación de frecuencia del evento inicial tomando en cuenta las protecciones ($CF_{consecuencia} = CF - E_{tot}$):		-2.5
Efectividad mínima requerida: ($E_{min} = CF_{consecuencia} - CF_{meta}$):		2.0
Aplicación de los criterios de E_{min}	Interpretación de los Criterios	



CAPÍTULO 4: DETERMINACIÓN DEL NIVEL INTEGRAL DE SEGURIDAD (SIL)



$E_{min} \leq 0$	<input type="checkbox"/>	Las protecciones son suficientes para el escenario de riesgo en cuestión.
$E_{min} < 0$	<input type="checkbox"/>	Hay un exceso de protecciones, por lo tanto se recomienda la relocalización de las protecciones no indispensables.
$E_{min} > 0$	<input checked="" type="checkbox"/>	Las protecciones son insuficientes para el escenario de riesgo en cuestión (la efectividad de las protecciones no alcanza para reducir la frecuencia del evento inicial hasta el valor de frecuencia meta del escenario), por lo tanto es necesario agregar protecciones adicionales.

En caso de que $E_{min} > 0$, aplicar los siguientes criterios:			
$E_{min} \leq 1.5$	<input type="checkbox"/>	$1.5 < E_{min} \leq 4$	<input checked="" type="checkbox"/>
Alternativas aplicables			
No.	Alternativa	CE	SIL _{equivalente}
1	Instalar Función Instrumentada de Seguridad (SIF) con la propuesta de configuración SIL 1 por muy baja presión en la succión y descarga del compresor 2-J.	2.0	1
¿Se recomienda un SIS?	SI <input checked="" type="checkbox"/>	NO <input type="checkbox"/>	En caso de requerirse un SIS, ¿Qué SIL Debe Cumplir?
			1

Recomendaciones, acciones, o comentarios adicionales.
1

Descripción de la Función Instrumentada de Seguridad (SIF)

Este sistema de seguridad que se puede apreciar en la **Figura 4.7** con color azul, es denominado Sistema de Paro de Emergencia (ESD) por pérdida del compresor tiene como objeto mantener un estado seguro en el convertidor 1-D en caso de que se pierda la presión que genera el compresor.

El sistema realiza el paro de la unidad de manera automática y segura respondiendo ante los siguientes iniciadores (**Tabla 4.14**):

Tabla 4.14. Entradas del sistema de paro de emergencia por pérdida del compresor 2-J de la planta FCC	
	Señal de muy baja (low-low) presión de descarga del primer paso del convertidor 2-J
	Señal de muy baja (low-low) presión de descarga del segundo paso del convertidor 2-J



Si el resultado de la votación 2oo2 es positivo se inicia un período de validación de 20 segundos para el iniciador respectivo, antes de proceder con la secuencia de paro de emergencia del compresor 2-J. Al iniciarse esta secuencia de paro de emergencia se des-energizan simultáneamente las salidas a campo, lo cual se traduce en los siguientes efectos (Tabla 4.15):

Tabla 4.15. Salidas del sistema de paro de emergencia por pérdida del compresor 2-J de la planta FCC

Lógica.	Solenoides Des-energizada	Acción	Elemento Final	Descripción.
	VS-06	CIERRA	VAAR-03	Corte de recirculación de flujo mínimo del primer paso (ANTI-SURGE)
	VS-07	CIERRA	VAAR-04	Corte de recirculación de flujo mínimo del segundo paso (ANTI-SURGE)
	VS-08	CIERRA	VAAR-05	Corte de la descarga del primer paso del compresor 2-J.
	VS-09	CIERRA	VAAR-06	Corte de la descarga del segundo paso del compresor 2-J.
	VS-10	CIERRA	VAAR-07	Corte de la succión del primer paso del compresor 2-J.
	VS-11	CIERRA	VAAR-08	Corte de la succión del segundo paso del compresor 2-J.

Con esta filosofía de paro de emergencia del compresor, consigue que el sistema siga presionado. Este enfoque de mantener el sistema presionado, permite operar normalmente mientras el operador investiga la causa del disparo y lo restablece.

En dado caso de que no se pueda arreglar el problema y se empieza a invertir el diferencial de presión en el convertidor 1-D, entonces actuara el Sistema de Paro de Emergencia (ESD) propuesto del convertidor.



Arreglo típico de instrumentación de las válvulas de aislamiento de acción remota.

La **figura 4.8** muestra el arreglo típico de instalación de una VAAR para el caso del compresor. La lógica 1:7 desenergiza cada válvula solenoide de este SIS lo cual hace que la válvula falle en posición segura, es decir que cierre. Esto despresuriza el actuador de la válvula VAAR por lo que también se va a falla segura y cierra inmediatamente. Así es como se cumple con el estado seguro del proceso, con las seis VAAR's cerradas.

Se cuenta con un acumulador para el aire de instrumentos con su respectivo indicador de presión PI-06, con capacidad para tres ciclos de cierre-apertura para que en caso de pérdida del aire de instrumentos principal. Se cuenta con PAL-06, una alarma por baja presión de aire de instrumentos.

En todas las VAAR de este trabajo se cuenta con interruptores de límite o comúnmente llamados sensores de posición. VZSO-08 y VZSC-08 son sensores de estado para las posiciones abierto (open) y cerrado (close) respectivamente. VZLO-08 y VZLC-08 son indicadores de estado para las posiciones abierto (open) y cerrado (close) respectivamente. Estos indicadores están en un panel o botonera en campo que por norma debe estar separada 15 metros de la VAAR. En este mismo panel se encuentra HS-102B dedicado al paro manual. La misma función la cumple HS-102A solo que este botón se encuentra en el cuarto de control. ZAX-102 se encarga de "resetear" la función de seguridad a su estado habitual. VZS-08 es un indicador de posición de la válvula que le otorga el permiso en caso de estar en la posición abierta de poner en marcha nuevamente el compresor, esto con el fin de evitar una sobrepresión que desencadene una explosión del compresor.

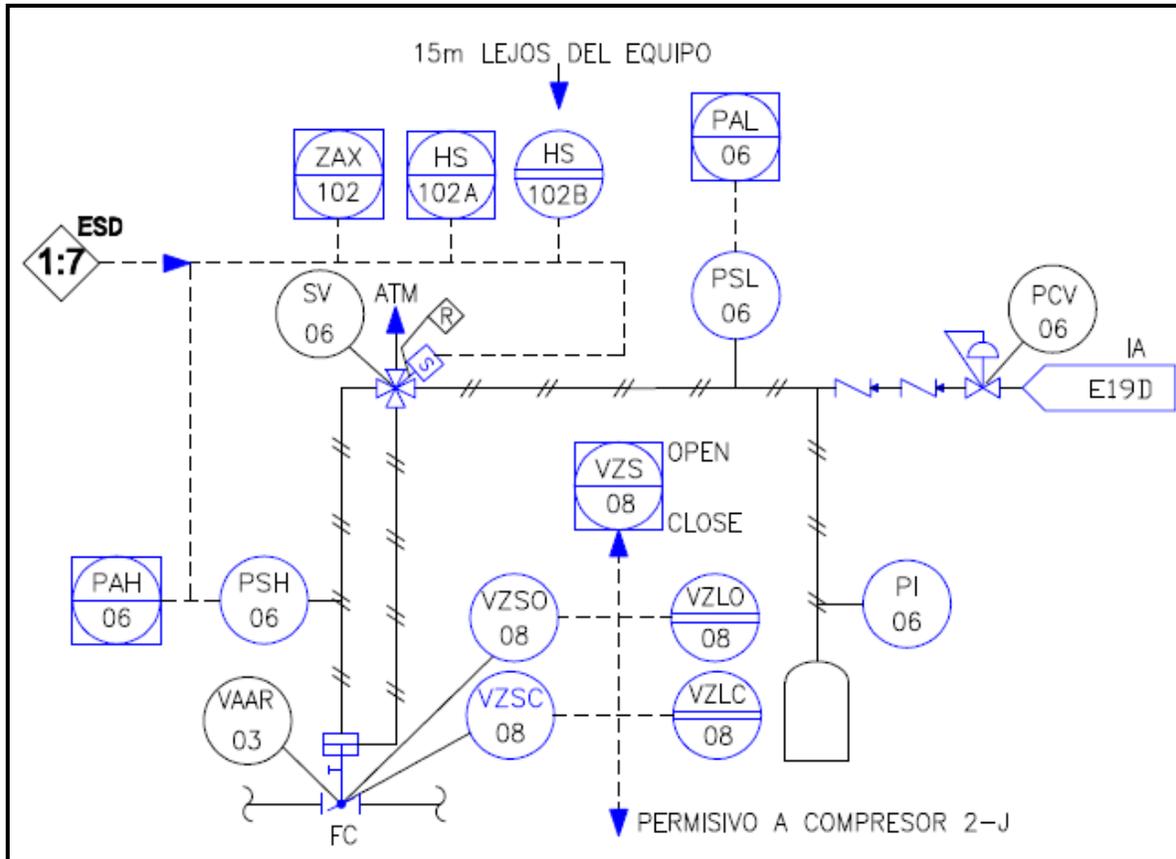


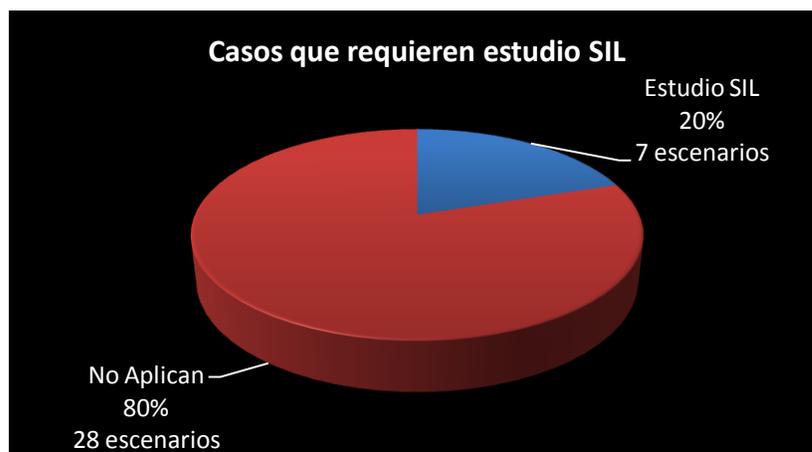
Figura 4.8. Instalación típica de las válvulas VAAR para el caso del compresor

4.5. Análisis de Resultados

De todos los 35 escenarios analizados en el HAZOP de la planta, seis tenían un nivel de riesgo tipo A y 29 eran nivel de riesgo tipo B.



De esos 35 escenarios, se separaron los que no se relacionaban con las capas de protección independientes, es decir que no requerían un estudio SIL y las que hacían referencia a la recomendación de la instalación de un sistema de detección de gas y fuego, por lo que quedaron 7 escenarios para realizar el estudio SIL.



De los escenarios analizados el 100%, es decir los 7 casos resultaron ser SIL1 como lo muestra la **tabla 4.16**.

Tabla 4.16. Resumen de las funciones instrumentadas de seguridad obtenidas

Nivel de riesgo según HAZOP	SIF	SIL
B	Paro de emergencia por sobrellenado del tanque de carga 12-F.	1
B	Paro de emergencia por baja presión diferencial en válvula de catalizador agotado PV-1.	1
B	Paro de emergencia por baja presión diferencial en válvula de catalizador regenerado PV-2.	1
B	Paro de emergencia por muy baja temperatura en el RISER del convertidor 1-D.	1
B	Paro de emergencia por muy alto nivel de catalizador en el separador-agotador del convertidor 1-D.	1
B	Paro de emergencia por muy bajo flujo de aire al regenerador del convertidor 1-D.	1
B	Paro de emergencia por baja presión diferencial en el separador-regenerador del convertidor 1-D.	1
B	Paro de emergencia por muy baja presión de descarga del primer y segundo paso del convertidor 2-J.	1



Cabe destacar que los siete escenarios están íntimamente ligados con la consecuencia catastrófica que resultaría de la pérdida del diferencial de presión a través del separador-regenerador del convertidor 1-D. Como se puede observar a simple vista, KBR Inc. (anteriormente *Kellogg Brown & Root*), que fue la compañía que diseñó este proceso, consideró que un operador con experiencia y bien entrenado sería la mejor protección frente a eventos anormales en el convertidor, esto se aprecia debido al uso excesivo de alarmas para las condiciones de emergencia del convertidor 1-D.

Sin embargo, la tendencia de hoy, es contar con menos operadores en las plantas y los que hay, no cuentan con tanta experiencia. Dada la naturaleza de la respuesta humana a situaciones de emergencia, es posible que el operador retrase la acción o tenga un error de juicio. En vista que la confiabilidad de un operador no llega a la confiabilidad que proporciona una SIF con SIL-1, en este trabajo se complementan las acciones del operador con este SIS propuesto, precisamente para responder con prontitud y correctamente ante una emergencia en el convertidor.

A pesar de que la gravedad de las consecuencias es catastrófica para los escenarios analizados, el que todas ellas hayan resultado SIL 1 no es de ninguna manera minimizar el problema, simplemente que la metodología empleada visualiza y valora todas las capas de protección que existen y en todas ellas al menos existe un sistema de alarmas y un lazo de control. Contrario a lo que plantearía un vendedor de SIS simplemente con observar que la gravedad de las consecuencias es catastrófica juzgaría que el SIS requerido es un SIL-2 o SIL-3, incrementando dramáticamente los costos.

Es notable la reducción del riesgo como lo muestra la **tabla 4.17** a continuación, para cada uno de los escenarios que se analizaron.



Tabla 4.17. Reducción del riesgo en la planta FCC de estudio

SIF	Magnitud de riesgo remanente según HAZOP	Magnitud de la reducción de riesgo según SIL de la función.	Riesgo residual remanente después de SIS
Paro de emergencia por sobrellenado del tanque de carga 12-F.	1.5	2.0	-0.5
Paro de emergencia por baja presión diferencial en válvula de catalizador agotado PV-1.	2.5	2.0	0.5
Paro de emergencia por baja presión diferencial en válvula de catalizador regenerado PV-2.	2.5	2.0	0.5
Paro de emergencia por muy baja temperatura en el RISER del convertidor 1-D.	2.0	2.0	0.0
Paro de emergencia por muy alto nivel de catalizador en el separador-agotador del convertidor 1-D.	2.0	2.0	0.0
Paro de emergencia por muy bajo flujo de aire al regenerador del convertidor 1-D.	2.0	2.0	0.0
Paro de emergencia por baja presión diferencial en el separador-regenerador del convertidor 1-D.	2.0	2.0	0.0
Paro de emergencia por muy baja presión de descarga del primer y segundo paso del convertidor 2-J.	2.0	2.0	0.0

Como se puede ver en la tabla anterior, la reducción de riesgo es visiblemente significativa, con esto se puede asegurar que al implementar los SIS propuestos, es posible controlar o contener los riesgos resultantes de cada escenario analizado. Además se puede reaccionar con efectividad ante cada desviación.

Es por ello que a diferencia de otros métodos, los SIS obtenidos aquí, son totalmente justificables.

Todos los SIS desarrollados, están ideados para evitar disparos en falso, es decir que ante una emergencia es posible que el operador responda a las alarmas de proceso, pero si no alcanza a hacerlo el SIS tomara las medidas pertinentes. Para ello se usa la filosofía de que los operadores respondan a alarmas de bajo o alto y los SIS lo hagan para muy bajo (bajo-bajo) o muy alto (alto-alto)



CONCLUSIONES Y RECOMENDACIONES



Se logró la determinación de los Sistemas Instrumentados de Seguridad (SIS) típicos de una planta FCC y de su Nivel Integral de Seguridad (SIL) además de que se realizó la propuesta del lazo de control para una planta de desintegración catalítica de gasóleos pesados (FCC) con una metodología semi-cuantitativa que ha demostrado ser efectiva y fácil de dominar, adaptada para la industria de refinación del petróleo.

La metodología permitió realizar un análisis exhaustivo de la normatividad ISA/IEC vigente, del proceso detallado que se lleva a cabo en una planta FCC típica, además del análisis HAZOP de esta misma planta. Se generaron las hojas de cálculo del SIL para cada escenario y se dio una descripción general de la función instrumentada de seguridad (SIF) que se propone definiendo así, el estado seguro del proceso para cada una de ellas.

De igual forma, gracias a la metodología se logró comprobar que cada una de las funciones de seguridad propuestas cumple con la reducción de riesgo necesaria para maximizar la seguridad de la planta, lo que verdaderamente lleva a una mejor justificación de los SIS en la planta.

Se está acostumbrado a un tipo de instrumentación en la materia de dinámica y control de procesos, sin embargo, al realizar la propuesta de los lazos de control para las SIF's, se familiarizo con la instrumentación típica de campo que requieren las funciones de seguridad, la cual es diferente a la instrumentación dedicada al control básico del proceso y de la que un ingeniero químico no está lo bastante relacionado al salir de la carrera, sin embargo que si debería por lo menos conocer.

Se logró comprobar que hay una nueva tendencia en cuanto a la realización de la normatividad, pasando de ser "recetas" a convertirse en normas que dan a conocer los procesos para obtener un resultado, más no el de pre-escribir la propia solución. Esto es algo muy importante ya que este tipo de normas va en aumento y es necesario que las nuevas generaciones de ingenieros las conozcan y se relacionen con ellas.

Durante el desarrollo de este trabajo se detectó el papel del ingeniero químico en un campo multidisciplinario como lo es la seguridad funcional y se llega a la conclusión que el aporte de éste es lo bastante significativo simplemente al dominar completamente el proceso y entender todos los peligros y riesgos que existen además de contar con el conocimiento de cuantificación del riesgo.



La experiencia que deja este trabajo es que la determinación de los SIS y de su SIL es cualquier cosa menos intuitivamente obvio, además de que como ingeniero químico no se debe ser complaciente con la seguridad. El arte en esta rama de la ingeniería resulta en pensar en lo impensable al concebir los escenarios de riesgo porque al realizar esto, se está realizando una cobertura más amplia en cuanto a la seguridad de la planta.

De igual forma se deja ver que a diferencia de otras metodologías y de las recomendaciones de los vendedores de SIS, la evaluación de riesgo y en sí mismo la seguridad global de una planta no debería ser simplemente una formalidad para satisfacer procedimientos o programas de gestión de proyectos como aun se sigue practicando. Realizar un análisis de riesgos no hará que una planta sea más segura, porque al final de todo, lo que genera es un simple informe en papel. Seguir las recomendaciones de ese estudio es lo que hará la planta más segura y eso es lo que se realizó en este trabajo.

Otro de los aspectos importantes en que se da a cuenta, es que cada organización tiene que decidir por sí sola “lo que es seguro”, es decir, debe definir claramente sus criterios de aceptabilidad de riesgos. Estas son las decisiones verdaderamente difíciles que pocos quieren hacer y menos escribirlas pero que al final de todo alguien debe hacerlas, porque al realizar una determinación del SIL, ya deben estar perfectamente definidas.

En lo que respecta a la seguridad de la planta, se detectó que se le confía excesivamente a la respuesta de los operadores los descontroles que rápidamente pueden llevar a una situación de emergencia, el presente trabajo no pone en duda la capacidad de los operadores para responder, por lo que la implementación de estos SIS de este estudio SIL realizado asegura una última barrera de protección en caso de una emergencia extrema. Ahora bien, también los SIS propuestos, son a prueba de disparos en falso, y se logro que ante una emergencia que realice el paro de la sección donde esta implementado el SIS, no cause un paro de planta y aun mejor, quede lista la sección para una rápida puesta en marcha.

Con base en la hipótesis planteada, se concluye que es posible realizar un estudio SIL con la información obtenida de un HAZOP, sin embargo, hay que recalcar que influye de manera importante la calidad con la que se realice el HAZOP, ya que errores que pudiera tener éste, son arrastrados al estudio SIL. Al realizar el estudio SIL ya no se puede detener a revisar si el HAZOP está bien realizado, debe confiarse plenamente en los datos que arroja este.



La mayoría de los SIL de los SIS de una planta resultan ser SIL-1, eso es más que suficiente incluso ante escenarios catastróficos y no como muchos de los proveedores de instrumentación manejan, que quieren vender instrumentos para SIL-2 o SIL-3 que resultan demasiado costosos. Aquí, mostró el proceso de cómo llegar a la decisión de determinar un SIS plenamente justificable.

Recomendaciones.

Para complementar este trabajo es necesario elaborar la especificación de requerimientos de seguridad (SRS) completas, para ello es imprescindible la aportación de las demás disciplinas como los son los ingenieros electrónicos que sin duda completaran cada una de ellas en cuanto a los aspectos de la tecnología y la programación.

Sin duda, se tiene que seguir capacitando ingenieros químicos en esta rama de la seguridad funcional que cada vez mas va cobrando fuerza con el objetivo de formar recursos para proyectos a futuro.

La metodología propuesta es semi-cuantitativa, se recomienda realizar el cálculo con una metodología cuantitativa como el ACR dedicado, un método que no es muy común o con algún software comercial de alguna empresa que se dedique al ramo de la seguridad industrial.



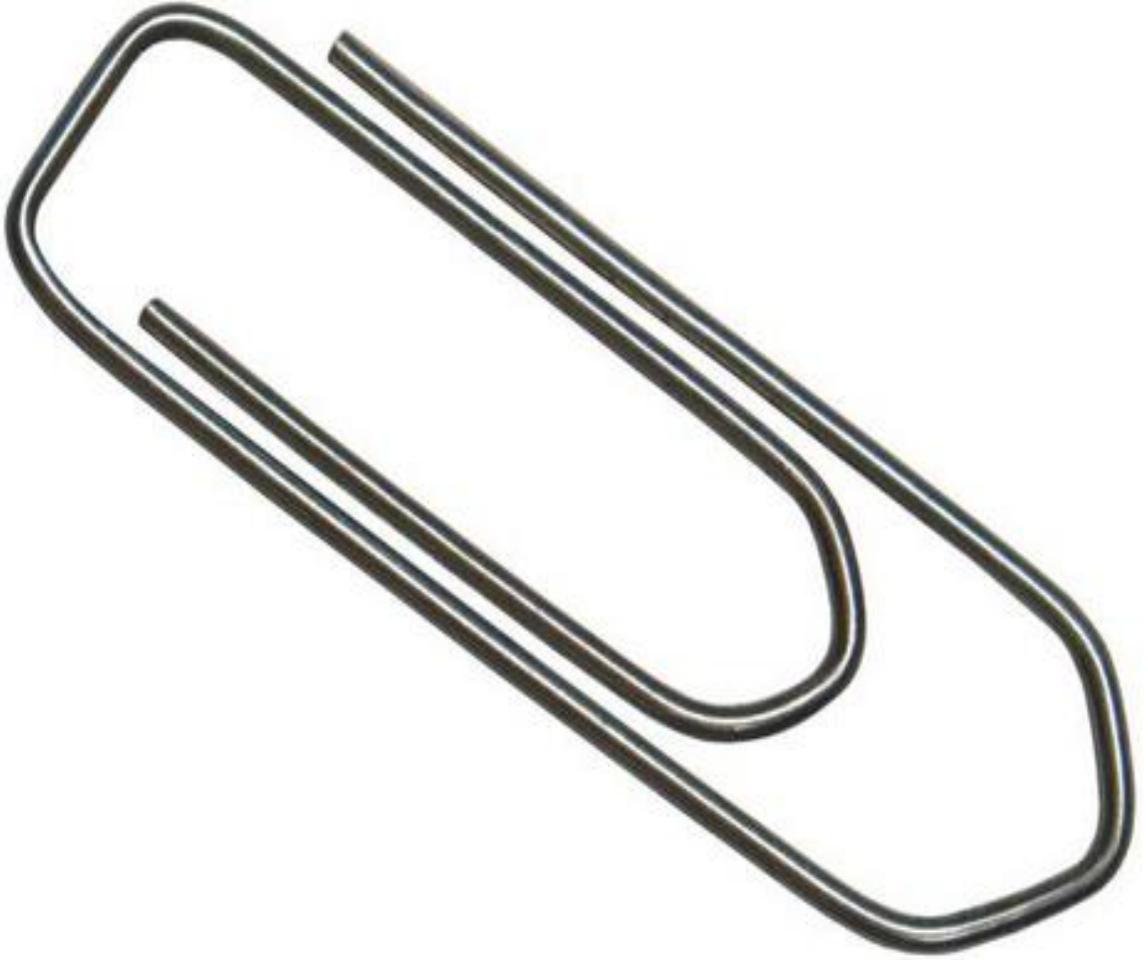
BIBLIOGRAFÍA

1. **Gruhn, Paul and Cheddie, Harry.** *Safety instrumented systems :design, analysis, and justification.* Second Edition. United States of America : ISA-The Instrumentation, Systems, and Automation Society,, 2006. ISBN 978-1556179099.
2. **American Institute Of Chemical Engineers (AIChE) - Center For Chemical Process Safety (CCPS).** *Guidelines For Hazard Evaluation Procedures.* Third Edition. United States of America : Wiley Interscience, 2008. ISBN 978-0816904914.
3. **McDonald, Dave.** *Practical Hazops, Trips And Alarms.* First Edition. United States of America : Newnes Elsevier, 2004. ISBN 9780750662741.
4. —. *Practical Industrial Safety, Risk Assessment, and Shutdown Systems.* First Edition. United States of America : Newnes Elsevier, 2004. ISBN 978-0750658041.
5. **American Institute Of Chemical Engineers (AIChE) - Center For Chemical Process Safety (CCPS).** *Guidelines for Safe Automation of Chemical Processes.* First Edition. United States of America : Wiley Interscience, 1993. ISBN 978-0-8169-0554-6.
6. **American Institute Of Chemical Engineers (AIChE) - Center For Chemical Process Safety (CCPS).** *Guidelines For Safe And Reliable Instrumented Protective Systems.* First Edition. United States of America : Wiley Interscience, 2007. ISBN 978-0471979401.
7. **American Institute Of Chemical Engineers (AIChE) - Center For Chemical Process Safety (CCPS).** *Layer Of Protection Analysis (LOPA): Simplified Process Risk Assessment.* United States of America : Wiley Interscience, 2001. ISBN 978-0816908110.
8. **ANSI/ISA-84.00.01-2004, Parts 1-3 (IEC 61511-1 to 3 Mod).** *Functional Safety: Safety Instrumented Systems for the Process Industry Sector and ISA-84.01-1996. Application of Safety Instrumented Systems for the Process Industries.*
9. **International Electrotechnical Commission (IEC).** *IEC 61508: Functional Safety of Electrical/Electronic/Programmable.* International Standart : s.n., 1999.
10. **(IEC), International Electrotechnical Commission.** *IEC 61508: Functional Safety Explained.* Disponible (en línea) <http://www.iec.ch/functionalsafety/explained/> : s.n., [Consultado: 35-05-2012].



11. **Marszal, Edward M. and Scharpf, Eric W.** *Safety Integrity Level Selection: Systematic Methods Including Layer Of Protection Analysis*. United States of America : International Society Of Instrumentation (ISA), 2002. ISBN 9781556177774.
12. **Machiavelo, Víctor.** *Metodos para la determinacion del SIL objetivo*. México : Disponible (en línea) https://www.redinsafe.com/home1/redinsaf/public_html/victorm/wp-content/uploads/2011/08/Metodos-SIL-Objetivo.pdf, [Consultado 23/05/12].
13. **Meyers, Robert A.** *Handbook of Petroleum Refining Processes*. Third Edition. United States of America : McGraw-Hill, 2004. ISBN 978-0-07-139109-2.
14. **Instituto Mexicano del Petróleo (IMP).** *Manual de Operacion de Planta FCC*.
15. *Determine SIS and SIL using HAZOPS*. **Cruz-Campa, H. Javier and Cruz-Goméz, M. Javier.** s.l. : American Institute of Chemical Engineers (AIChE), March 2010, Process Safety Progress, Vol. Volumen 29, pp. 22-31.
16. **American Institute Of Chemical Engineers (AIChE) - Center For Chemical Process Safety (CCPS).** *Guidelines for Chemical Process Quantitative Analysis*. Second Edition. United States of America : Wiley Interscience, 2000. ISBN 978-0-8169-0720-5.
17. **American Institute Of Chemical Engineers (AIChE) - Center For Chemical Process Safety.** *Guidelines for Process Equipment Reliability Data with Data Tables*. United States of America : Wiley Interscience, 1989. ISBN 978-0816904228.

ANEXOS



ANEXO A: Tablas empleadas en la determinación del SIL

Tabla 1. Calificación de frecuencia (CF) para los eventos iniciales

CF = \log_{10} (F)	Equivalencia en frecuencia (F) con la matriz de riesgos de PEMEX Refinación	Orden de magnitud Frecuencia o Posibilidad	Descripción cualitativa
+1		Una vez por mes	Ocurre frecuente o regularmente
0	1	Una vez por año	Probable que ocurra ocasionalmente /varias veces durante la vida de la planta
-1	2	10% de probabilidad en un año	Probablemente sucederá más de una vez en la vida de la planta
-2	3	1% de probabilidad en un año	No se espera que ocurra, pero podría ocurrir durante la vida de la planta
-3	4	1 en 1000 de probabilidad en un año	Sería una sorpresa que ocurriera durante la vida de la planta
-4		1 en 10,000 de probabilidad en un año	Extremadamente remota, no se espera que sea posible

Tabla 2. Ejemplos de calificaciones para la efectividad de las protecciones

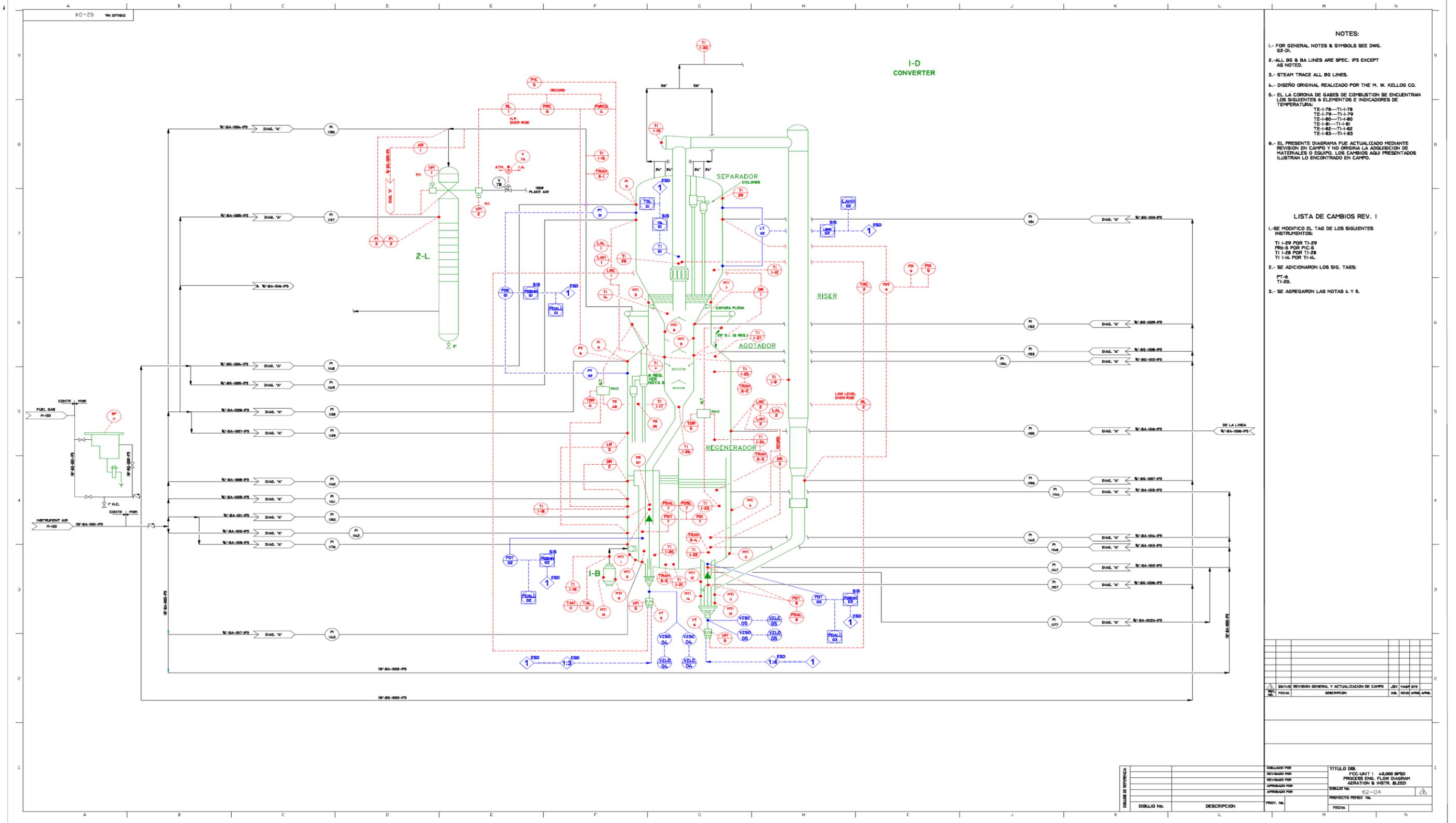
Valor (CE)	Confiabilidad	Probabilidad de falla bajo demanda (PFD)	SIL equivalente	Ejemplos típicos
0	0%	100%		Sin salvaguardas o salvaguardas no diseñadas para el escenario analizado. Operación compleja y con muy poco tiempo para responder.
0.5	68.37%	31.63%		Actuación de un operador frente a la activación de una alarma.
1.0	90%	10%		Operación simple, respuesta con tiempo adecuado (confiabilidad normal del ser humano).
1.5	96.83%	3.162%		
2.0	99%	1%	1	Lazo de control automático sencillo con pruebas funcionales periódicas. Protección pasiva (válvula de relevo).
2.5	99.68%	0.32%	2	Una combinación de protecciones con calificaciones que sumadas den 2.5 o 3 de CE.
3.0	99.9%	0.1%		
3.5	99.96%	0.04%	3	Dos lazos de control automáticos sencillos independientes en el mismo equipo o sección con pruebas funcionales periódicas.
4.0	99.99%	0.01%		

Tabla 3. Calificación de efectividad (CE) de las capas de protección independientes

CE	Confiabilidad en %	Probabilidad de Falla Bajo Demanda (PFD) en %	Número de fallas esperadas en 1000 demandas	NIS Equivalente
0	0	100	1000	
0.5	69.31	31.62	300	
1	90	10	100	
1.5	96.83	3.16	30	
2	99	1	10	1
2.5	99.68	0.3162	3	1
3	99.9	0.1	1	2
3.5	99.96	0.03162	0.001	2
4	99.99	0.01	0.0001	3

Tabla 4. Calificación de efectividad (CE) para equipos, instrumentos y sistemas

Equipos / Instrumentos / Sistemas	Probabilidad de Falla Bajo Demanda			Calificación de Efectividad (CE)		
	Baja	Típica	Alta	Alta	Típica	Baja
Motor AC	2.00E-04	1.39E-01	3.30E-01	3.7	0.9	0.5
Inversor	9.95E-03	2.21E-01	6.32E-01	2.0	0.7	0.2
Equipos / Instrumentos / Sistemas	Probabilidad de Falla Bajo Demanda			Calificación de Efectividad (CE)		
Equipos / Instrumentos / Sistemas	Baja	Típica	Alta	Alta	Típica	Baja
Transformador de potencia	1.00E-03	1.98E-02	6.76E-02	3.0	1.7	1.2
Generador de diesel	7.77E-01	1.00E+00	1.00E+00	0.1	0.0	0.0
Analizador (AR)	4.51E-01	7.25E-01	1.00E+00	0.3	0.14	0.0
Transmisor de flujo neumático	1.78E-02	6.32E-01	9.82E-01	1.7	0.2	0.0
Transmisor de nivel neumático	1.98 E-02	5.51E-01	9.50E-01	1.7	0.3	0.0
Transmisor de presión	1.80 E-03	5.51E-01	9.70E-01	2.7	0.3	0.0
Transmisor de temperatura	1.39 E-02	5.51E-01	9.70E-01	1.9	0.3	0.0
PDT en la industria en general	7.97 E-03	4.32E-01	8.65E-01	2.1	0.4	0.1
PDT en condiciones	2.96 E-02	8.35E-01	1.00E+00	1.5	0.1	0.0
Switch de flujo eléctrico	8.96 E-03	2.74E-01	7.77E-01	2.0	0.6	0.1
Válvula de seguridad (PSV)	2.00 E-03	1.19E-02	3.92E-02	2.7	1.9	1.4
Switch de nivel eléctrico	8.46 E-03	9.95E-03	1.98E-02	2.1	2.0	1.7
Switch de presión eléctrico	3.99 E-03	3.62E-01	8.35E-01	2.4	0.4	0.1
Sistema de polvo contra incendio	2.00E-04	9.95E-03	4.88E-02	3.7	2.0	1.3
Switch de temperatura eléctrico	8.00 E-04	1.98E-02	8.61E-02	3.1	1.7	1.1
Sistema de agua contra incendio	1.00 E-03	7.69E-02	2.95E-01	3.0	1.1	0.5
Detector de flama	3.00 E-04	8.39E-02	1.00E+00	3.5	1.0	0.0
Detector de fuego	1.00 E-04	8.46E-03	2.96E-02	4.0	2.1	1.5
Convertidor I/P	8.96 E-03	4.23E-01	9.18E-01	2.0	0.4	0.0
Válvula actuada por solenoide	5.89E-03	3.30E-01	8.50E-01	2.2	0.5	0.1
Controlador de proceso	1.98 E-02	5.82E-02	9.18E-01	1.7	1.2	0.0
Controlador electrónico	2.96 E-02	7.98E-01	9.99E-01	1.5	0.1	0.0



NOTES:

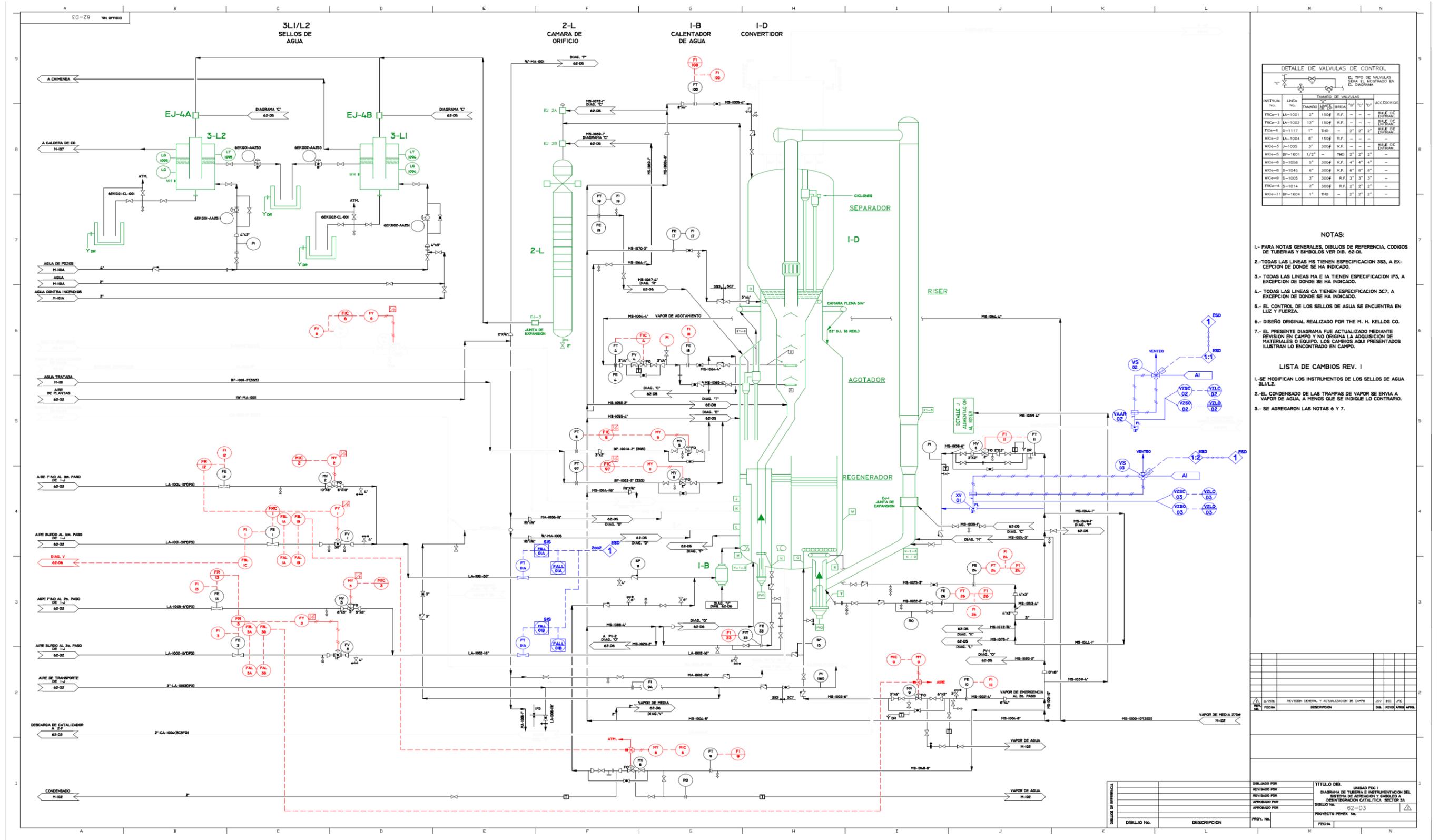
- FOR GENERAL NOTES & SYMBOLS SEE DWG. GE-DI.
- ALL BG & BA LINES ARE SPEC. IPS EXCEPT AS NOTED.
- STEAM TRACE ALL BG LINES.
- DISEÑO ORIGINAL REALIZADO POR THE M. W. KELLOGG CO.
- EL LA CORONA DE GASES DE COMBUSTION SE ENCUENTRAN LOS SIGUIENTES ELEMENTOS E INDICADORES DE TEMPERATURA:
 TE-1-78—TI-1-78
 TE-1-79—TI-1-79
 TE-1-80—TI-1-80
 TE-1-81—TI-1-81
 TE-1-82—TI-1-82
 TE-1-83—TI-1-83
- EL PRESENTE DIAGRAMA FUE ACTUALIZADO MEDIANTE REVISION EN CAMPO Y NO ORIGINA LA ADQUISICION DE MATERIALES O EQUIPO. LOS CAMBIOS AQUI PRESENTADOS ILUSTRAN LO ENCONTRADO EN CAMPO.

LISTA DE CAMBIOS REV. I

- SE MODIFICO EL TAG DE LOS SIGUIENTES INSTRUMENTOS:
 TI 1-29 POR TI-29
 PR-5 POR PIC-5
 TI 1-28 POR TI-28
 TI 1-14 POR TI-14.
- SE ADICIONARON LOS SIG. TAGS:
 PT-6
 TI-20.
- SE AGREGARON LAS NOTAS 4 Y 5.

NO.	FECHA	DESCRIPCION	ELAB.	REVIS.	APRUB.
1		REVISION GENERAL Y ACTUALIZACION DE CAMPO	JSV	HABD	GPE

DIBUJADO POR	DIBUJADO POR	TITULO DEL
REVISADO POR	REVISADO POR	FCC-UNIT 1 48,000 BPSD
APROBADO POR	APROBADO POR	PROCESS ENG. FLOW DIAGRAM
APROBADO POR	APROBADO POR	AERATION & INSTR. BLEED
		DIBUJO NO. 62-D4
		PROYECTO PEREX NO.
		FECHA



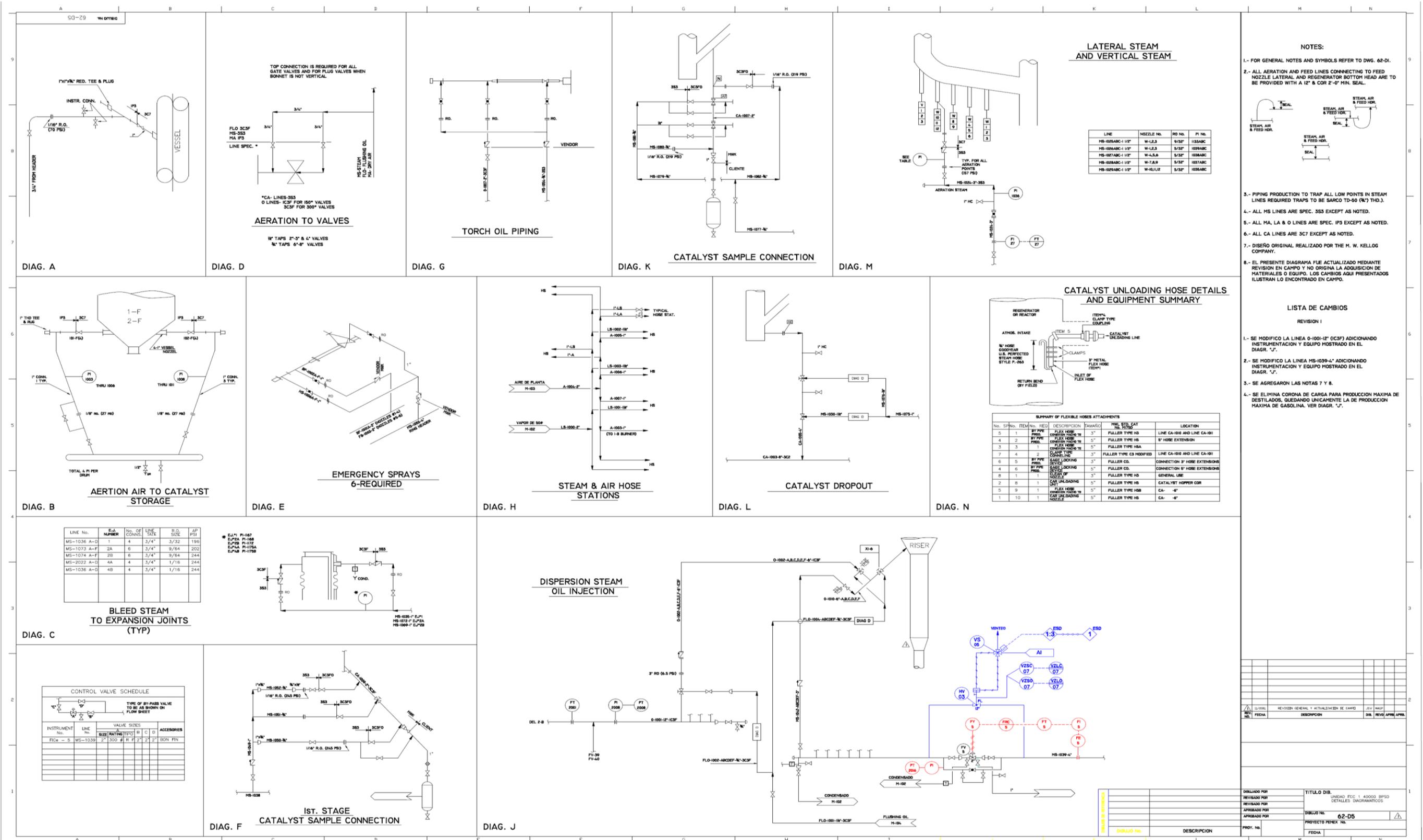
DETALLE DE VALVULAS DE CONTROL

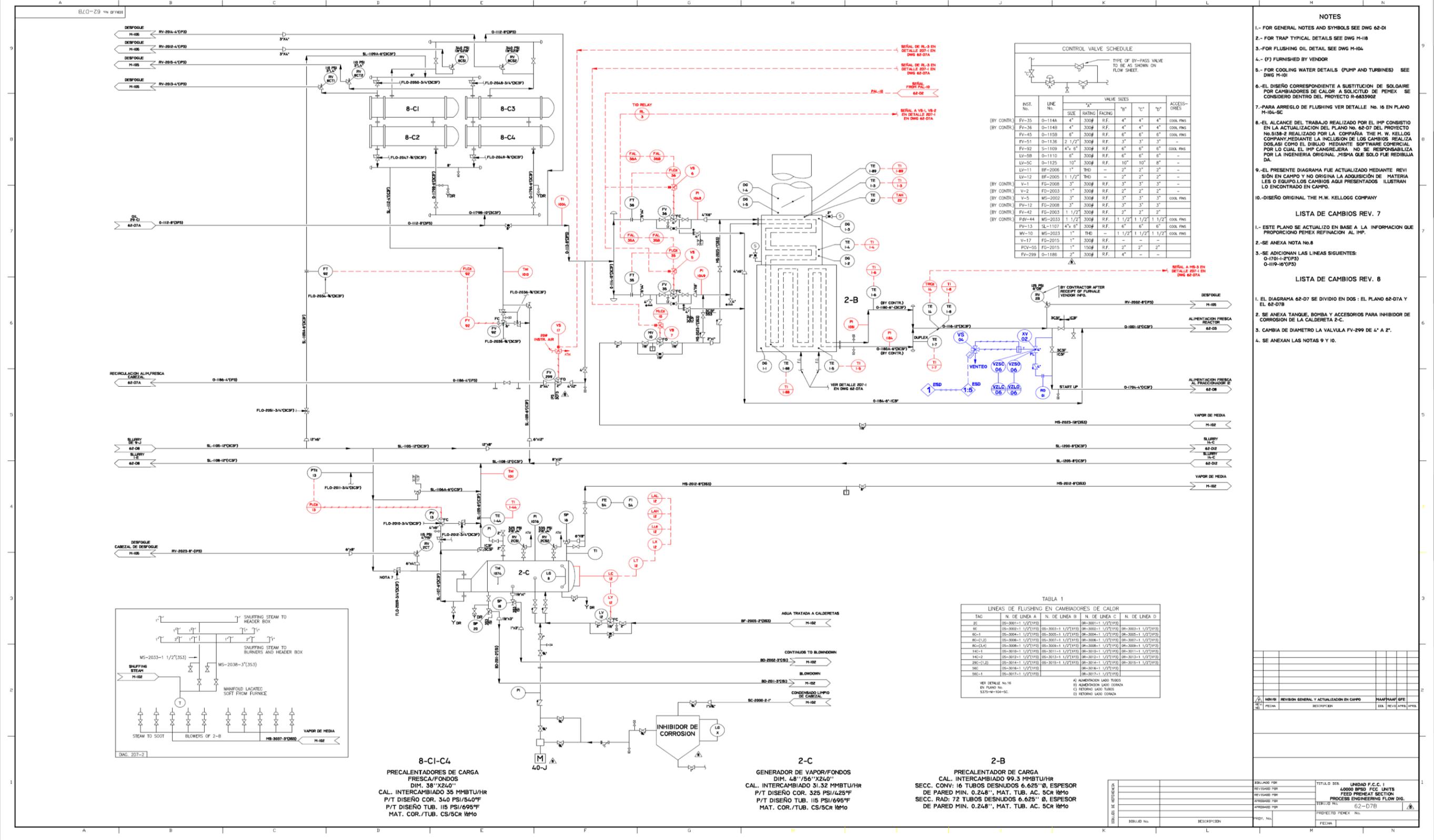
INSTRUM. No.	LINEA No.	TAMANO	TIPO	INDIC.	10"	12"	16"	ACCESORIOS
FRC-1	LA-1001	2"	150#	R.F.	-	-	-	MULE DE EXPANSION
FRC-3	LA-1002	12"	150#	R.F.	-	-	-	MULE DE EXPANSION
FIC-8	S-1117	1"	THD	-	2"	2"	2"	MULE DE EXPANSION
MIC-2	LA-1004	8"	150#	R.F.	-	-	-	MULE DE EXPANSION
MIC-3	LA-1005	3"	300#	R.F.	-	-	-	MULE DE EXPANSION
MIC-5	BF-1001	1/2"	THD	2"	2"	2"	-	-
MIC-6	S-1058	5"	300#	R.F.	4"	4"	4"	-
MIC-8	S-1045	6"	300#	R.F.	6"	6"	6"	-
MIC-9	S-1005	3"	300#	R.F.	3"	3"	3"	-
FRC-4	S-1014	3"	300#	R.F.	2"	2"	2"	-
MIC-11	BF-1004	1"	THD	-	2"	2"	-	-

- NOTAS:
- 1.- PARA NOTAS GENERALES, DIBUJOS DE REFERENCIA, CODIGOS DE TUBERIAS Y SIMBOLOS VER DIB. 62-01.
 - 2.- TODAS LAS LINEAS HS TIENEN ESPECIFICACION 3SS, A EXCEPCION DE DONDE SE HA INDICADO.
 - 3.- TODAS LAS LINEAS HA E IA TIENEN ESPECIFICACION IP3, A EXCEPCION DE DONDE SE HA INDICADO.
 - 4.- TODAS LAS LINEAS CA TIENEN ESPECIFICACION SC7, A EXCEPCION DE DONDE SE HA INDICADO.
 - 5.- EL CONTROL DE LOS SELLOS DE AGUA SE ENCUENTRA EN LUZ Y FUERZA.
 - 6.- DISEÑO ORIGINAL REALIZADO POR THE M. H. KELLOS CO.
 - 7.- EL PRESENTE DIAGRAMA FUE ACTUALIZADO MEDIANTE REVISION EN CAMPO Y NO ORIGINAL LA ADQUISICION DE MATERIALES O EQUIPO. LOS CAMBIOS AQUÍ PRESENTADOS ILUSTRAN LO ENCONTRADO EN CAMPO.

- LISTA DE CAMBIOS REV. I
- 1.- SE MODIFICAN LOS INSTRUMENTOS DE LOS SELLOS DE AGUA 3L1/L2.
 - 2.- EL CONDENSADO DE LAS TRAMPAS DE VAPOR SE ENVIA A VAPOR DE AGUA, A MENOS QUE SE INDIQUE LO CONTRARIO.
 - 3.- SE AGREGAN LAS NOTAS 6 Y 7.

REVISOR	FECHA	DESCRIPCION	DM	REVISOR	FECHA	DESCRIPCION





NOTES

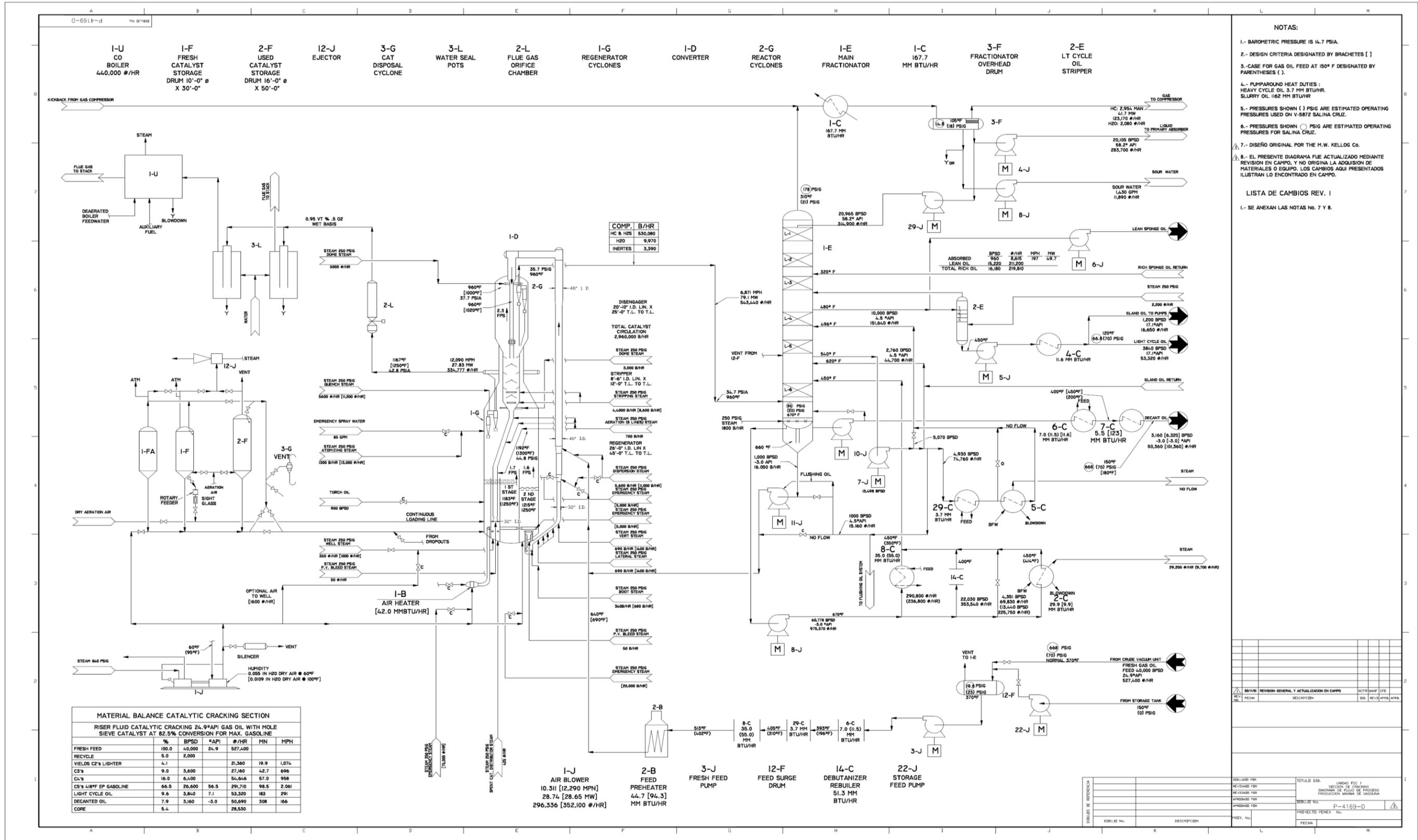
- FOR GENERAL NOTES AND SYMBOLS SEE DWG 62-D1
- FOR TRAP TYPICAL DETAILS SEE DWG M-18
- FOR FLUSHING OIL DETAIL SEE DWG M-104
- (F) FURNISHED BY VENDOR
- FOR COOLING WATER DETAILS (PUMP AND TURBINES) SEE DWG M-81
- EL DISEÑO CORRESPONDIENTE A SUSTITUCIÓN DE SOLDADURA POR CAMBIADORES DE CALOR A SOLICITUD DE PEMEX SE CONSIDERÓ DENTRO DEL PROYECTO R-6835902
- PARA ARREGLO DE FLUSHING VER DETALLE No. 16 EN PLANO M-104-SC
- EL ALCANCE DEL TRABAJO REALIZADO POR EL IMP CONSISTE EN LA ACTUALIZACIÓN DEL PLANO No. 62-D7 DEL PROYECTO No. R-6835902 REALIZADO POR LA COMPAÑÍA THE M. W. KELLOGG COMPANY, MEDIANTE LA INCLUSIÓN DE LOS CAMBIOS REALIZADOS COMO EL DIBUJO MEDIANTE SOFTWARE COMERCIAL POR LO CUAL EL IMP CARGUERA NO SE RESPONSABILIZA POR LA INGENIERÍA ORIGINAL, MISHA QUE SOLO FUE REDIBUJADA.
- EL PRESENTE DIAGRAMA FUE ACTUALIZADO MEDIANTE REVISIÓN EN CAMPO Y NO ORIGINAL LA ADQUISICIÓN DE MATERIALES O EQUIPOS. LOS CAMBIOS AQUÍ PRESENTADOS ILUSTRAN LO ENCONTRADO EN CAMPO.
- DISEÑO ORIGINAL THE M.W. KELLOGG COMPANY

LISTA DE CAMBIOS REV. 7

- ESTE PLANO SE ACTUALIZÓ EN BASE A LA INFORMACIÓN QUE PROPORCIONÓ PEMEX REFINACIÓN AL IMP.
- SE ANEXA NOTA No. 8
- SE ADICIONAN LAS LINEAS SIGUIENTES:
O-1701-1-2"(10)
O-1119-16"(10)

LISTA DE CAMBIOS REV. 8

- EL DIAGRAMA 62-D7 SE DIVIDIO EN DOS: EL PLANO 62-D7A Y EL 62-D7B
- SE ANEXA TANQUE, BOMBA Y ACCESORIOS PARA INHIBIDOR DE CORROSIÓN DE LA CALDERETA 2-C.
- CAMBIA DE DIAMETRO LA VALVULA FV-299 DE 4" A 2".
- SE ANEXAN LAS NOTAS 9 Y 10.



NOTAS:

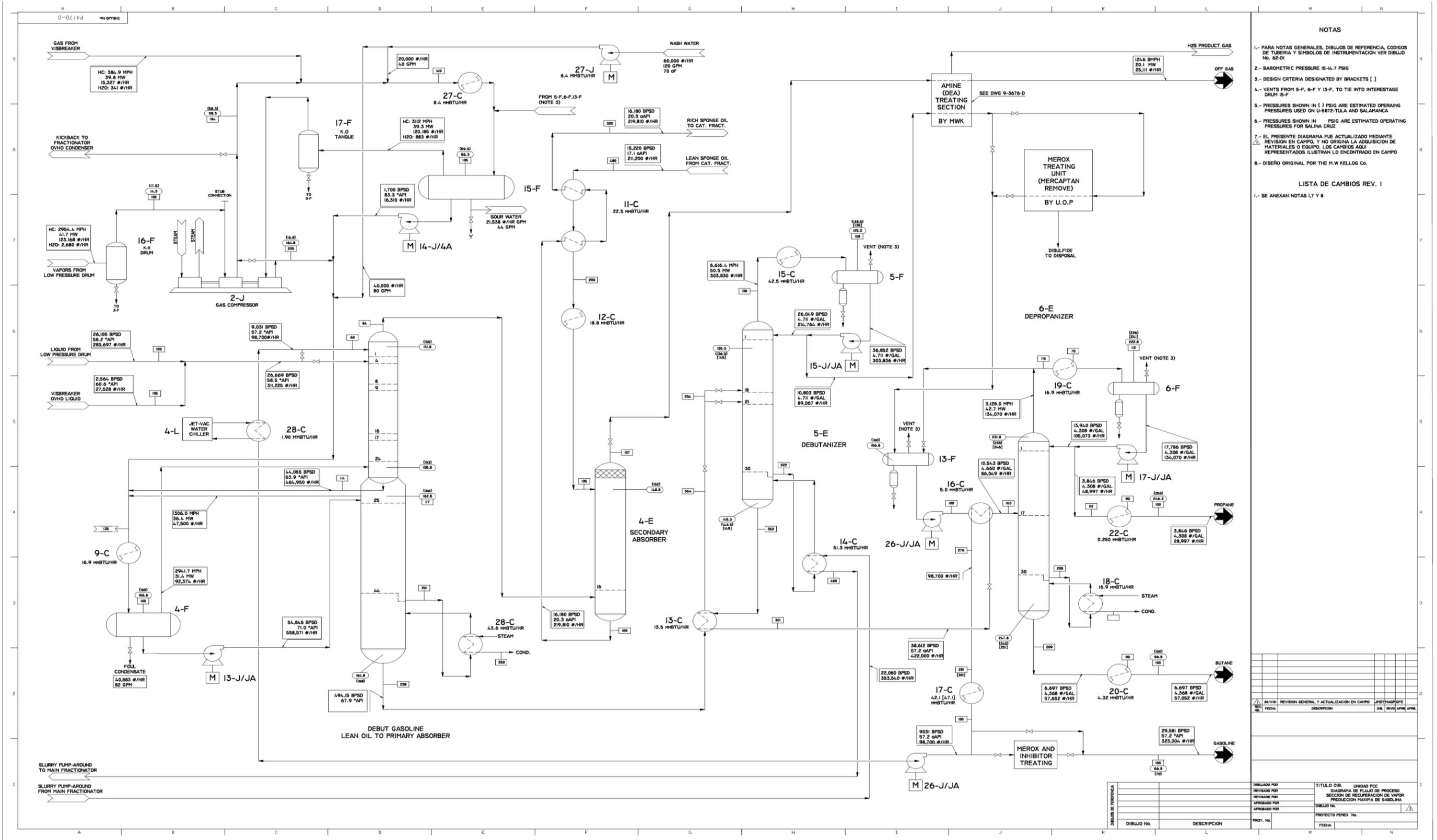
- 1.- BAROMETRIC PRESSURE IS 14.7 PSIA.
- 2.- DESIGN CRITERIA DESIGNATED BY BRACKETES ()
- 3.- CASE FOR GAS OIL FEED AT 150° F DESIGNATED BY PARENTHESES ().
- 4.- PUMPAROUND HEAT DUTIES :
HEAVY CYCLE OIL 3.7 MM BTU/HR.
SLURRY OIL 162 MM BTU/HR
- 5.- PRESSURES SHOWN () PSIG ARE ESTIMATED OPERATING PRESSURES USED ON V-5872 SALINA CRUZ.
- 6.- PRESSURES SHOWN () PSIG ARE ESTIMATED OPERATING PRESSURES FOR SALINA CRUZ.
- 7.- DISEÑO ORIGINAL POR THE M.W. KELLOGG CO.
- 8.- EL PRESENTE DIAGRAMA FUE ACTUALIZADO MEDIANTE REVISION EN CAMPO, Y NO ORIGINAL LA ADQUISICION DE MATERIALES O EQUIPO. LOS CAMBIOS ADJQI PRESENTADOS ILUSTRAN LO ENCONTRADO EN CAMPO.

LISTA DE CAMBIOS REV. 1

1.- SE ANEXAN LAS NOTAS No. 7 Y 8.



ANEXOS: Anexo C. DFP's de una planta FCC



- NOTAS**
- 1.- PARA NOTAS GENERALES, DIBUJOS DE REFERENCIA, CODIGOS DE TUBERIA Y SIMBOLOS DE INSTRUMENTACION VER DIBUJO NO. 62-DI
 - 2.- BAROMETRIC PRESSURE IS-14.7 PSIG
 - 3.- DESIGN CRITERIA DESIGNATED BY BRACKETS []
 - 4.- VENTS FROM 5-F, 6-F Y 15-F, TO THE INTO INTERESTAGE DRUM IS-F
 - 5.- PRESSURES SHOWN IN () PSIG ARE ESTIMATED OPERATING PRESSURES USED ON U-5872-TULA AND SALAMANCA
 - 6.- PRESSURES SHOWN IN PSIG ARE ESTIMATED OPERATING PRESSURES FOR SALINA CRUZ
 - 7.- EL PRESENTE DIAGRAMA FUE ACTUALIZADO MEDIANTE REVISION EN CAMPO, Y NO ORIGINA LA ADOSICION DE MATERIALES O EQUIPO. LOS CAMBIOS ADU REPRESENTADOS ILUSTRAN LO ENCONTRADO EN CAMPO
 - 8.- DISEÑO ORIGINAL FOR THE M.W KELLOG Co.

LISTA DE CAMBIOS REV. I
1.- SE ANEXAN NOTAS I,7 Y 8

NO.	FECHA	DESCRIPCION	DR.	REVISOR	APR.