TRABAJO ESPECIAL DE GRADO

DETERMINACIÓN DE UN SISTEMA INSTRUMENTADO DE SEGURIDAD (SIS) Y SU NIVEL DE INTEGRIDAD DE SEGURIDAD (SIL)

Prof. Guía: Ing. Tamara Pérez

Tutor Industrial: Ing. Rosa Alvarado

Presentado ante la Ilustre
Universidad Central de Venezuela
Por el Bachiller Rodríguez P., Oswaldo A.
para optar por el título de Ingeniero Electricista

Caracas, 2005

CONSTANCIA DE APROBACIÓN

Caracas, 02 de junio de 2005

Los abajo firmantes, miembros del Jurado designado por el Consejo de Escuela de Ingeniería Eléctrica, para evaluar el Trabajo Especial de Grado presentado por el Bachiller Oswaldo A. Rodríguez P., titulado:

"DETERMINACIÓN DE UN SISTEMA INSTRUMENTADO DE SEGURIDAD (SIS) Y SU NIVEL DE INTEGRIDAD DE SEGURIDAD (SIL) "

Consideran que el mismo cumple con los requisitos exigidos por el plan de estudios conducente al Título de Ingeniero Electricista en la mención de Electrónica, y sin que ello signifique que se hacen solidarios con las ideas expuestas por el autor, lo declaran APROBADO.

Prof. Panayotis Tremante
Jurado

Prof. José Alonso
Jurado

Prof. Tamara Pérez
Prof. Guía

DEDICATORIA

A mi Madre, mis hermanos Tomás y Rafael, mi tía Belén, mi abuela Teresa, mi tío Tico y toda mi familia.

AGRADECIMIENTOS

Quiero agradecer al Departamento de Instrumentación de VEPICA por la oportunidad brindada y por todo el apoyo prestado en la realización de este trabajo. Quiero agradecer especialmente a la Ing. Rosa Alvarado, al Ing. Juan Camafeita y a la Ing. María Del Valle López por su valiosa ayuda y apoyo.

Gracias a la Ing. Lilia González por todo su orientación en las etapas iniciales del desarrollo de este trabajo.

Gracias a la profesora Tamara Pérez por sus acertadas correcciones y sugerencias.

Gracias a mis amigos de la Escuela de Ingeniería Eléctrica: Rafael Romero, Juan Colmenares, Stiven Frenández, Carlos Ibarras, Andrés De Andrade, Darihelen Montilla, Tulio García, Julio Torralba, Juan Galeno, Ilwin Ruiz, Julide Flores, Ivan Márquez, Jaime Rodrigues, José Benavides y Osman Tovar por su amistad, compañerismo y apoyo durante el desarrollo de mi carrera universitaria.

Gracias a Anaís Álvarez por su comprensión y apoyo incondicional.

Mil gracias a mi Madre, mis hermanos Tomás y Rafael, mis tíos Belén y Tico, mi abuela Teresa y mis padrinos Elvira y Pedro y toda mi familia por su comprensión, apoyo y amor durante toda mi vida.

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

Pág.

SIMBOLOS Y ABREVIATURAS

ANSI. Instituto de Estándares Nacionales Americanos (American National Standards Institute).

API. Instituto de Petróleo Americano (American Petroleum Institute)

BHD. Bitumen húmedo diluido.

BPCS. Sistema de Control Básico del Proceso (Basic process control system).

BPSD. Barriles estándar por día.

DC. Cobertura de diagnóstico (Diagnostic coverage).

dec. Decrementando.

DSDS. Sistema de Distribución y Almacenamiento de Diluente.

RRF. Factor de reducción de riesgo (Risk Reduction Factor).

FTA. Análisis de árbol de fallas (Fault tree analysis).

FMEDA. Análisis de Diagnóstico, Efectos y Modos de Falla (Failure Modes, Effects and Diagnostic Analysis).

HAZOP. Análisis de Peligro y Operabilidad (Hazard and Operability).

HFT. Tolerancia de falla de hardware (Hardware fault tolerance).

IEC. Comisión Electrotécnica Internacional (International Electrotechnical Commission).

IPL. Capas Independientes de Protección.

ISA. Sociedad de Instrumentación, Automatización y Sistemas **(**The Instrumentation, Systems and Automation Society).

ISO. Organización Internacional de Estandarización (International Organization for Standardization)

inc. Incrementando.

LACT. Sistema de medición reflujo de transferencia de custodia.

MBbls. Miles de Barriles.

MMSCFD. Millones de pies cúbicos estándar por día.

MPE-3. Estación de Flujo.

OREDA. Datos de Confiabilidad Costa fuera (Offshore Reliability Data).

PFD. Probabilidad de falla en demanda (Probability of failure on demand)

PFDavg. Probabilidad de falla en demanda promedio (Average probability of failure on demand)

SFF. Fracción de falla segura (Safe failure fraction)

SIF. Función Instrumentada de Seguridad (Safety instrumented function)

SIL. Nivel de integridad de seguridad (Safety integrity level)

SIS. Sistema Instrumentado de Seguridad (Safety instrumented system)

TÜV. Asociación de Vigilancia Técnica (Technischer Uberwachungs-Verein)

λ : tasa de falla

λd : tasa de falla peligrosa

λdd : tasa de falla peligrosa detectada

λdu : tasa de falla peligrosa no detectada

λs : tasa de falla segura

λsd : tasa de falla segura detectada

λsu : tasa de falla segura no detectada

Rodríguez P., Oswaldo A.

DETERMINACIÓN DE UN SISTEMA INSTRUMENTADO DE SEGURIDAD (SIS) Y SU NIVEL DE INTEGRIDAD DE SEGURIDAD (SIL)

Prof. Guía: Ing. Tamara Pérez. **Tutor Industrial:** Ing. Rosa Alvarado. Tesis. Caracas, UCV. Facultad de Ingeniería. Escuela de Ingeniería Eléctrica. Ingeniero Electricista. Opción: Electrónica, Computación y Control. Institución: VEPICA, 2005. 115h. + anexos.

Palabras Claves: Sistemas Instrumentados de Seguridad, Nivel de Integridad de Seguridad.

Resumen. Se realiza el cálculo del Nivel de Integridad de Seguridad (SIL), de forma cualitativa y cuantitativa, de las facilidades de proceso en una planta de extracción de crudo pesado y la planta de tratamiento asociada de acondicionamiento del producto para el transporte, tomando como referencia la producción de petróleo extra pesado bajo la patente de Orimulsion® en Jose. Para el cálculo cualitativo se emplea el método de Gráfica de Riesgo y para el cálculo cuantitativo se emplea el método Semi-Cuantitativo, ambos contemplados en la norma ANSI/ISA 84.00.01-2004. Se analizan los resultados obtenidos por ambos métodos y se toman como válidos los resultados cuantitativos gracias a sus características de objetividad y confiabilidad. Se realiza la especificación y diseño del Sistema Instrumentado de Seguridad (SIS) que cumpla los requerimientos del SIL obtenido del cálculo cuantitativo. Para el diseño del SIS se desarrolla un programa que emplea un algoritmo genético para determinar la mejor configuración de cada una de las Funciones Instrumentadas de Seguridad (SIF) que conforman el SIS en términos de menor probabilidad de falla en demanda promedio (PFD_{AVG}) y de menor complejidad en la arquitectura de votación.

INTRODUCCIÓN

El presente trabajo realiza y describe la determinación del Nivel de Integridad de Seguridad (SIL) de forma cualitativa y cuantitativa de una planta de extracción de crudo pesado, incluyendo las facilidades de proceso y de tratamiento inicial asociada, tomando como referencia la producción de petróleo extra pesado bajo la patente de Orimulsion® en Jose. Con el resultado obtenido se realizan las especificaciones y diseño del Sistema Instrumentado de Seguridad (SIS) requerido.

Este trabajo se desarrolla debido a los requerimientos de las Empresas Productoras de Petróleo clientes de VEPICA de realizar la determinación del SIL y el posterior diseño del SIS, dentro de las actividades de Ingeniería contratadas en el desarrollo de sus diferentes proyectos.

El trabajo está estructurado de la siguiente manera:

En el capítulo I se plantean los objetivos y justificación del trabajo, mientras que en el capítulo II, correspondiente al marco teórico, se presentan todos los conceptos, definiciones y métodos relacionados con Sistemas Instrumentados de Seguridad y Niveles de Integridad de Seguridad. En el capítulo III se describe la planta y la instrumentación presente en el proceso al cual se le determinó el Nivel de Integridad de Seguridad. En el capítulo IV se realiza la determinación del SIL de forma cualitativa y cuantitativa. Para el cálculo cualitativo se emplea el método de Gráfica de Riesgo y para el cálculo cuantitativo se emplea el método Semi-Cuantitativo ambos contemplados en la norma ANSI/ISA 84.00.01-2004. Finalmente en el capítulo V se establecen las pautas de diseño, configuración y arquitectura del Sistema Instrumentado de Seguridad. Para la etapa del diseño del SIS se desarrolló una aplicación en Microsoft Access la cual, empleando un algoritmo genético, determina la mejor configuración de cada una de las Funciones Instrumentadas de Seguridad (SIF) que conforman el SIS en términos de menor probabilidad de falla en demanda promedio (PFD_{AVG}) y de menor complejidad en la arquitectura de votación.

CAPÍTULO I

PLANTAMIENTO DEL PROBLEMA

Debido a los cambios positivos en las innovaciones tecnológicas, los Sistemas de control han variado en su diseño, configuración y funcionalidad. En la búsqueda de obtener mejores resultados en la confiabilidad de los sistemas de control, se han desarrollado nuevos términos y tecnologías asociados a ellos que permiten tener diseños de gran confiabilidad (grado de certeza de operación exitosa), sin falla.

La industria de procesos moderna tiende a ser técnicamente muy compleja, además de involucrar energías y substancias que tienen el potencial de ocasionar serios daños a personas, instalaciones y propiedades durante la ocurrencia de un accidente.

En 1996, en respuesta al incremento del número de accidentes industriales, la ISA (The Instrumentation, Systems and Automation Society), estableció un estándar para manejar la clasificación de los Sistemas Instrumentados de Seguridad ("Safety Instrumented System" - SIS) para los procesos industriales dentro de los Estados Unidos de América. Este estándar, ISA S84.01 (actualmente ANSI/ISA 84.00.01-2004), introduce el concepto de Niveles de Integridad de Seguridad ("Safety Integrity Level" - SIL). En consecuencia, la Comisión Electrotécnica Internacional ("International Electrotechnical Comisión" - IEC) estableció un estándar industrial neutral, IEC 61508, para ayudar a cuantificar la seguridad en sistemas electrónicos programables relacionados a la seguridad. Posteriormente la IEC estableció el estándar IEC 61511 específico para Sistemas Instrumentados de Seguridad en el sector de la industria de procesos.

El estándar IEC 61508 define seguridad como "libertad de riesgo inaceptable". En otras palabras, la seguridad absoluta nunca puede ser alcanzada, más bien el riesgo sólo se puede reducir hasta un nivel aceptable.

Existen diversas soluciones para alcanzar la reducción de riesgo requerida. Una de dichas soluciones es el uso de un SIS. Los Sistemas Instrumentados de Seguridad son muy importantes en la administración de riesgos debido a que reducen o evitan las consecuencias de los peligros al personal, al ambiente e instalaciones. Los riesgos deben prevenirse como un objetivo inicial del diseño y deben ser mitigados para reducir el riesgo al personal. Por lo tanto, los Sistemas Instrumentados de Seguridad cumplen una función primordial evitando los eventos de riesgo o minimizando la severidad de las consecuencias al personal, medio ambiente e instalaciones.

Los Sistemas Instrumentados de Seguridad y su Nivel de Integridad de Seguridad, han revolucionado los sistemas de protección de las plantas industriales, haciéndolos más robustos y con una disponibilidad mayor a la de sus predecesores, garantizando así la seguridad de la instalación. Estas condiciones han traído como consecuencia la implementación de una serie de métodos de análisis para cálculo del Nivel de Integridad de Seguridad que sirve de base para el diseño del Sistema de Protección. La selección del método para una aplicación específica depende de diversos factores, tales como: la complejidad de la aplicación, la naturaleza del riesgo y de la reducción de riesgo requerida y de la experiencia y habilidades de las personas disponibles para realizar el estudio.

Debido a los requerimientos de confiabilidad y seguridad planteados en las normas internacionales antes mencionadas (ANSI/ISA 84.00.01-2004, IEC 61508, IEC 61511), cualquier proyecto de ingeniería, procura y construcción dirigido a la industria petrolera y petroquímica contempla el diseño de su Sistema Instrumentado de Seguridad asociado y el cálculo de su respectivo Nivel de Integridad de Seguridad .

La empresa VEPICA desde su creación en 1972 se ha convertido en una de las empresas líderes en la rama de consultoría de ingeniería en Venezuela, realizando numerosos proyectos de gran envergadura para la industria petrolera a nivel nacional, estableciendo asociaciones con empresas internacionales como: FISH, ABB, Kellogs,

JPC, etc. y recientemente a nivel internacional gracias a su asociación con WOOD Group, Empresa internacional especializada en Operación y mantenimiento de instalaciones de producción petroleras.

Actualmente la empresa VEPICA para la determinación de Sistemas Instrumentados de Seguridad (SIS) y su Nivel de Integridad de Seguridad (SIL) en el desarrollo de proyectos de Ingenierías Básicas y de Detalle subcontrata a Empresas especializadas en el área, lo cual trae como consecuencia el incremento del costo de la oferta de un proyecto y posibles inconsistencias en criterios de diseño entre las dos partes.

1.1. Justificación

Este trabajo surge por el requerimiento de desarrollar la determinación del Nivel de Integridad de Seguridad (SIL) requerido de forma cualitativa y cuantitativa, y el posterior diseño del Sistema Instrumentado de Seguridad (SIS) que cumpla el SIL determinado, dentro de las actividades de Ingeniería contratadas por parte de las diferentes Empresas Productoras de Petróleo clientes de VEPICA (PDVSA, Asociaciones estratégicas como AMERIVEN, SINCOR, PETROZUATA y otros).

El presente trabajo de grado se justifica por lo siguiente:

- Todos los proyectos de ingeniería relacionados con la industria petrolera a nivel mundial están solicitando entre sus actividades de ingeniería la determinación del SIL y el posterior diseño del SIS.
- Al realizar la determinación del SIL y diseño del SIS dentro de VEPICA, se ahorran gastos administrativos y se mejora la eficiencia en la implementación del ciclo de vida de seguridad de un proyecto.

1.2. Alcance

El alcance de este trabajo de grado abarca la determinación del Nivel de Integridad de Seguridad (SIL) de forma cualitativa y cuantitativa, y el diseño del Sistema Instrumentado de Seguridad (SIS) que cumpla con el SIL requerido para las

facilidades de proceso de una planta de extracción de crudo pesado y su planta de tratamiento asociada.

La determinación del SIL se basa principalmente en el estudio de los lazos críticos del proceso.

El estudio abarca el proceso y los equipos que existirán durante la fase de operación comercial de la instalación. Este estudio no contempla los equipos de uso temporal.

En el diseño del Sistema Instrumentado de Seguridad (SIS), se toman en cuenta principalmente factores de confiabilidad y disponibilidad de los equipos a emplear.

1.3. Limitaciones

En el desarrollo de este trabajo se emplearon versiones demo de los softwares especializados necesarios para realizar el cálculo cuantitativo del Nivel de Integridad de Seguridad. Estos demos presentan limitaciones en prestaciones y tiempo de utilización.

1.5. Objetivos

1.5.1. Objetivo General

Determinar un Sistema Instrumentado de Seguridad ("Safety Instrumented System" - SIS) y su Nivel de Integridad de Seguridad ("Safety Integrity Level" - SIL), con el fin de alcanzar un nivel de confiabilidad que permita la operación segura, así como un nivel de riesgos aceptable para los trabajadores y terceros en las facilidades de proceso en una planta de extracción de crudo pesado y la planta de tratamiento asociada que permite acondicionar el producto para el transporte, tomando como referencia la producción de petróleo extra pesado bajo la patente de Orimulsion® en Jose.

1.5.2. Objetivos Específicos

- Determinar del Riesgo Meta, de acuerdo a IR-P-02 y condiciones de la instalación para el proyecto objeto del estudio. Se tomará como referencia la producción de petróleo extra pesado bajo la patente de Orimulsion® en Jose.
- Identificar Peligros, Escenarios, Capas Independientes de Protección y Lazos Críticos.
- Realizar el estudio Cuantitativo/Cualitativo de datos para la determinación del SIL por ambos procedimientos.
- Especificar el Sistema Instrumentado de Seguridad para cubrir los requerimientos exigidos por el número SIL resultante de los cálculos.

1.6. Metodología

En la realización del presente trabajo de grado se siguió la metodología que se plantea a continuación:

Levantamiento de Información

Se estudió la bibliografía disponible y las diferentes normas aplicables al tema, las cuales se mencionan en la sección de Bibliografía del presente documento. Gracias al uso de Internet se encontró información actualizada y de gran utilidad para el desarrollo de este trabajo. Las principales páginas consultadas también se mencionan en la Bibliografía.

Para la obtención de las tasas de falla de equipos se emplearon extractos de la base de datos OREDA 1997 y la norma PDVSA IR-S-02.

Familiarización con Documentos del Proyecto

Para realizar estudio de la determinación del SIL se estudiaron los siguientes documentos:

- Diagramas de Tubería e Instrumentación (PI&D's).
- Diagramas de Flujo de Procesos.
- Bases de Diseño del Proceso.
- Filosofía de Operación y Control

Estudio del SIL

Se determinó el SIL del proyecto de forma cualitativa empleando el método de Gráfico de Riesgo contemplado en la norma ANSI/ISA 84.00.01-2004. Se determinó el SIL del proyecto de forma cuantitativa empleando el método Semi-Cuantitativo contemplado en la norma ANSI/ISA 84.00.01-2004.

Diseño del SIS

Se elaboró la especificación y verificación del Sistema Instrumentado de Seguridad para cubrir los requerimientos exigidos por el número SIL resultante de los cálculos.

CAPÍTULO II

MARCO TEÓRICO

2.1. Peligro

El peligro se define como aquella "condición química o física de un sistema, planta o proceso que tiene el potencial para causar daño a las personas, la propiedad y/o el ambiente. Se debe entender como la combinación de una sustancia peligrosa y un ambiente operacional, tal que la ocurrencia de ciertos eventos no deseados, pueden resultar en un accidente". [1]

2.2. Identificación de Peligros

Como su nombre lo indica la identificación de peligros pretende encontrar las condiciones de daño potencial presentes en una planta o proceso. La identificación de peligros es un paso crítico en el Análisis Cuantitativo de Riesgos, por cuanto un peligro omitido es un peligro no analizado. La identificación de peligros se debe efectuar lo antes posible en el diseño y construcción de una planta y/o proceso de acuerdo a la tabla 2.1 donde se muestra el estimado de costo en la detección y corrección de peligros según el estado del diseño

Tabla 2.1. Costo estimado en la detección y corrección de peligros

Etapa	Costo ($)
A nivel de Ingeniería Conceptual	1
A nivel de Ingeniería Básica	10
A nivel de Ingeniería de Detalle	100
En Construcción	1000
Después de la planta construida	10.000
Después de accidente por no detectar y corregir el peligro	1.000.000

Algunos de los métodos y técnicas desarrolladas mundialmente para la identificación de peligros son:

- Análisis Preliminar de Peligros (PHA)
- Método “Que pasaría si....?”
- Índices Dow–Mond
- Estudios de Peligros y Operabilidad (HAZOP)
- Modos de fallas, efectos y análisis de criticidad (FMECA)
- Análisis de Árbol de Fallas (FTA)
- Análisis de Árbol de Eventos (ETA)
- Análisis de Error Humano
- Evaluaciones Técnicas de Seguridad Industrial[2]

En el presente trabajo se emplearon los métodos de Análisis de Árbol de Fallas (FTA) y Análisis de Árbol de Eventos (ETA), los cuales se describen en el anexo 1 y 2 respectivamente.

2.3. Riesgo

El riesgo referido a un evento peligroso, se define como la contingencia de sus consecuencias (o daño). Tiene carácter cuantitativo, siendo su expresión más generalizada el producto de la probabilidad de ocurrencia del evento peligroso considerado (absoluta o referida a un período de tiempo determinado) por las consecuencias esperadas. [3]

2.3.1. Cuantificación del Riesgo.

Las medidas más comunes de cuantificación del riesgo son las llamadas riesgo individual y riesgo social, que combinan la información de posibilidad y magnitud de las perdidas o lesiones provenientes de un peligro. La medida del riesgo individual considera el riesgo de un ser humano que pueda estar en cualquier punto de la zona

de efectos del accidente y la medida del riesgo social considera el riesgo a las poblaciones que están en tales zonas de efectos.

2.3.2. Riesgo Individual

Puede definirse riesgo individual como el riesgo a una persona en la proximidad de un peligro, considerando la naturaleza de la lesión al individuo, la posibilidad de que la misma ocurra y el período de tiempo en que puede ocurrir. Aún cuando las lesiones son de gran preocupación hay limitada información disponible sobre el grado de las lesiones, por tanto, los análisis cuantitativos de riesgo frecuentemente estiman el riesgo de lesiones irreversibles o fatalidades para las cuales existen más estadísticas registradas. El riesgo individual puede ser estimado para los individuos más expuestos, para grupos de individuos en lugares determinados o para un individuo promedio en una zona de efectos.

El riesgo individual para un nivel específico de daño se calcula tomando en consideración las siguientes variables:

- La frecuencia del evento.
- La probabilidad de que el efecto del evento llegue a la ubicación específica. Esto incluye las variables climáticas y de dirección del viento, con el consiguiente cambio de dispersión.
- La probabilidad de que una persona esté en el lugar.
- La probabilidad de que una persona llegue a un refugio o escape de una atmósfera peligrosa.

2.3.3. Riesgo Social

El riesgo social es una relación entre la frecuencia y el número de personas de una población sometido a un nivel específico de lesiones y daños debido a la ocurrencia de un accidente. En caso de accidentes mayores con potencial para afectar a grupos de personas, el riesgo social constituye una medida del riesgo a tal grupo de personas y es expresado frecuentemente en términos de distribución de frecuencia de eventos de resultantes múltiples. Sin embargo, el riesgo social también puede ser expresado

en términos similares a los riesgos individuales. El cálculo del riesgo social requiere la misma información de frecuencia y consecuencias que el riesgo individual, pero adicionalmente requiere una definición de la población en riesgo alrededor de la instalación. Esta definición puede incluir el tipo de población (por ejemplo: residencial, industrial, escolar, etc.), la posibilidad de personas presentes o factores de mitigación existentes.

El riesgo social para un nivel específico de daño se calcula tomando en consideración los siguientes factores:

- Frecuencia del evento.
- La probabilidad de que el evento llegue a una ubicación específica, considerando variables climáticas y la dirección del viento, con el consiguiente cambio de dispersión.
- La probabilidad de que una o varias personas estén en el lugar.
- La probabilidad de que una o varias personas lleguen a un refugio o escapen de los efectos nocivos.
- El número de personas afectadas por el evento.[2]

2.4. Definiciones de Confiabilidad

El término variable aleatoria se emplea para definir una variable independiente que puede tomar cualquier valor dentro de un conjunto de posibles valores. En ingeniería de confiabilidad la variable aleatoria es *T*: tiempo para fallar o tiempo de falla.

2.4.1. Confiabilidad (Reliability)

La confiabilidad (R) es una medición del éxito y es generalmente definido como la probabilidad de que un dispositivo ejecute la función asignada cuando ésta es requerida siempre que esté dentro de los límites operacionales del diseño.

Matemáticamente *R* es una definición precisa de la probabilidad de que un dispositivo opere satisfactoriamente en el intervalo de tiempo de cero a *t*. En términos de la variable aleatoria T, se tiene que:

$$R(t) = P(T > t) \qquad \text{Ec. 2.1}$$

2.4.2. No Confiabilidad (Unreliability)

La no Confiabilidad *(F)* es una medición de falla (no éxito) y es definida como la probabilidad de que un dispositivo falle en un intervalo de tiempo de cero a *t*.

$$F(t) = P(T \leq t) \qquad \text{Ec. 2.2}$$

La relación entre la Confiabilidad y la No Confiabilidad es:

$$F(t) = 1 - R(t) \qquad \text{Ec. 2.3}$$

F(t) es una función de distribución acumulativa. Ésta comienza con una probabilidad de cero y se va incrementando hasta alcanzar una probabilidad de uno.

2.4.3. Disponibilidad (Availability)

En términos matemáticos la Disponibilidad (A) es la probabilidad de que un dispositivo tenga una operación exitosa en el tiempo *t*. No hay un intervalo de tiempo involucrado en este índice. Si el sistema está operando, éste es disponible. No importa si éste ha fallado en el pasado y ha sido reparado o ha estado operando continuamente desde el tiempo *t=0* sin fallas. La Disponibilidad es una medida de éxito usada principalmente para sistemas reparables, aunque ésta puede ser técnicamente aplicada también a sistemas no reparables. Para sistemas no reparables la Disponibilidad, *A(t)*, es igual a Confiabilidad, *R(t)*. En sistemas reparables *A(t)* es mayor o igual que *R(t)*.

2.4.4. Indisponibilidad (Unavailability)

La Indisponibilidad (U) es una medición de falla usada principalmente para sistemas reparables, y es definida como la probabilidad de que un sistema se encuentre fallado en el tiempo *t*. La relación entre la Disponibilidad y la Indisponibilidad es:

$$U(t) = 1 - A(t) \qquad \text{Ec. 2.4}$$

2.4.5. Probabilidad de falla

La probabilidad de falla durante cualquier intervalo de tiempo de operación es dada por la función de densidad de probabilidad de falla. Esta función de densidad de probabilidad de falla está dada por:

$$f(t) = \frac{dF(t)}{dt} \qquad \text{Ec. 2.5}$$

La función de densidad puede ser matemáticamente descrita en términos de la variable aleatoria T:

$$\lim_{\Delta t \to 0} P(t < T \leq t + \Delta t) \qquad \text{Ec. 2.6}$$

Esto puede ser interpretado como la probabilidad de que el tiempo (o momento) de falla T, ocurra entre el tiempo de operación *t* y el próximo intervalo de operación $t + \Delta t$.

2.4.6. Tasa de Falla (Failure Rate)

La tasa de falla instantánea λ, es una medida que indica el número de fallas por unidad de tiempo para una cantidad de dispositivos expuestos a la falla.

$$\lambda(t) = \frac{Fallas\ por\ unidad\ de\ tiempo}{Cantidad\ Expuesta} \qquad \text{Ec. 2.7}$$

La tasa de falla tiene unidades de 1/tiempo. Es una práctica común usar unidades de "fallas por billón (10^9) de horas". Esta unidad es conocida como "FIT" para unidad de falla. La función de tasa de falla está relacionada con las demás funciones de confiabilidad. Se puede demostrar que:

$$\lambda(t) = \frac{f(t)}{R(t)} \qquad \text{Ec. 2.8}$$

2.4.7. Tiempo Medio para Fallar (*MTTF*)

MTTF es el índice que señala el tiempo promedio de falla de un dispositivo y no la vida mínima esperada de éste. Está definido a partir de la definición estadística de valor esperado:

$$E(X) = \int_{-\infty}^{+\infty} x \cdot f(x)\,dx \qquad \text{Ec. 2.9}$$

Usando la variable aleatoria "tiempo de falla T" con la función de densidad de probabilidad *f(t)*, la fórmula para el valor esperado es:

$$E(T) = \int_{0}^{+\infty} t \cdot f(t)\,dt \qquad \text{Ec. 2.10}$$

Substituyendo, la siguiente ecuación en Ec.2.10

$$f(t) = \frac{-d[R(t)]}{dt} \qquad \text{Ec. 2.11}$$

se obtiene,

$$E(T) = -\int_{0}^{+\infty} t \cdot d[R(t)] \qquad \text{Ec. 2.12}$$

integrando por partes se obtiene que,

$$MTTF = E(t) = \int_{0}^{+\infty} R(t)dt \qquad \text{Ec 2.13}$$

Así, *MTTF* es la evaluación de la integral definida de la función de Confiabilidad *R(t)*.

2.4.8. Tiempo Medio para Reparar (*MTTR*)

MTTR es el valor esperado de la variable aleatoria tiempo para reparar. Al igual que *MTTF*, *MTTR* es típicamente un valor promedio.

2.4.9. Tiempo Medio entre Fallas (*MTBF*)

MTBF es un término que aplica sólo a sistemas reparables, y así como *MTTF* y *MTTR* es un promedio que en este caso indica el tiempo promedio entre fallas, esto implica que el dispositivo ha fallado y ha sido reparado. Matemáticamente,

$$MTBF = MTTF + MTTR \qquad \text{Ec. 2.14}$$

Debido a que *MTTR* es usualmente más pequeño que *MTTF*, *MTBF* es aproximadamente igual a *MTTF*. El término *MTBF* es, en algunos casos, incorrectamente sustituido por *MTTF*, el cual aplica a sistemas reparables y no reparables.

2.4.10. Función Distribución de Falla (Distribución Exponencial)

Una función de densidad de probabilidades muy útil en el campo de la Ingeniería de Confiabilidad es la exponencial. Para esta distribución *f(t)*:

$$f(t) = \lambda \cdot e^{-\lambda \cdot t} \qquad \text{Ec. 2.15}$$

Integrando esta función se puede obtener que:

$$F(t) = \int_0^t \lambda \cdot e^{-\lambda \cdot t} \cdot dt = 1 - e^{-\lambda \cdot t} \qquad \text{Ec. 2.16}$$

De acuerdo a la ecuación Ec. 2.3, se obtiene que la Confiabilidad (*R*) de un sistema con distribución de falla exponencial es:

$$R(t) = e^{-\lambda \cdot t} \qquad \text{Ec. 2.17}$$

La tasa de fallas es igual a:

$$\lambda(t) = \frac{f(t)}{R(t)} = \frac{\lambda \cdot e^{-\lambda \cdot t}}{e^{-\lambda \cdot t}} = \lambda \qquad \text{Ec. 2.18}$$

Esto indica que la distribución de probabilidad exponencial negativa presenta una tasa de falla constante.

El MTTF de un componente con una función de densidad de probabilidades exponencial puede ser obtenido a partir de la definición de *MTTF*:

$$MTTF = \int_0^{+\infty} R(t)\,dt \qquad \text{Ec. 2.19}$$

Substituyendo *R(t)* se tiene,

$$MTTF = \int_0^{+\infty} e^{-\lambda \cdot t}\, dt \qquad \text{Ec. 2.20}$$

e integrando,

$$MTTF = -\frac{1}{\lambda} \cdot \left[e^{-\lambda \cdot t} \right]_0^{\infty} = \frac{1}{\lambda} \qquad \text{Ec. 2.21}$$

Entonces para la distribución de probabilidad exponencial negativa, el *MTTF* es inversamente proporcional a la tasa de fallas. [4]

2.5. Sistemas Instrumentados de Seguridad (SIS)

Es un sistema instrumentado usado para implementar una o más funciones instrumentadas de seguridad. El Sistema Instrumentado de Seguridad proporciona los mecanismos necesarios para llevar el proceso a una condición segura cuando una o varias condiciones predeterminadas son violadas. Estos sistemas son diseñados para detectar fallas o desviaciones dentro del proceso y desencadenar las acciones apropiadas, salvaguardando tanto la vida de las personas, los equipos, la continuidad de la producción y las exigentes regulaciones ambientales. Los Sistemas Instrumentados de Seguridad, se destinan específicamente a prevenir o minimizar los daños que puedan ocasionar a las personas, equipos y ambiente. Estos sistemas están en capacidad de tomar acciones automáticas e independientes del operador en los casos de que las desviaciones de cualquiera de las variables del proceso se escapen del Sistema de Control Básico del Proceso (BPCS), abortando el control normal de la planta y llevándola a un estado predeterminado y seguro.

El SIS incluye todos los elementos desde el sensor hasta el elemento final de control, incluyendo entradas, salidas, fuentes de poder y soluciones lógicas. La interfaz para el SIS es considerada como parte del mismo, si ella posee un impacto potencial en su función de seguridad. Estas serán la interfaz del operador, la interfaz de ingeniería de mantenimiento y la interfaz de comunicación. Como se puede apreciar en la figura 2.1, los SIS están conformados principalmente por tres partes:

a) Las entradas del sistema, que representan las señales provenientes de los sensores de campo (transmisores), o por otro tipo de dispositivo que afecte las secuencias lógicas (botón de accionamiento manual), estas señales de entrada son las señales del proceso que se están sensando, tales como flujo, presión y temperatura.

b) La lógica de enclavamiento (logic solver), que representa en forma simbólica la toma de decisiones generadas por el estado de las entradas y define el estado de las salidas, por lo tanto es el encargado de monitorear las entradas y tomar la acción correctiva ante una condición de falla en el proceso.

c) Las salidas del sistema, que son las señales destinadas a operar los equipos o elementos finales de control conectados al proceso (válvulas solenoides, arrancadores de motores, etc.), estos elementos finales de control se encuentran entre el elemento controlador lógico y el proceso, ejecutando una acción de paro. [4]-[5]

En Sistemas Instrumentados de Seguridad donde se implementen funciones instrumentadas de seguridad con distinto nivel de integridad de seguridad, el hardware y/o software compartido o común debe cumplir los requerimientos del mayor nivel SIL en el sistema. [6]

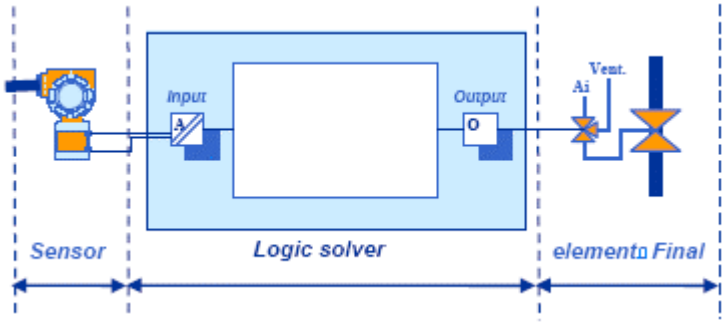

figura 2.1. Sistema Instrumentado de Seguridad

2.5.1. Tipos de SIS: aplicaciones y tecnologías

Dependiendo de la aplicación, dos diferentes tipos de SIS pueden distinguirse. Los primeros son sistemas preventivos como los sistemas de Parada de Emergencia (ESD) y los segundos son sistemas de mitigación como los sistemas de Fuego y Gas (F&G). Los sistemas ESD son diseñados de acuerdo al principio de des-energizar

para disparar mientras que los sistemas F&G se diseñan de acuerdo al principio energizar para disparar.

2.5.2. Estados de operación de un SIS

Un SIS puede encontrarse en cualquiera de los siguientes estados de operación:

Estado de operación satisfactoria

Se entiende por estado de operación satisfactoria aquel estado donde todos los componentes del SIS están operando correctamente y cualquier demanda de protección o parada de la planta puede ser satisfecha a cabalidad.

Estado de falla segura

Es aquel estado donde el SIS presenta una falla que da lugar a una parada para protección no requerida, deteniendo la operación de un equipo o sistema cuando las condiciones operacionales reales no requerían tal acción. Su principal consecuencia es la pérdida de producción, aunque puede tener un impacto en la seguridad dado que un alto porcentaje de accidentes están ubicados en los momentos de parada y arranque.

Estado de falla peligrosa

Es aquel estado donde el SIS está en la condición de no actuar ante una posible demanda del sistema (falla en demanda). Es decir, la planta continúa en operación, pero dado que el SIS no está operativo, éste no actuará ante una demanda de protección (demanda de parada) de la Planta.

Estado de falla peligrosa detectado

Este estado es el mismo "Estado de Falla Peligrosa" (detected, overt o revealed) pero en cual el autodiagnóstico del sistema ha logrado descubrir el elemento fallado en el SIS reportándolo oportunamente al operador.

Estado de falla peligrosa no detectado

Este estado es el mismo "Estado de Falla Peligrosa" (undetected, unrevealed o covert) pero en el cual el autodiagnóstico del sistema no ha logrado descubrir el elemento fallado en el SIS. Por tal motivo la falla se mantiene oculta y el camino que queda para descubrirla es a través de la inspección y prueba periódica del sistema.

Estado de Falla de Alto Riesgo (Hazardous)

Es aquel estado donde el SIS presenta una falla y no es capaz de actuar ante una demanda de la planta en una condición de alto riesgo que pudiese dar lugar a pérdidas humanas y materiales si los otros niveles de protección no logran reducir el riesgo de estado. [4]

2.5.3 Capas Independientes de Protección (IPL)

Son aquellas capas de protección que cumplen con las siguientes características:

- Cada IPL debe ser independiente de las otras capas. En otras palabras, no debe existir una falla que pueda dejar fuera de funcionamiento dos o más capas de protección.
- Una IPL es específicamente diseñada para prevenir o mitigar las consecuencias de un evento peligroso.
- La IPL se diseña de tal manera que la misma puede ser auditada.
- El Sistema del Control Básico de Proceso (BPCS) no puede ser considerado como una IPL.
- Las alarmas que son anunciadas y que son dependientes del BPCS, no se pueden considerar como IPL adicional.
- Cualquier otro sistema instrumentado puede ser considerado como una IPL sí y sólo si:
  - Es totalmente independiente del BPCS y del SIS.
  - Su falla no es responsable de iniciar un evento peligroso.[7]

2.6. Funciones Instrumentadas de Seguridad (SIF).

Es una capa de protección instrumentada independiente, cuyo propósito es llevar al proceso a un estado seguro cuando se violan condiciones predeterminadas.

Cuando se diseña una función instrumentada de seguridad, es necesario considerar si la aplicación es de modo de operación continuo o de demanda. La mayoría de las aplicaciones en la industria de procesos operan en modo de demanda debido a que en este sector las demandas son poco frecuentes. Hay algunas aplicaciones en las cuales las demandas son frecuentes (por ejemplo, mayores que una vez por año) y es más apropiado considerar la aplicación como operando en modo continuo. [5]-[6]

2.6.1. Parámetros de una SIF

Los elementos o subsistemas que componen una función instrumentada de seguridad presentan los siguientes parámetros de seguridad:

2.6.1.1. Cobertura de diagnóstico (*DC*)

Es el cociente de la tasa de fallas detectadas (detectadas por pruebas de diagnóstico) entre la tasa de fallas total de un componente o subsistema. La cobertura de diagnóstico no incluye las fallas detectadas en procedimientos de prueba. Para aplicaciones de seguridad la cobertura de diagnóstico (DC) se calcula de acuerdo a la siguiente expresión:

$$DC = \frac{\lambda dd}{\lambda d} \qquad \text{Ec. 2.22}$$

donde λd y λdd representan la tasa de falla peligrosa y la tasa de falla peligrosa detectada respectivamente.

2.6.1.2. Falla de causa común

Es la falla del resultado de uno o más eventos, causando fallas coincidentes de dos o más componentes separados conduciendo a la falla del sistema. Es una falla simple que es capaz de producir la falla completa de un sistema redundante. La falla

de causa común se expresa a través de "β", la cual indica el porcentaje o fracción del total de fallas que es debido a causa común. Desde el punto de vista práctico un sistema sujeto a falla de causa común se modela como un sistema compuesto por dos elementos trabajando en serie. El primero de estos elementos contribuyendo con un peso de "β" por ciento, como un sistema sencillo, ya que cualquier falla de causa común hace fallar al sistema completo, y el segundo contribuyendo con un peso de "1-β" por ciento en su esquema de redundancia.

Factores típicos de Falla de causa común son la vibración, la temperatura, la humedad, las ondas electromagnéticas, etc. Valores típicos de "β" se encuentran en el rango de 0.1% a 10%. En aquellos casos en donde no se conoce con certeza el valor de "β" generalmente éste se asigna igual a 10%, lo cual se considera bastante conservador. [4]-[5]

2.6.1.3. Fracción de falla segura (*SFF*)

Es la fracción de la tasa de falla de hardware de un dispositivo que resulta en una falla segura o falla peligrosa detectada. Este valor se determina a partir de la siguiente ecuación:

$$SFF = 1 - \frac{\lambda du}{\lambda} \qquad \text{Ec. 2.23}$$

donde λdu representa la tasa de falla peligrosa no detectada.

2.6.1.4. Tolerancia de falla de Hardware (*HFT*)

Es el máximo número de fallas en un subsistema, resultante de fallas aleatorias de hardware, que pueden ocurrir sin llevar a la SIF a un estado de falla peligroso.

Para este aspecto la norma IEC 61508 clasifica los elementos o subsistemas en dos tipos: A y B.

Un subsistema es tipo A si se cumplen cada una de las siguientes condiciones:

- Los modos de falla de todos los componentes que lo constituyen están bien definidos.

- El comportamiento del subsistema bajo condiciones de falla puede ser completamente determinado.
- Para el subsistema existen suficientes datos de fallas confiables, extraídos de experiencia en campo.

Un subsistema es tipo B si se cumplen cada una de las siguientes condiciones:

- El modo de falla de al menos uno de los componentes que lo constituyen no están bien definidos.
- El comportamiento del subsistema bajo condiciones de falla no puede ser completamente determinado.
- Para el subsistema no existen suficientes datos de fallas confiables, extraídos de experiencia en campo.

2.7. Nivel de Integridad de Seguridad (SIL)

El nivel de integridad de seguridad es un nivel discreto para la especificación de los requerimientos de integridad de las funciones de seguridad a ser asignadas a sistemas instrumentados de seguridad.

Cada nivel discreto se refiere a cierta probabilidad de que un sistema referido a seguridad realice satisfactoriamente las funciones de seguridad requeridas bajo todas las condiciones establecidas en un período de tiempo dado. El SIL se define numéricamente para poder tener un valor objetivo con qué comparar diferentes soluciones y diseños.

El SIL requerido de una SIF es asignado tomado en cuenta la reducción de riesgo que se requiere implantar con dicha SIF. De acuerdo a la norma ANSI/ISA 84.00.01-2004, para una SIF operando en modo de demanda, el SIL requerido debe ser especificado de acuerdo la tabla 2.2, mientras que para una SIF operando en modo continuo el SIL requerido debe especificarse de acuerdo a la tabla 2.3.

Tabla 2.2. SIL para operación en modo de demanda

Nivel de Integridad de Seguridad (SIL)	Probabilidad de falla en demanda promedio (*PFDAVG*)	Factor de Reducción de Riesgo (*RRF*)
4	$\geq 10^{-5}\ a < 10^{-4}$	$> 10000\ \ a\ \ \leq 100000$
3	$\geq 10^{-4}\ a < 10^{-3}$	$> 1000\ \ a\ \ \leq 10000$
2	$\geq 10^{-3}\ a < 10^{-2}$	$> 100\ \ a\ \ \leq 1000$
1	$\geq 10^{-2}\ a < 10^{-1}$	$> 10\ \ a\ \ \leq 100$

Es necesario destacar que es posible emplear varios sistemas con SIL menor para satisfacer la necesidad de un sistema con SIL mayor, por ejemplo, emplear un sistema con SIL 2 y uno con SIL 1 para satisfacer la necesidad de un sistema con SIL 3.[5]-[6]

Tabla 2.3. SIL para operación en modo continuo

Nivel de Integridad de Seguridad (SIL)	Frecuencia de falla peligrosa (por hora)
4	$\geq 10^{-9}\ a < 10^{-8}$
3	$\geq 10^{-8}\ a < 10^{-7}$
2	$\geq 10^{-7}\ a < 10^{-6}$
1	$\geq 10^{-6}\ a < 10^{-5}$

La integridad de seguridad está compuesta de los siguientes dos elementos:

2.7.1. Integridad de seguridad de hardware

Es la parte de la integridad de seguridad relacionada con las fallas aleatorias de hardware en un modo de falla peligroso. En algunos casos, es necesario emplear arquitecturas redundantes para poder cumplir con los requerimientos de integridad de seguridad de hardware.

2.7.2. Integridad de seguridad sistemática

Es la parte de la integridad de seguridad relacionada con las fallas sistemáticas en un modo de falla peligroso. En este caso, la implementación de canales redundantes no contribuye a la disminución de las fallas sistemáticas. Ejemplos de fallas sistemáticas son:

- Errores en el diseño del SIS.
- Errores en la implementación del hardware.
- Errores de software.
- Errores de interacción humana.
- Errores de diseño de hardware.
- Errores de modificación.[5]

2.8. Ciclo de Vida de Seguridad

Las etapas del ciclo de vida de seguridad se presentan en la figura 2.2 y son descritos a continuación:

a. **Identificación de peligros y riesgos**. El objetivo es determinar los peligros y los eventos peligrosos del proceso y su equipo asociado, la secuencia de eventos que lleven a un evento peligroso, el riesgo del proceso asociado a los eventos peligrosos, los requerimientos de reducción de riesgo y las funciones de seguridad requeridas para alcanzar la reducción de riesgo necesaria.

b. **Asignación de funciones de seguridad a capas de protección**. El objetivo es la asignación de las funciones de seguridad a capas de protección y para cada función instrumentada de seguridad, su respectivo nivel de integridad de seguridad.

c. **Especificación de los requerimientos de seguridad del SIS**. El objetivo es especificar los requerimientos para cada SIS, en términos de las funciones

instrumentadas de seguridad requeridas y su respectivo nivel de integridad de seguridad, con la finalidad de cumplir con los requerimientos de seguridad funcional.

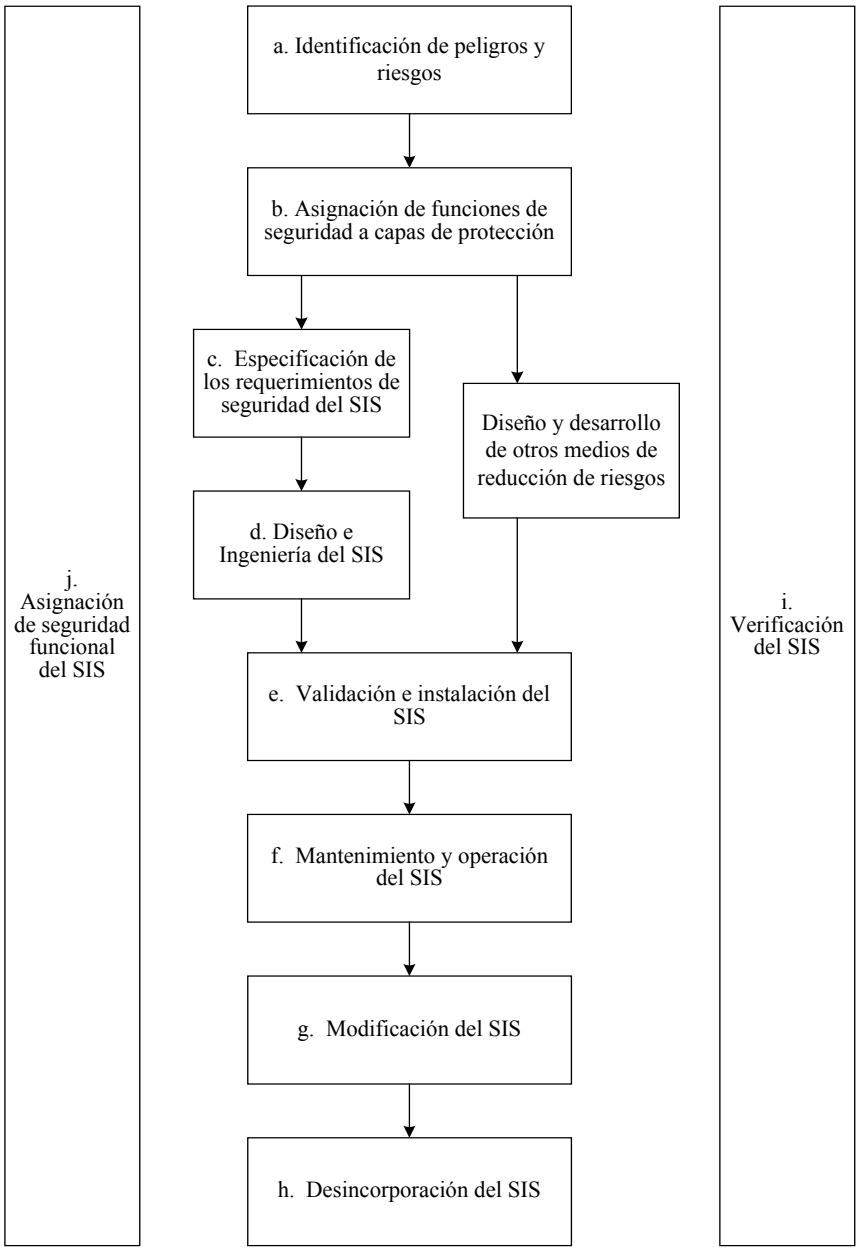

figura 2.2. Etapas del ciclo de vida de Seguridad.

d. **Diseño e Ingeniería del SIS.** El objetivo es diseñar el SIS que cumpla con los requerimientos de las funciones instrumentadas de seguridad e integridad de seguridad.

e. **Validación e instalación del SIS**. El objetivo es integrar y probar el SIS. Validar que el SIS cumpla con en todos los aspectos los requerimientos de seguridad en términos de las funciones instrumentadas de seguridad y el nivel de integridad de seguridad asociado.

f. **Mantenimiento y operación del SIS**. El objetivo es asegurar que la seguridad funcional del SIS es mantenida durante la operación y mantenimiento.

g. **Modificación del SIS**. El objetivo es realizar correcciones, mejoramientos o adaptaciones del SIS, asegurando que el nivel de integridad de seguridad es alcanzado y mantenido.

h. **Desincorporación del SIS**. El objetivo es asegurar que previo a la desincorporación del SIS de servicio activo, se realice una apropiada revisión y se obtenga la autorización requerida.

i. **Verificación del SIS**. El objetivo es probar y evaluar las salidas de una etapa determinada para asegurar la validez y consistencia con respecto a los productos y normas colocados como entrada a dicha fase.

j. **Asignación de seguridad funcional del SIS**. El objetivo es investigar y llegar a la conclusión de que la seguridad funcional del SIS ha sido alcanzada. [6]

A continuación en la tabla 2.4 se presentan las entradas y salidas de cada una de las etapas del Ciclo de Vida de Seguridad.

Tabla 2.4. Entradas y Salidas de las Etapas del Ciclo de Vida de Seguridad

	Etapa	Entradas	Salidas
a	Identificación de peligros y riesgos	Diseño del proceso, ubicación de equipos, arreglos principales y seguridad objetivo.	Descripción de los peligros, de las funciones de seguridad requeridas y la reducción de riesgo asociada.
b	Asignación de funciones de seguridad a capas de protección	Descripción de las funciones instrumentadas de seguridad y su respectivo nivel de integridad de seguridad.	Descripción de la asignación de los requerimientos de seguridad
c	Especificación de los requerimientos de seguridad del SIS	Descripción de la asignación de los requerimientos de seguridad.	Requerimientos de seguridad del SIS; requerimientos de seguridad de software.
d	Diseño e Ingeniería del SIS.	Requerimientos de seguridad del SIS. Requerimientos de seguridad de software.	Diseño del SIS en conformidad con los requerimientos de seguridad del SIS. Plan de prueba para la integración del SIS.
e	Validación e instalación del SIS	Diseño del SIS. Plan de prueba de integración del SIS. Requerimientos de seguridad del SIS. Plan de validación de seguridad del SIS.	Completo funcionamiento del SIS en conformidad con los resultados de diseño del SIS obtenidos de las pruebas de integración del mismo.
f	Mantenimiento y operación del SIS	Requerimientos del SIS. Diseño del SIS. Planes de operación y mantenimiento del SIS.	Resultado de las actividades de operación y mantenimiento.
g	Modificación del SIS	Requerimientos de seguridad del SIS revisados	Resultados de la modificación del SIS.
h	Desincorporación del SIS	Requerimientos de seguridad "como construido" e información del proceso.	SIS colocado fuera de servicio.
i	Verificación del SIS	Plan de verificación del SIS por cada etapa.	Resultados de la verificación del SIS por cada etapa.
j	Asignación de seguridad funcional del SIS.	Planes para la asignación de la seguridad funcional del SIS. Requerimientos de seguridad del SIS.	Resultados de la asignación de la seguridad funcional del SIS.

2.9. Métodos para la determinación del Nivel de Integridad de Seguridad (SIL)

En la norma ANSI/ISA 84.00.01-2004 parte 3 se contemplan diversos métodos para la determinación de nivel de integridad de seguridad de una planta y/o proceso. Estos métodos son:

- Método Semi-cuantitativo.
- Método de Matriz de Capas de Seguridad (cualitativo).
- Método de Gráfica de Riesgo Calibrada (Semi-cualitativo).
- Método de Gráfica de Riesgo (cualitativo).
- Método de Análisis de Capas de Protección.

En el presente trabajo se empleó el Método de Gráfica de Riesgo y el Método Semi-cuantitativo para la determinación del SIL de forma cualitativa y cuantitativa respectivamente. Cabe destacar que se emplearon los métodos antes mencionados ya que estos son los de mayor uso en la industria petrolera y petroquímica a nivel mundial.

2.9.1. Método General de Gráfica de Riesgo para la determinación de Nivel de Integridad de Seguridad (SIL)

Este método está contemplado en el anexo E de la norma ANSI/ISA 84.00.01-2004 parte 3. La gráfica de riesgo está basada en el principio de que el riesgo es proporcional a la consecuencia y frecuencia del evento peligroso. En otras palabras el riesgo simplificado está basado en la siguiente ecuación:

$$\boldsymbol{R}\ (\text{Riesgo}) = \boldsymbol{f}\ (\text{Frecuencia}) \times \boldsymbol{C}\ (\text{Consecuencia}) \qquad \text{Ec. 2.24}$$

donde,

R: Riesgo sin el sistema instrumentado de seguridad (SIS)

f: Frecuencia del evento peligroso sin el SIS

C: Consecuencia del evento

Las consecuencias están relacionadas al daño asociado con la salud y seguridad de las personas y al daño del ambiente.

La frecuencia (f) es la combinación de:

- Frecuencia y tiempo de exposición en la zona peligrosa (F).
- Probabilidad de evitar el evento peligroso (P).
- Probabilidad de que el evento peligroso ocurra sin la adición de un SIS (W).

Esto produce los siguientes cuatro parámetros de riesgo:

- Consecuencia del evento peligroso (C).
- Frecuencia y tiempo de exposición en la zona peligrosa (F).
- Posibilidad de evitar el evento peligroso (P).
- Probabilidad de ocurrencia del evento peligroso (W).

La definición de estos parámetros (C, F, P y W) son presentados en las tablas 2.5, 2.6, 2.7 y 2.8.

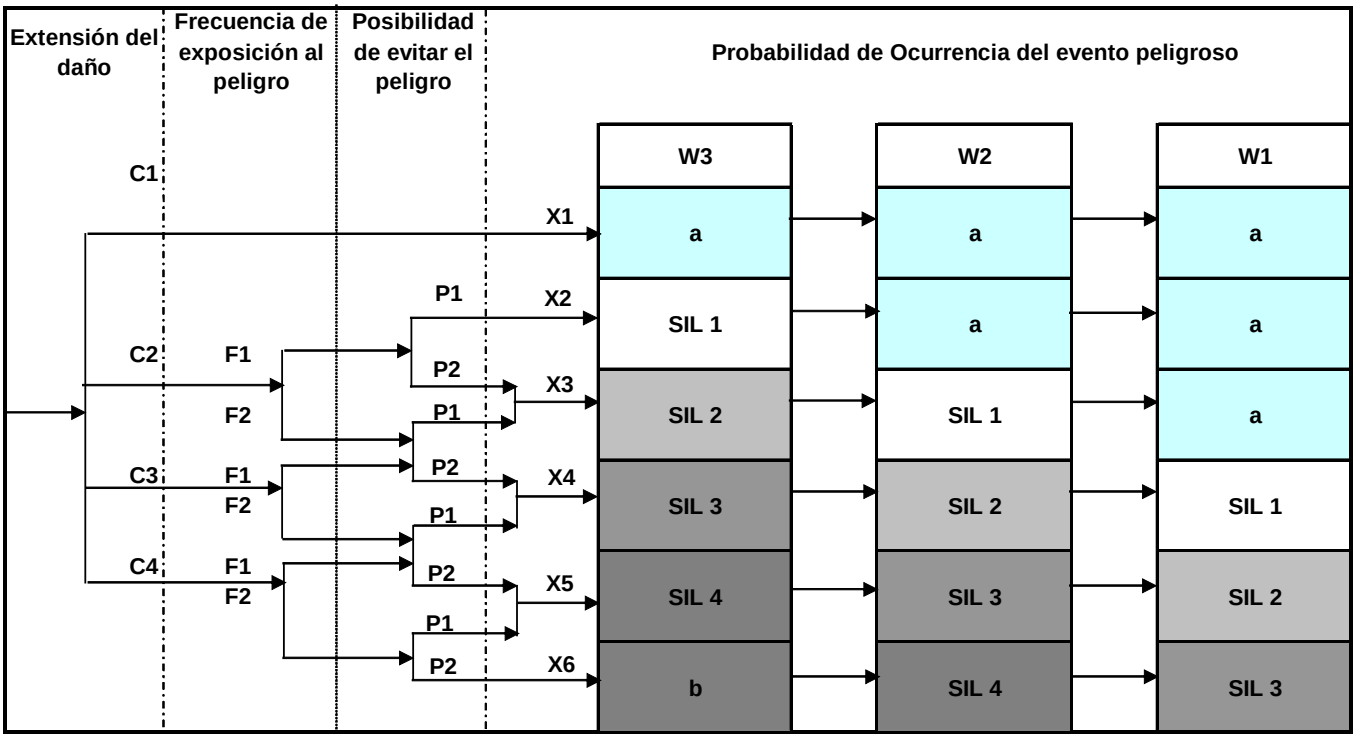

figura 2.3. Método Cualitativo de gráfica de riesgo para determinación del SIL

La metodología del Gráfico de Riesgo es la siguiente:

1.- El gráfico es usado separadamente para determinar el SIL requerido por cada SIF.

2.- La combinación de los parámetros de riesgo descritos anteriormente, permite el desarrollo de la gráfica del riesgo. En la figura 2.3, los parámetros mayores indican un riesgo mayor (C1< C2 < C3 < C4; F1 < F2; P1 < P2; W1 < W2 < W3).

3.- El uso de los parámetros de riesgo C, F y P conllevan a un número de salidas X_1, X_2, X_3, ...X_N. Cada una de estas salidas es direccionada a una de las tres escalas de

probabilidad de ocurrencia del evento peligroso (W1, W2 y W3). Cada punto en esta escala es una indicación del SIL requerido.

4.- De la Gráfica de Riesgo se pueden obtener los siguientes resultados:

- SIL requerido para mitigar el riesgo: SIL (1, 2 ,3 ó 4).
- No necesidad de la implementación de un SIS (indicado por la letra "a").
- No suficiencia de la implementación de un SIS (indicado por la letra "b").

Tabla 2.5. Severidad de Consecuencias (C)

Parámetro	Clasificación	Severidad del Evento
C1	Muy Baja	Heridas leves al personal, sin daños al ambiente o sin daños al equipo.
C2	Baja	Lesiones mayores al personal o daños menores al ambiente, daños menores al equipo, no implica parada del proceso.
C3	Moderada	Una fatalidad o daños al ambiente recuperables al mediano plazo, daños al equipo y breve parada del proceso.
C4	Alta	Varias fatalidades o daño permanente al ambiente, graves daños al equipo y parada del proceso por un largo período de tiempo.

Tabla 2.6. Frecuencia de exposición al peligro (F)

Parámetro	Clasificación	Comentarios
F1	Menor	Muy baja a baja frecuencia de exposición al peligro.
F2	Mayor	Muy alta frecuencia de exposición al peligro.

Tabla 2.7. Posibilidad de Evitar el peligro (P)

Parámetro	Clasificación	Comentarios
P1	Posible	Posible bajo ciertas condiciones específicas (*)
P2	Poco Posible	Casi imposible evitar el peligro (*)

(*) Este parámetro toma en consideración lo siguiente:

- Operación del proceso [supervisado (operado por personal entrenado ó no entrenado) ó no supervisada.]
- Rapidez del desarrollo del evento peligroso (rápido, inmediato o lento).
- Facilidad de identificación del peligro: inmediatamente, detectado por medios técnicos o no detectado.
- Rutas de escape posibles: Posible o imposible en ciertas circunstancias.

Tabla 2.8. Probabilidad de ocurrencia del evento peligroso (W)

Tipo de Evento	**Frecuencia (veces/año)**	**Probabilidad de ocurrencia**
Eventos de muy baja probabilidad de ocurrencia, tales como fallas múltiples de instrumentos, errores humanos múltiples ó fallas espontáneas de equipos.	$F < 10^{-4}$	W1 Muy Baja
Eventos de baja probabilidad de ocurrencia, incluyen la combinación de fallas de instrumentos con fallas humanas.	$10^{-4} < F < 10^{-2}$	W2 Baja
Eventos de probabilidad mediana alta, tales como fallas de válvulas ó de instrumentación.	$F > 10^{-2}$	W3 Moderada a Alta

2.9.2. Método Semi-Cuantitativo para la determinación de Nivel de Integridad de Seguridad (SIL)

Este método está contemplado en el anexo B de la norma ANSI/ISA-84.00.01-2004 parte 3. El procedimiento se fundamenta en la estimación de frecuencias y la determinación de consecuencias y su probabilidad de ocurrencia. Para la estimación de frecuencias, se utiliza la técnica de árbol de fallas, para la determinación de consecuencias se emplea la técnica de árboles de eventos y programas de simulación. En general este método consiste en reducir el riesgo impuesto por el proceso hasta un riesgo meta, a través de las capas independientes de protección ("Independent Protection Layers" - IPL) y del SIS.

Los pasos del método Semi-cuantitativo son los siguientes:

1. Identificar el nivel de Riesgo Aceptable permitido.
2. Identificar peligros del proceso.
3. Identificar capas de protección independientes.
4. Determinar la frecuencia de ocurrencia de las consecuencias (evento final) que origina el evento iniciador, por medio del siguiente procedimiento:

    a. Elaborar el árbol de fallas (demandas) y calcular la frecuencia ***F*** de ocurrencia del evento iniciador, utilizando las diferentes tasas de falla disponibles.

    b. Para el evento iniciador determinar las consecuencias y la probabilidad de ocurrencia ***P*** de éstas a través de árbol de eventos y programas de simulación.

    c. Cuantificar el riesgo asociado al evento iniciador, utilizando la frecuencia ***F*** y la probabilidad de las consecuencias ***P***. Este es el valor del riesgo real presente en la instalación.

$$Rs = F \cdot P \qquad \text{Ec. 2.25}$$

5. Calcular el valor de frecuencia de ocurrencia final del riesgo identificado (***Rf***), multiplicando el aporte de las capas independientes de protección (***AIPL***), por el valor ***Rs*** (el valor ***AIPL*** representa la probabilidad de falla de una determinada IPL y se obtiene de reportes estadísticos).
6. Determinar la probabilidad de falla en demanda (***PFDAVG***) que permita reducir el riesgo hasta la meta de nivel de riesgo establecido (Riesgo Aceptable), dividiendo el valor del Riesgo Aceptable (***Ra***), entre el valor de frecuencia de ocurrencia final del riesgo (***Rf***):

$$PFD_{AVG} = \frac{Ra}{Rt} \qquad \text{Ec. 2.26}$$

7. Con el valor ***PFDAVG*** obtenido se asigna el Nivel de Integridad de seguridad de acuerdo a la tabla 2.9.

Tabla 2.9. Niveles de Integridad de Seguridad (SIL)

Niveles de Integridad de Seguridad	Probabilidad de falla en Demanda (PFD average)
1	$10^{-1}\ a\ 10^{-2}$
2	$10^{-2}\ a\ 10^{-3}$
3	$10^{-3}\ a\ 10^{-4}$
4	$10^{-4}\ a\ 10^{-5}$

2.10. Métodos para la verificación del SIL de una SIF

Luego de diseñar una función instrumentada de seguridad se debe verificar que ésta cumple con el nivel de integridad de seguridad requerido de la aplicación para la cual fue diseñada. Para realizar este cálculo se emplean diversos métodos, de entre los cuales se destacan: Ecuaciones Simplificadas, Análisis de Árboles de Falla y Modelos de Markov, los cuales están contemplados en el reporte técnico ISA TR84.00.02.

El método de las Ecuaciones simplificadas es el más sencillo pero no proporciona suficiente precisión en los resultados. El método de Markov es algo más preciso pero su uso es mucho más complejo. Por su parte, el método de Análisis de Árbol de Falla es relativamente sencillo y proporciona resultados de precisión adecuada.

2.10.1. Cálculo del SIL empleando Ecuaciones Simplificadas

La técnica de las ecuaciones simplificadas implica la determinación de la Probabilidad de Falla en Demanda (PFD) para los sensores de campo [Field Sensor (FS)],Unidad Controlador [Logia Solver (LS)], de los elementos finales control [Final Elements (FE)], y de los sistemas de apoyo [Support Systems (SS)]. Los PFDs se suman para entonces obtener el PFDsis.

$$PDF_{SIS} = \sum PFD_{FS} + \sum PFD_{LS} + \sum PFD_{FE} + \sum PFD_{SS} \qquad \text{Ec. 2.24}$$

Las ecuaciones simplificadas usadas para calcular los PFDs son derivadas de los modelos de Markov, sin embargo, las simplificaciones de los modelos introducen algunas limitaciones. A diferencia de los modelos de Markov, este método no maneja los tiempos variables de reparación, fallas dependientes en el tiempo, o fallas dependientes de las secuencias.

Es importante resaltar que las ecuaciones que se emplean en este método no permiten el modelado de tecnologías diversas. Los sensores o los elementos finales usados en cada estrategia de la votación deben tener la misma tasa de falla. En consecuencia este método no permite el modelado de un interruptor y un transmisor o de una válvula de control y una válvula de bloqueo a la vez.

El método tampoco permite el modelado de interacciones entre los dispositivos del SIS o lógicas de falla complejas, como sensores de temperatura en configuración 1oo2 detectando el mismo evento potencial que unos sensores de presión en configuración 2oo3. Por lo tanto, este método es sólo utilizado para modelar SIS(s) simples. Sin embargo, la matemática utilizada en esta metodología es sencilla, lo cual hace que este método sea excelente para primera aproximación. [8]

2.10.2. Método de Árboles de Falla

La técnica gráfica de análisis de árboles de falla permite visualizar fácilmente las fallas. Debido a que la lógica de falla presente es planteada, se puede evaluar diferentes tecnologías y estrategias de votación complejas. Sin embargo, el análisis de árbol de falla no es fácilmente adaptable a los SIS que tienen fallas dependientes del tiempo. El análisis de árboles de falla es una de las técnicas más utilizadas para el modelado de sistemas instrumentados de seguridad con índices de integridad SIL2 y SIL3. El método matemático del Análisis de Árbol de falla es diferente al del análisis de los modelos de Markov. El Análisis de Árbol de falla asume que las fallas de dispositivos redundantes son independientes e incondicionales. En Análisis de Árbol de falla, la PFD_{AVG} es calculada para cada dispositivo tomando en cuenta la arquitectura y votación. En consecuencia las ecuaciones que se derivan de este método son diferentes a las del método de Ecuaciones simplificadas. Con ecuaciones

diferentes, los valores de PFD_{AVG} que se obtiene son diferentes. Sin embrago, ambos métodos proporcionan aproximaciones aceptables de la PFD_{AVG} de un SIS.

Hay tres beneficios principales asociados con el uso del Análisis de Árbol de Fallas como método para la verificación del SIS. Primero, la representación gráfica de la lógica de fallas es fácilmente entendible por analistas de riesgo, ingenieros y gerentes de proyectos. Segundo, el método ha sido usado por años en la industria de procesos para la determinación de riesgos. Finalmente, la disponibilidad de herramientas de software facilita la calidad y precisión de los cálculos. [8]

2.10.3. Modelo de Markov

Un matemático ruso, Andrei Andreyevich Markov (1856-1922), definió el proceso de Markov, en el cual la variable futura es determinada por la variable presente pero es independiente de los predecesores. Markov dio particular énfasis a las cadenas de Markov (secuencias en las que la variable toma un valor discreto en particular). Este método aplica perfectamente al proceso de falla/reparación debido a que las combinaciones de falla crean estados discretos del sistema. Adicionalmente, el proceso falla/reparación se mueve entre estados discretos sólo como resultado del estado y la falla actual. La técnica del modelo de Markov, utiliza en su elaboración el álgebra de matrices y son excelentes para el modelado de SIS(s) con relaciones complejas, requerimientos de tiempo dependientes y tiempos de reparación variables. Esta técnica es utilizada extensivamente para el modelaje de Sistemas Electrónicos Programables.

El modelo de Markov es una poderosa herramienta de modelaje, y la construcción del modelo de Markov es probablemente la parte más difícil del análisis, pero una vez que la misma es entendida, las fallas del SIS son definidas como “estados de Markov”. El Modelo de Markov permite el modelaje de múltiples sistemas en el cual el nivel de redundancia varía con el tiempo debido a fallas de los componentes y a la reparación de los mismos. [4]

2.11. Arquitecturas

Las arquitecturas comerciales que se encuentran actualmente en le mercado son las siguientes:

- Arquitectura 1oo1
- Arquitectura 1oo2
- Arquitectura 2oo2
- Arquitectura 2oo3
- Arquitectura 1oo1D
- Arquitectura 1oo2D
- Arquitectura 2oo2D

La descripción de cada una de estas arquitecturas se presenta en el anexo 3.

CAPÍTULO III

DESCRIPCIÓN DE LA PLANTA Y DEL PROCESO BAJO ESTUDIO

3.1. Introducción

El proyecto objeto del estudio corresponde a un caso típico de las facilidades para la producción de petróleo extra pesado (Pozos y Estación de Flujo) bajo la patente de Orimulsion® en Jose.

Los mayores elementos que conforman la sección aguas arriba (Upstream Section) en la producción de crudo extra pesado se mencionan a continuación.

- **Facilidades de Superficie**. Pozos productores de crudo pesado agrupados en Separadores (Clusters), Red de recolección y distribución del producto (Bitumen Húmedo Diluido, BHD) para su inicial condicionamiento en la Estación de Flujo. La producción promedio de los pozos se estima en 1300 BPSD (Bitumen neto / base seco) a una presión máxima de 150 psig y una temperatura de operación de 100 ºF. La ingeniería contempla 8 Cluster y 64 Pozos. El número de señales por Cluster: 16 AI, 8 AO, 16 DI y 8 DO.

- **Estación de Flujo**, instalación para el tratado del BHD a partir de sus condiciones iniciales. Capacidad de 140 MBPSD de Bitumen diluido húmedo y 23 MMSCFD (Millones de Pies Cúbicos Estándar por Día) de gas asociado. El número de señales a contemplar para el PLC de la Estación son: 40 AI, 14 AO, 285 DI y 90 DO.

La estación de Flujo está conformada por los siguientes equipos:

- Separadores de Producción
- Depurador de Gas Vertical
- Tanque de Almacenamiento de Producto

- Paquetes de Inyección de Químicos (Demulsificante y Antiespumante)
- Bombas de Transferencia de Producto
- Unidad de Medición del Producto (Unidad de Medición de Transferencia y Custodia)
- Tanques de Almacenamiento de Diluente y bombas de Inyección de Diluente.

- **Sistema Distribución y Almacenamiento de Diluente (DSDS)**, provee la nafta (diluente) para diluir el crudo pesado en las cabeceras de pozo con la finalidad de mejorar su capacidad de ser bombeada.

3.2. Descripción del proceso y filosofía de operación

Los Diagramas de Flujo del Proceso y Diagramas de Tubería e Instrumentación (P&ID) de la planta y proceso bajo estudio se presentan en el anexo 4.

3.2.1. Facilidades de Superficie (FSF)

Las Facilidades de Superficie consisten en el cabezal del pozo, válvula multipuerto selectora de pozo, sistema de medición multifásico, cabezal de producción principal, línea de distribución de diluente y subcabezales. Se estima la perforación de 75 pozos de forma escalonada distribuidos en 16 clusters para reducir la erosión del ambiente y simplificar el sistema FSF.

Los pozos productores son mayormente horizontales por lo que se utilizarán Bombas electro-sumergibles (BES), los cuales envían continuamente el Bitumen Húmedo Diluido (BHD) producido hacia la válvula multipuerto NPS 4" x 8" (identificada como ZZ00-UVM-1003, donde ZZ se refiere a la identificación del cluster) instalada en cada cluster con un máximo de 6 pozos por válvula. Aquellos cluster con arreglos de 7 a 12 pozos tienen dos (2) válvulas multipuerto (ZZ00-

UVM-1003 & ZZ00-UVM-1007). Esta válvula multipuerto es usada para realizar procedimientos de prueba de pozos en cada cluster.

Las bombas electro-sumergibles tienen su propio sistema de control local. Todas las variables de monitoreo de la bomba (indicaciones y alarmas como tasa flujo de producción del pozo, protecciones del motor, tensión, falla de alimentación eléctrica, presión, variaciones de velocidad/frecuencia, etc.) son supervisadas por el sistema de control local y las señales son enviadas vía comunicación serial RS-485 al PLC del cluster usando protocolo Modbus. Desde este, las señales son enviadas a la sala de control de la estación de flujo MPE-3 vía radio. La supervisión de los Pozos reside en el PLC de la Estación de Flujo ya que la filosofía de operación de los Clusters es que sean instalaciones desatendidas.

El proceso cuenta con una conexión de toma de muestra. Ésta se encuentra colocada aguas abajo del límite de batería del paquete de la bomba electro-sumergible, en la línea de producción del pozo, para tomar muestras del BHD producido específicamente por cada pozo. Esto permite evaluar la gravedad API experimentalmente.

La producción promedio por pozo horizontal está estimada alrededor de 1300 BPSD de Bitumen neto de 8° API, a una presión máxima de 150 psig y 100°F.

El Bitumen es apropiadamente diluido (usando nafta de 51°API) con la finalidad de hacer más fácil el transporte y procesamiento del crudo pesado.

Las condiciones de operación de presión y temperatura del BHD son continuamente medidos por medio de ZZYY-PIT-1002 y ZZYY-TE-1002 por cada pozo antes de enviar la producción de crudo a la válvula multipuerto (YY indica el número del pozo o 00 para localización del cluster). La línea de gas asociado está conectada a la línea del cabezal del pozo. Por esto, una válvula de presión autorreguladora (ZZYY-PCV-1301) está instalada en la línea de gas y ajustada a 150 psig.

En operación normal, la producción es enviada a la estación de flujo MPE-3 a través de las líneas de distribución de producción principal. La línea de prueba de pozo es conectada a la válvula multipuerto (ZZ00-UVM-1003). Las señales de la

válvula multipuerto son enviadas vía comunicación serial (RS-485 usando protocolo Modbus) desde el Panel de Control Local al PLC del cluster y al sistema SCADA.

Un Skid de Medición de Flujo multifásico (ZZ00-U-1001) está colocado para medir la producción de operación de los pozos, la cual se compara con la obtenida por la prueba de pozos. Todas las variables de medición (densidad de la mezcla, presión, temperatura, caudal de diluente, caudal de Bitumen, caudal de gas, corte de agua, etc.) son enviados vía comunicación serial (RS-485 usando protocolo Modbus) al PLC de los clusters y al sistema SCADA.

De acuerdo a los procedimientos típicos de prueba, cada pozo es probado una vez al mes durante 24 horas.

Cada cluster tiene un sistema de distribución de diluente que permite la inyección de diluente dentro de cada pozo. Este procedimiento es llevado a cabo a través de "well casing" o chaqueta de protección del pozo por medio de un control de flujo activado por el controlador ZZYY-FIC-1201 y ZZYY-FV-1201, de acuerdo al caudal de diluente medido por ZZYY-FIT-1201.

La tasa de inyección de diluente está estimada alrededor de 25% de la tasa de producción de Bitumen seco del pozo. La presión máxima de inyección de diluente está fijada en 350 psig. Un by-pass con una válvula de globo manual está colocado con la finalidad de inyectar diluente superficialmente en caso de ser requerido. Esta válvula también permite regular manualmente la presión de inyección de diluente la los niveles requeridos. Para este propósito, dos indicadores locales de presión están colocados (aguas arriba ZZYY-PI-1201 y aguas abajo ZZYY-PI-1203 de la válvula de globo manual) para monitorear las variaciones de presión cuando la válvula de globo está siendo manipulada.

Finalmente, el BHD desde cada cluster es colectado y enviado a través de las líneas de producción principal hacia los múltiples de producción en la estación de flujo MPE-3.

El diluente es distribuido a cada cluster desde la estación de flujo MPE-3 por medio de una múltiple salida y su correspondiente línea de distribución principal.

Adicionalmente, un Paquete compresor de Aire (ZZ00-U-2001) ha sido instalado o previsto para suplir aire de instrumento a los sistemas neumáticos existentes en las Facilidades de Superficie. Este paquete cuenta con su propio panel indicando las siguientes señales:

- Alarma de alta presión en la descarga del compresor.
- Alarma de baja presión a la salida del receptor de aire.
- Alarma de baja-baja presión a la salida del receptor de aire. En este caso se toman acciones de apagado de todo el sistema de compresión de aire.

El estado de operación del sistema compresor de aire es monitoreado continuamente en el PLC del cluster.

Para monitoreo, control y supervisión, un PLC/RTU está instalado en cada cluster. Toda la data de las bombas electro-sumergibles, condiciones operativas de cada Pozo (presión y temperatura), presión de operación de cada línea de producción principal y toda la data del Skid de medición de flujo multifásico es enviado (vía radio) a la sala de control de la estación de flujo MPE-3 y cierta información al sistema SCADA.

3.2.2. Estación de Flujo MPE-3

3.2.2.1. Facilidades de Entrada de BHD

La estación de flujo MPE-3 ha sido diseñada con una capacidad de 140 MBPSD de Bitumen húmedo diluido (BHD) y 23 MMSCFD de gas asociado.

Las líneas de unión de producción principal desde los cluster son recolectadas en un múltiple de producción de 30". El múltiple de entrada trabaja a una presión de operación 60 psig. El flujo multifásico desde los cluster es enviado directamente a los separadores de producción (separadores horizontal gas/líquido) 0002-V-1001A/B. Estos separadores están colocados en paralelo, y tienen suficiente capacidad para permitir la separación inicial de las fases gas/líquido (70 MBPD y 11,5 MMSCFD cada uno).

Los separadores de producción operan a 60 psig y 100°F aproximadamente. Los químicos antiespumantes y demulsificadores son inyectados aguas arriba de los separadores de producción a medida que sean requeridos.

La presión de operación de los separadores de producción es mantenida por medio de un sistema de control de presión localizado en las líneas de salida de gas. Las válvulas de control de presión 0002-PV-1302/1305 constituyen los elementos finales de control, los cuales son activados por medio de los controladores 0002-PIC-1302/1305 respectivamente para cada separador de producción 0002-V-1001A/B.
Cada separador de producción cuenta con un sistema de control de nivel (0002-LT-1005/1015) activados por medio del transmisor de nivel 0002-LT-1005/1015. Estos sistemas de control manipulan las válvulas de control 0002-LV-1005/1015 respectivamente para cada recipiente con la finalidad de mantener el nivel de líquido requerido.

Ante la presencia de un escenario de sobrepresión, estos recipientes están protegidos por las válvulas de alivio 0002-PSV-1300/1301 para el separador de producción 0002-V-1001A, y con 0002-PSV-1303/1304 para el separador de producción 0002-V-1001B.

Se han instalado dos válvulas (con un punto de ajuste "set point" de 85 psig) por cada recipiente para disponer de una válvula auxiliar si alguna operación de mantenimiento es requerida en cualquier momento y por seguridad en caso de falla de una de las válvulas. Esto garantiza la segura operación continua de los separadores.

Como parte del proceso de separación de gas/líquido, el Bitumen húmedo diluido es transferido a un tanque pulmón 0002-TK-1001, el cual opera a pocas pulgadas por debajo de la presión atmosférica. El propósito de esto es separar algunos componentes livianos que todavía se encuentren en la fase líquida, garantizando un crudo con las características requeridas que permitan la operación estable de la planta Deshidratadora/Desaladora. La temperatura de operación es continuamente monitoreada en el tanque 0002-TK-1001 por medio del transmisor de temperatura 0002-TT-1038. La presión de operación en el tanque es establecida por medio de un sistema de control de presión 0002-PIC-1323 localizado en el cabezal de venteo.

El tanque pulmón está protegido contra vacío y condiciones de sobrepresión por la válvula 0002-PSVS-1321 (de acuerdo a lo establecido en el API STD 2000), el cual será activado a 2" H_2O para vacío y 8" H_2O para sobrepresión.

Adicionalmente, el nivel de líquido es continuamente monitoreado en la sala de control y por el sistema SCADA a través del 0002-LIT-1033.

Después de la separación de gas/líquido, el Bitumen húmedo diluido es transferido a la Planta Deshidratadora/Desaladora (Planta DD) por medio de las bombas de transferencia de BHD 0002-P-1001A/B/C (dos en operación y una de respaldo), tipo tornillo con una capacidad de diseño de 2300 gpm y cabezal diferencial de 760 pies cada una.

La presión del cabezal de descarga es controlada por medio del sistema de control de presión 0002-PIC-1036. Para esto, el indicador-transmisor de presión 0002-PIT-1036 localizado en el cabezal de descarga mide la presión de operación y envía una señal al controlador de presión el cual manipula la válvula 0002-PV-1036 localizada en la línea de recirculación hacia el tanque pulmón.

Cada bomba está provista con una válvula de alivio (0002-PSV-1007/1017/1038 respectivamente para 0002-P-1001A/B/C) con la finalidad de proteger el sistema de bombeo de condiciones de sobrepresión.

El procedimiento de encendido de las bombas de transferencia de BHD 0002-P-1001A/B/C pude ser llevado a cabo localmente o remotamente con manipular los interruptores 0002-HS-1013/1023/1029 respectivamente, localizados en los paneles locales de las bombas.

En el caso particular de la bomba de respaldo 0002-P-1001C, es arrancada automáticamente (de acuerdo a la lógica del sistema de control), en caso de que alguna de las bombas principales deje de operar debido a fallas mecánicas. Cabe resaltar que el apagado de la bomba 0002-P-1001A o 0002-P-1001B debido a la falla del equipo es un permisivo para arrancar la bomba 0002-P-1001C.

El panel local de las bombas cuenta con un interruptor de parada local/remoto 0002-HS-1012/1022/1028 para cada bomba. El arreglo típico de las variables

monitoreadas de las bombas incluye falla e indicadores de parada/arranque (para referencia ver plano: PP-000415-120-16201-D0003).

Antes que el BHD sea bombeado hacia la planta DD, este es medido a través del Sistema Medición de flujo de transferencia de Custodia de BHD (unidad LACT) 0002-U-1001. La unidad LACT está diseñada para manejar 457gpm (caudal correspondiente a 140 MBPSD) y monitorear la densidad de la mezcla, corte de H_2O, flujo total, presión, temperatura, incluyendo sistema de muestreo para control de calidad del Bitumen húmedo diluido enviado hacia la planta DD para los procesos de desalación y deshidratación.

3.2.2.2. Manejo del Gas

El gas separado en los separadores de producción 0002-V-1001A/B es enviado hacia el depurador vertical 0002-V-1301 bajo el control de presión activado por el 0002-PIC-1302/1305 respectivamente, el cual regula el porcentaje de apertura de las válvulas 0002-P-1302/1305 con la finalidad de mantener la presión de operación de los separadores alrededor de 60 psig.

El depurador de gas tiene suficiente capacidad para manejar el caudal máximo esperado (23 MMSCFD) y una cantidad de condensado de 3000 BPSD. Aquí la espuma del líquido es removida constantemente y cualquier líquido condensado en el fondo del depurador es enviado al tanque de BHD 0002-TK-1001. Para esta operación se tiene una válvula ON/OFF 0002-YV-1830 en la salida de líquido del depurador de gas.

Para escenarios de sobrepresión, el depurador de gas está protegido con válvulas de alivio 0002-PSV-1810/1811. Dos válvulas (con un punto de ajuste “set point” en 65 psig) han sido instaladas con la finalidad de proveer una válvula de respaldo si cualquier operación de mantenimiento es requerida en algún momento. Esto garantiza la segura operación continua del recipiente y de todo el sistema.

Está colocado un by-pass aguas abajo del depurador de gas para desviar el caudal de gas durante alguna condición de avería. Este sistema también garantiza la

presión constante de entrada a la Planta Compresora a través del sistema de control de presión 0002-PIC-1819.

El gas depurado es medido a través del elemento de flujo tipo vortex 0002-FE-1314 y totalizado por medio del 0002-FQI-1314, con compensación de presión y temperatura, cuya señal es enviada al sistema de control de la estación y al SCADA.

Un sistema de medición de flujo adicional (elemento de flujo tipo vortex 0002-FE-1320 y totalizado por medio de 0002-FQI-1320, con compensación de presión y temperatura) está instalado aguas abajo del by-pass. Esto permite determinar, por medio de balance de masas, el gas a ser quemado en el sistema de mechurrio con la finalidad de establecer los reportes gubernamentales en lo referente a producción de gas.

Para estos reportes gubernamentales, el gas a ser quemado debe ser analizado para determinar su calidad y así garantizar la no contaminación del ambiente. Para esto se instala un analizador cromatográfico en línea aguas abajo del depurador de gas pero aguas arriba del by-pass. Una vez depurado, el gas es enviado hacia el Paquete de Compresión de Gas 0006-U-1301 para compresión inicial hasta 590 psig, luego es enviado directamente al Paquete de tratamiento de Gas 0006-U-1302 para tratamiento de $H_2O/H_2S/CO_2$. Ambos paquetes están físicamente localizados dentro del área de la estación de flujo MPE-3.

3.2.2.3. Servicios

Los servicios de la Estación de Flujo incluyen:

a. Paquete Compresor de aire

El Paquete de Compresión de Gas 0002-U-2001 está colocado en la estación de flujo con suficiente capacidad para suplir aire de instrumento a los sistemas neumáticos. La presión de aire de instrumento está fijada alrededor de 100 psig.

b. Abastecimiento de Energía Eléctrica

Un sistema de energía eléctrica está diseñado e instalado en la estación de flujo MPE-3 para proveer de energía eléctrica a todos los equipos de la estación de

flujo así como la de los Cluster (motores de las bombas, iluminación instrumentos, sistemas de control, facilidades de comunicación, RTU's).

c. Sistemas de Drenaje

El agua contaminada y los drenajes aceitosos de los equipos del proceso son recolectados en un sistema de drenaje abierto, el cual incluye alcantarillas localizadas cerca de los equipos del proceso en áreas encerradas. Estas alcantarillas transfieren el agua aceitosa a través del sistema de tuberías del drenaje. Este sistema termina en el sumidero de recolección 0002-X-1701.

Referente a los drenajes cerrados de los equipos, estos son recolectados en un cabezal de 4" el cual lleva este producto al tambor K.O. del mechurrio 0002-V-1801.

Cuando el tambor alcanza el nivel alto de líquido, la bomba principal del tambor K.O. 0002-P-1801A es arrancada o puesta en operación. Los drenajes colectados son retornados al proceso, hacia el tanque 0002-TK-1001 para su reprocesamiento. Si el nivel de líquido continúa incrementando y alcanza el nivel alto-alto de líquido, la bomba de respaldo 0002-P-1801B entra en operación. Ambas bombas son detenidas cuando el nivel bajo y bajo-bajo en el tambor es respectivamente alcanzado.

El arranque/parada de estas bombas es activado desde el PLC debido a la medición del transmisor de nivel 0002-LT-1801, localizado en el tambor K.O. del mechurrio 0002-V-1801.

d. Sistema de Agua Contra Incendio / Agua de Servicios

Un tanque común para el sistema de agua contra incendio y Agua de Servicio 0002-TK-1901 con una capacidad de 11,84 MBbls ha sido instalado.

El agua es extraída de pozos localizados cerca del área de la estación de flujo MPE-3. Para este servicio, una bomba vertical sumergible 0002-P-2401 está instalada para bombear el agua desde los pozos hacia el tanque de agua de extinción de incendio con una capacidad de diseño mínima de 605 gpm de acuerdo a las normas de sistemas de extinción de incendios.

El agua contenida entre los niveles alto y alto-alto en el tanque 0002-TK-1901 es la empleada como agua para los servicios de las utilidades. El resto del volumen de agua es mantenida constante para el sistema de extinción de incendios.

3.2.2.4. Sistema de Inyección de Diluente

El proyecto contempla un área física independiente donde se almacena el Diluente que se requiere para facilitar el transporte del BHD, esta área física se denomina Sistema de Distribución y Almacenamiento de Diluente (DSDS) El Diluente se envía desde el DSDS al Tanque de Almacenamiento de Diluente 0002-TK-1201 en la estación de flujo MPE-3. La capacidad de operación del tanque es alrededor de 5 MBbl, el cual garantiza la inyección continua de diluente a los clusters por un tiempo (más de tres horas), en caso de algún problema en DSDS.

El tanque de almacenamiento de diluente 0002-TK-1201 tiene un lazo de control de nivel (0002-LV-1201), el cual controla la alimentación de Diluente al mismo. El lazo de Control prevé alarmas de alto y bajo nivel (por medio del transmisor de nivel 0002-LIT-1201). El caudal de diluente total que se alimenta desde DSDS es medido antes de entrar al tanque por medio del elemento de flujo de tipo ultrasónico 0002-FE-1201. La señal del 0002-FIT-1201 está compensada por temperatura a través del 0002-TT-1201 y es visible en el PLC y el sistema SCADA. Adicionalmente, el nivel de líquido es continuamente monitoreado en el sistema de control y SCADA a través de la indicación 0002-LIT-1201.

El diluente es enviado a cada cluster a través de las líneas de inyección de diluente por medio de las bombas de inyección de diluente 0002-P-1201A/B/C (dos operando y una de respaldo), con una capacidad de diseño de 535,23 gpm y cabezal diferencial de 1610 pies cada una. Manipulando los interruptores local/remoto 0002-HS-1210/1216/1222 respectivamente puede llevarse a cabo el encendido de las bombas 0002-P-1201A/B/C local o remotamente. El arreglo típico de las variables monitoreadas de las bombas incluye falla, indicación del estatus de las bombas (arranque/parada), interruptores local/remoto y de arranque/parada. Estas variables pueden ser leídas desde la sala de control y el sistema SCADA.

La presión del cabezal de descarga de las bombas es controlada por medio del lazo de control 0002-PIC-1225. Para esto, el indicador-transmisor de presión 0002-PIT-1225, localizado en el cabezal de descarga mide la presión de operación y envía una señal al controlador de presión (sistema de Control), el cual manipula la válvula 0002-PV-1225 localizada en el cabezal de descarga. El sistema de bombeo también cuenta con un sistema de recirculación hacia el tanque, para la protección de las bombas en caso de alguna condición de avería, condición de bajo flujo de entrada, la cual genera que el flujo de diluente en el cabezal de descarga disminuya. Este sistema está compuesto por la válvula de control de flujo 0002-FV-1202, manipulada por el controlador de flujo 0002-FIC-1202 y el elemento de flujo tipo placa orificio 0002-FE-1202.

El caudal del diluente es continuamente medido por medio de 0002-FE-1202 en el cabezal de descarga de las bombas, en caso de que una condición de flujo mínimo sea detectada el transmisor de flujo 0002-FIT-1202 envía una señal al controlador de flujo en el sistema de control. Y la acción opera automáticamente la válvula de control 0002-FV-1202.

3.2.2.5. Inyección de Químicos

La inyección de antiespumantes y demulsificantes son requeridos antes del proceso de separación gas/líquido. Por esta razón, han sido colocadas las facilidades para inyectar estos productos aguas arriba de los separadores de producción 0002-V-1001A/B/C. Por lo tanto el Paquete de Inyección de Demulsificante 0002-U-2101 y el Paquete de Inyección de Antiespumante 0002-U-2102 están considerados como parte de las facilidades de la estación de flujo MPE-3.

3.2.2.6. Facilidades del Sistema de Mechurrios

Las facilidades de Mechurrios cuenta con un tambor de “knock out drum” (tambor K.O.) 0002-V-1801 diseñado para manejar hasta 23 MMSCFD y 3000 BPSD de líquido.

Este líquido condensado es bombeado de vuelta al tanque de Bitumen por medio de las bombas del tambor K.O. 0002-P-1801A/B (una en operación y una de respaldo). Estas operan de forma discontinua. La señal de nivel alto-alto medida por el 0002-LT-1815 arranca la bomba principal 0002-P-1801A, y la señal de nivel bajo-bajo también medida por el 0002-LT-1815 la detiene. En caso de que el nivel continúe incrementando, la señal de nivel alto-alto arranca la bomba de respaldo 0002-P-1801B y la señal de nivel bajo la detiene.

Adicionalmente, el transmisor de nivel 0002-LT-1804 ha sido incluido en el tambor K.O. para monitorear de forma continua el nivel en el recipiente desde la sala de control.

El arranque inicial de las bombas 0002-P-1801A/B se puede llevar a cabo manipulando los interruptores local/remoto 0002-HS-1810/1815 (respectivamente para cada bomba) localizados en el panel local de las bombas, y activando el botón de pulsar arranque/parada.

El arreglo típico de las variables monitoreadas en el PLC de estas bombas incluye falla, indicación del estatus de las bombas (arranque/parada) e interruptor remoto de arranque/parada.

El gas es enviado al mechurrio de alta presión 0002-X-1801 para ser quemado, el cual está diseñado para manejar un caudal máximo de 23 MMSCFD. El sistema de mechurrio está provisto con un paquete de ignición (0002-X-1802) con generador de llama electrónico (como opción primaria de ignición) y frontal (como respaldo manual).

Adicionalmente existe un sistema de mechurrio de baja presión (LP low pressure) para permitir desviar el gas recuperado desde el proceso bajo las siguientes condiciones: mantener la presión requerida en la entrada de la unidad Recuperadora de Vapor (0002-X-1301) o si algún problema es detectado en la unidad y ésta debe ser apagada. La capacidad de diseño de este sistema es de 2,42 MMSCFD.

Cada sistema de mechurrio (0002-X-1801/1803) tiene un panel de control dedicado para el control de la operación. El gas residual del paquete de la planta de

compresión de gas 0006-U-1301 es llevado continuamente al sistema de mechurrio a una presión de 25 psig para ser quemado.

Una válvula de globo manual y un medidor de flujo tipo rotámetro (0002-FI-1818) están colocados para controlar el caudal de gas de purga para este servicio. Adicionalmente, una válvula reguladora ha sido colocada para mantener la presión de operación al nivel requerido. Para el servicio de ignición y gas piloto, se toma gas de proceso desde la salida del depurador de gas 0002-V-1301 con la finalidad de cubrir este requerimiento.

3.2.3. Sistema de Distribución y Almacenamiento de Diluente (DSDS)

Los tanques de almacenamiento de Diluente 0004-TK-1201/1202 están diseñados con una capacidad de 138 MBbl cada uno, los cuales proveen suministro de diluente continúo. Estos tanques trabajan de forma alternada; es decir, que mientras un tanque está siendo usado para recibir y almacenar diluente, el otro está entregando diluente a las estaciones requeridas. Para realizar estas operaciones se cuenta con varias válvulas motorizadas localizadas en las entradas y salidas de cada tanque. Para el tanque 0004-TK-1201 se tienen las válvulas 0004-YV-1263/1264 en la entrada/salida y para el tanque 0004-TK-1202 se tienen las válvulas 0004-YV-1265/1266 en la entrada/salida.

El cabezal de alimentación de diluente está provisto con la válvula de cierre de emergencia “shutdown” 0004-SDV-1200. Esta válvula es activada en caso de que el diluente en algunos de los tanques alcance el nivel de líquido alto-alto, el cual es detectado por medio de los transmisores de nivel 0004-LT-1202/1262 respectivamente para cada tanque. Esta acción evita cualquier condición de sobrellenado en el tanque. Adicionalmente una alarma es activada en el sistema de control y SCADA.

El nivel de líquido es monitoreado independientemente en cada tanque por medio de los transmisores de nivel 0004-LIT-1201/1261 respectivamente para cada tanque. Además, alarmas de bajo y alto nivel están configuradas en la sala de control

y el SCADA. El diluente es enviado a todas las estaciones de flujo y planta Deshidratadora/Desaladora a través de una tubería de 21km de largo y 12" de diámetro. Esto es realizado por medio de las bombas de diluente 0004-P-1201A/B/C. Cabe resaltar que las bombas en operación succionarán desde un tanque común. Cada bomba está diseñada con una capacidad de 1070 gpm y un cabezal diferencial de 540 pies. La presión del cabezal de descarga de las bombas es controlada por medio del lazo de control 0004-PIC-1270. Para esto, el transmisor-indicador de presión 0004-PIT-1270, localizado en el cabezal de descarga, mide la presión de operación y envía una señal al controlador de presión el cual manipula a la válvula 0004-PV-1270 localizada en el cabezal de descarga.

El procedimiento de arranque de las bombas 0004-P-1201A/B/C puede ser llevado a cabo local o remotamente manipulando los interruptores local/remoto 0004-HS-1210/1217/1224. El panel consta además de un interruptor de parada local/remoto 0004-HS-1209/1216/1223 para cada bomba. Con el propósito de proteger las bombas en caso de condiciones mínimas de flujo, se tiene una línea de recirculación de 4"con un lazo de control de flujo colocado en el lado de descarga de cada bomba. El caudal del diluente es continuamente monitoreado en cada línea de descarga, pero si se detecta una condición de flujo mínimo, el transmisor de nivel 0004-FIT-1226/1227/1228 envía una señal al sistema de control para que el FIC, controlador de flujo manipule la válvula 0004-FV-1226/1227/1228.

Para monitoreo y supervisión, una RTU está instalada en el área de DSDS. El nivel de líquido de los tanques de almacenamiento, caudal de diluente entregado a las estaciones de flujo y las señales de las bombas son enviadas a la sala de control de la estación de flujo MPE-3 y al sistema SCADA.

3.2.3.1. Servicios

El área del DSDS cuenta con los siguientes servicios:

a. Paquete Compresor de Aire

El Paquete de Compresión de Gas 0004-U-2001 está colocado en el área de DSDS con suficiente capacidad para suplir aire de instrumento a los sistemas

neumáticos. La presión de aire de instrumento está fijada alrededor de 100 psig máxima y 60 psig mínima.

b. Abastecimiento de Energía Eléctrica

Los requerimientos eléctricos del área DSDS son suplidos por una línea de distribución de 35,5kV. Este sistema de abastecimiento de energía eléctrica es requerido para los siguientes elementos:

- Todas las señales de los instrumentos y sistemas de control.
- Motores de las bombas de diluente (0004-P-1001A/B/C).
- Paquete de compresión de aire (0004-U-2001).
- Servicios generales: iluminación, etc.

c. Sistemas de Drenaje

El agua contaminada y los drenajes aceitosos de los equipos del proceso son colectados en un sistema de drenaje abierto, el cual incluye alcantarillas localizadas cerca de los equipos del proceso en áreas encerradas. Estas alcantarillas transfieren el agua aceitosa a través del sistema de tuberías del drenaje. Este sistema termina en el sumidero de recolección 0004-X-1701.

d. Sistema de Agua Contra Incendio / Utilidades

Un tanque común para el sistema de agua contra incendio y utilidades 0004-TK-1901 con una capacidad de 25 MBbls ha sido colocado.

Como se mencionó anteriormente, el tanque del sistema contra incendio suple de agua las utilidades y a la red de sistema contra incendio.

El agua es extraída de pozos localizados cerca del área de DSDS. Para este servicio, una bomba vertical sumergible 0004-P-2401 está colocada para bombear el agua desde los pozos hacia el tanque de agua de extinción de incendio con una capacidad de diseño mínima de 1453 gpm de acuerdo a las normas de sistemas de extinción de incendios.

El agua contenida entre los niveles alto y alto-alto en el tanque 0004-TK-1901 es la empleada como agua para los servicios de las utilidades. El resto del volumen de agua es mantenida constante para el sistema de extinción de incendios.

3.3. Datos del sitio

Los datos que se presentan a continuación corresponden al lugar de ubicación de la planta bajo estudio.

a) Temperatura Ambiental

Tabla 3.1. Temperatura ambiental

Max Temperatura	90 ºF (32.2 ºC)
Min. Temperatura	72 ºC (22 ºC)
Promedio	82.4 ºF (28 ºC)

b) Velocidad y dirección del viento

Tabla 3.2. Velocidad y dirección del viento

Velocidad Max. del Viento	22.1 *m/s* (72 *ft/s*)
Velocidad Promedio del Viento	17.5 *m/s* (57.4 *ft/s*)
Dirección Predominante del Viento	Noreste (NE)

c) Precipitación

Tabla 3.3. Precipitación

Cantidad Max.	1300 mm/año
Cantidad Min.	800 mm/año
Temporada de lluvia	7 meses (Mayo - Noviembre)
Temporada de sequía	5 meses (Diciembre - Abril)

d) Humedad relativa

Tabla 3.4. Humedad Relativa

Max.	100 %
Min.	82 %
Promedio	97 %

e) Características sísmicas (COVENIN 1756 – Zona 4)

Tabla 3.5. Características sísmicas

Aceleración Horizontal	0.25 g
Aceleración Vertical	0.7 g

f) Características del Suelo

Tipo de suelo: arenoso.

3.4. Propiedades de la materia prima

Las materias primas con que se trabaja en el proceso son: Bitumen húmedo diluido (BHD), gas asociado y diluente.

3.4.1. Bitumen Húmedo diluido

Las características del Bitumen húmedo diluido (BHD) se presentan a continuación:

Tabla 3.6. Análisis químico de BHD

	COMPONENTE	mol	%	COMPOSICIÓN MOLAR
Bitumen neto seco	Carbón	0.829	0.187	0.1550230
	Hidrógeno	0.106	0.187	0.0198220
	Nitrógeno	0.0078	0.187	0.0014580
	Sulfuro	0.0543	0.187	0.0101541
	Oxígeno	0.0029	0.187	0.0005423
Nafta	n-heptano	0.5	0.7317	0.3658500
	2-methyl heptano	0.5	0.7317	0.3658500
Agua	H20	1	0.0813	0.0813000

Tabla 3.7. Análisis físico de BHD

Peso residual	98.34	
% Peso (residual)	52.75%	
Gravedad ºAPI @ 60 ºF	16 ± 1	
Gravedad específica @ 60/60 ºF	0.9625	
Densidad @ 86 ºF	59.46	lb / ft^3
Viscosidad dinámica @ 100 ºF @ 320 ºF	442 - 413 4.73 - 4.71	*cP* *cP*
Calor de Combustión	15278 - 14470	*Btu/lb*
Contenido de NaCl	689 - 848	*Lb/1000 Bbl*
Contenido de agua (basado en Bitumen neto seco)	10 - 12	% volumen

3.4.2. Gas asociado

Las características del gas asociado se describen a continuación:

Tabla 3.8. Composición Gas asociado

COMPONENTE	COMPOSICIÓN MOLAR (%)	GPM
N2	0.32	0.000
CO2	13.69	0.000
C1	85.15	0.000
C2	0.34	0.000
C3	0.28	0.076
i-C4	0.04	0.013
n-C4	0.08	0.025
i-C5	0.02	0.006
n-C5	0.01	0.003
C6+	0.07	0.084

H2S (*ppm V/V*): 30

GPM Total: 0.17

Gravedad específica a 60º F: 0.697

Calor de combustión total (*BTU/SCF*) 883

Peso Molecular (*Lb/mol*): 20.2

3.4.3. Diluente

Las características de la nafta empleada como diluente son las siguientes:

Tabla 3.9. Análisis de Nafta

Gravedad APIº @60 ºF	50.9
Densidad @ 60 ºF @ 100 ºF @ 120 ºF	48.41 lb/ft^3 47.29 lb/ft^3 46.76 lb/ft^3
Viscosidad Kinemática @ 60 ºF @ 100 ºF @ 120 ºF	1.37 *cSt* 1.32 *cSt* 1.30 *cSt*
Presión de Vapor @ 60 ºF @ 100 ºF @ 120 ºF	1.70 *psi* 2.40 *psi* 3.00 *psi*
Contenido Sulfúrico	0.21 % peso

3.5. Condiciones operacionales de los equipos

A continuación se describen las condiciones operacionales de los equipos del proceso involucrados en el presente estudio.

3.5.1. Equipos mayores del proceso

Tabla 3.10. Condiciones operacionales de equipos mayores del proceso

Sistema/Equipo	Identificador	Presión *(psig)*	Temperatura *(^oF)*	Capacidad (MBbls)
Separador de producción	0002-V-1001 A/B	85	150	---
Tanque de BHD	0002-TK-1001	15.3	150	7272
Depurador de Gas	0002-V-1301	65	150	---
Tanque Amortiguador de Diluente	0002-TK-1201	Atm	140	6808
Tambor K.O.	0002-V-1801	50	150	---
Tanque Almacenamiento de Diluente	0004-TK-1201/2	Atm	140	174

3.5.2. Equipos menores del proceso

Tabla 3.11. Condiciones operacionales de equipos menores del proceso

Sistema/Equipo	Identificador	Capacidad de diseño *(gpm)*	Cabezal diferencial *(ft)*	Capacidad hidráulica *(HP)*	Presión min de succión *(psig)*	Presión max de descarga *(psig)*
Bomba de transferencia de BHD	0002-P-1001A/B/C	2300	760	419.4	-2.76	309.91
Bomba de inyección de diluente	0002-P-1201A/B/C	535.23	1610	166	-1.51	529.74
Bombas de Tambor K.O.	0002-P-1801A/B	142.3	70	2	-3.03	23.59
Bomba Agua Cruda	0002-P-2401	605	---	---	-0.89	150
Bombas de diluente	0004-P-1201A/B/C	1070	540	112	-1.93	178.44
Bomba Agua Cruda	0004-P-2401	1453	---	---	-0.89	150

CAPÍTULO IV

DETERMINACIÓN DEL NIVEL DE INTEGRIDAD DE SEGURIDAD (SIL)

El Nivel de Integridad de Seguridad (SIL) de la planta y proceso bajo estudio se determinó de forma cualitativa y cuantitativa.

4.1. Metodología empleada para la determinación del Nivel de Integridad de Seguridad (SIL)

Para la determinación de Nivel de Integridad de Seguridad (SIL) de la planta y proceso bajo estudio, se empleó la siguiente metodología basada en la norma PDVSA IR-P-02:

a) **Estudio del proceso + BPCS**

Este estudio permite conocer el proceso a evaluar y obtener información de vital importancia en la determinación del Nivel de Integridad de Seguridad (SIL).

b) **Identificación de Peligros**

Se identifican los peligros y las causas que pudieran llevar el proceso a un estado no seguro, entendiéndose éste como liberación incontrolada de energía y/o productos tóxicos.

c) Identificación de Capas Independientes de Protección Diferentes del SIS.

Las IPL se identifican con la finalidad de ser consideradas en la estimación de frecuencias de los eventos peligrosos.

d) **Determinación del SIL empleando un Método Cualitativo.**

Se lleva a cabo un estudio cualitativo para establecer una primera aproximación del SIL de la planta.

***e)* Determinación del SIL empleando un Método Cuantitativo.**

Se realiza un estudio cuantitativo para establecer una segunda aproximación del SIL de la planta.

***f)* Comparación y Análisis de los resultados.**

Con la finalidad de establecer el SIL definitivo de la planta, se realiza una comparación de los resultados obtenidos por los métodos cualitativos y cuantitativos y se analiza la confiabilidad de cada uno de los resultados.

4.2. Estudio del Proceso

En primer lugar se realizó la recopilación y estudio de los documentos "Bases de Diseño", "Filosofía de Operación y Control", Diagramas de Flujo del Proceso y Diagramas de Tuberías e Instrumentación (P&ID) del proceso bajo estudio. Esto se realizó con la finalidad de conocer el objetivo y alcance de la instalación estudiada. La descripción de la planta y del proceso se detalla completamente en el capítulo III del presente documento. Por otra parte, los Diagramas de Tubería e Instrumentación (P&ID) y Diagramas de Flujo del Proceso se presentan en el anexo 5.

4.3. Identificación de los Eventos Peligrosos

La identificación de peligros se llevó a cabo por medio de la identificación de los lazos críticos que pudieran llevar al proceso a un estado no seguro. Los lazos críticos que se consideraron para la determinación del Nivel de Integridad de Seguridad del proceso bajo estudio se describen en la tabla 4.1. Es importante resaltar que para sistemas y/o equipos que por su similitud en diseño, instrumentación y condiciones de proceso, presentan lazos críticos iguales (como por ejemplo los separadores de producción 0002-V-1001 A y B) se analiza uno sólo de estos lazos, teniendo en cuenta que los resultados que se obtengan del estudio son aplicables de forma igual y por separado a cada uno de estos sistemas y/o equipos.

Tabla 4.1. Lazos críticos

Lazo	Plano	Sistema/Equipo Principal	Descripción del Lazo	Consecuencia
01	110-D0001	Arreglo típico de pozos	Avería del pozo	Pérdida de producción del pozo - Daño mayor al ambiente
02	120-D0002	Separadores de producción 0002-V-1001A/B	Sobrepresión en separador de producción	Avería del proceso - Posible daño del equipo - Posible daño al ambiente
03	120-D0002	Separadores de producción 0002-V-1001A/B	Sobrenivel de liq. en separador de producción	Avería del proceso - Posible daño del equipo - Posible daño al ambiente
04	120-D0003	Bomba 0002-P-1001A/B/C	Falla bomba principal de transferencia de BHD	Daño mayor al equipo - Posible avería del proceso
05	120-D0003	Tanque de BHD 0002-TK-1001	Sobrepresión en el tanque de BHD	Avería del proceso - Posible daño del equipo - Posible daño al ambiente
06	120-D0003	Tanque de BHD 0002-TK-1001	Sobrellenado de líquido en el tanque de BHD	Pérdida de BHD - Daño mayor al ambiente - Posible lesión al personal
07	120-D0004	Depurador de Gas 0002-V-1301	Sobrepresión en el depurador de gas	Avería del proceso - Posible daño del equipo - Posible daño al ambiente
08	120-D0004	Depurador de Gas 0002-V-1301	Sobrenivel de condensado en el depurador de gas	Avería del proceso - Posible daño del equipo
09	120-D0005	Tanque amortiguador de diluente 0002-TK-1201	Sobrellenado de líquido en el tanque amortiguador de diluente	Pérdida de diluente - Daño menor al ambiente - Posible lesión al personal
10	120-D0005	Bomba 0002-P-1201A/B/C	Falla bomba principal de inyección de diluente	Daño mayor al equipo - Posible avería del proceso
11	120-D0007	Tambor K.O. Del mechurrio 0002-V-1801	Sobrepresión en el tambor K.O. del mechurrio	Avería del proceso - Posible daño del equipo - Posible daño al ambiente
12	120-D0007	Tambor K.O. Del mechurrio 0002-V-1801	Sobrenivel de liq. en el tambor K.O. del mechurrio	Avería del proceso - Posible daño del equipo
13	120-D0007	Bomba 0002-P-1801A/B	Falla bomba principal del tambor K.O.	Daño mayor al equipo - Avería del proceso
14	120-D0012	Tanque agua extinción de incendio 0002-TK-1901	Falta de agua en el tanque	Daño al sistema de bombeo contra incendio - Incapacidad de control de incendios
15	130-D0001	Tanque 0004-TK-1201/2	Sobrellenado de líquido en el tanque de almacenamiento de diluente	Pérdida de diluente - Daño menor al ambiente - Posible lesión al personal
16	130-D0001	Bomba 0004-P-1201A/B/C	Falla bomba principal de inyección de diluente	Daño mayor al equipo - Posible avería del proceso
17	130-D0004	Tanque agua extinción de incendio 0004-TK-1901	Falta de agua en el tanque	Daño al sistema de bombeo contra incendio - Incapacidad de control de incendios

4.4. Identificación de IPL'S diferentes del SIS

Las capas independientes de protección (IPL) identificadas se muestran a continuación en la tabla 4.2 ordenadas según el lazo crítico que afecten.

Tabla 4.2. Capas Independientes de Protección

Lazo	Plano	IPL
01	110-D0001	Integridad mecánica
02	120-D0002	PSV1800 - PSV1801
03	120-D0002	PSV1800 - PSV1801
04	120-D0003	PSV1007
05	120-D0003	PVSV1321
06	120-D0003	Dique de contención
07	120-D0004	PSV1810 - PSV1811
08	120-D0004	PSV1810 - PSV1811
09	120-D0005	Dique de contención
10	120-D0005	---
11	120-D0007	---
12	120-D0007	---
13	120-D0007	---
14	120-D0012	---
15	130-D0001	Dique de contención
16	130-D0001	---
17	130-D0004	---

4.5. Determinación del SIL por método cualitativo

Para la determinación del Nivel de Integridad de Seguridad (SIL) de forma cualitativa para cada uno de los lazos críticos considerados, se empleó el método de Análisis de Gráfica de Riesgo contemplado en el anexo E de la norma ANSI/ISA 84.00.01-2004 parte 3, el cual se describe en el punto 2.9.1 del capítulo II del presente documento.

Con la finalidad de optimizar el tiempo empleado en el Análisis de Gráfica de Riesgo se desarrolló una aplicación en Microsoft Access usando como plataforma de programación Microsoft Visual Basic para aplicaciones y consultas SQL, que permite

determinar el Nivel de Integridad de Seguridad de acuerdo a la figura 2.3 del capítulo II. Esta aplicación se llamó **"cualitativo"** y su listado puede encontrarse en el anexo 12 con los comentarios y explicaciones de la funcionalidad de los procedimientos desarrollados. En la figura 4.1 se muestra un diagrama de flujo general de la aplicación desarrollada.

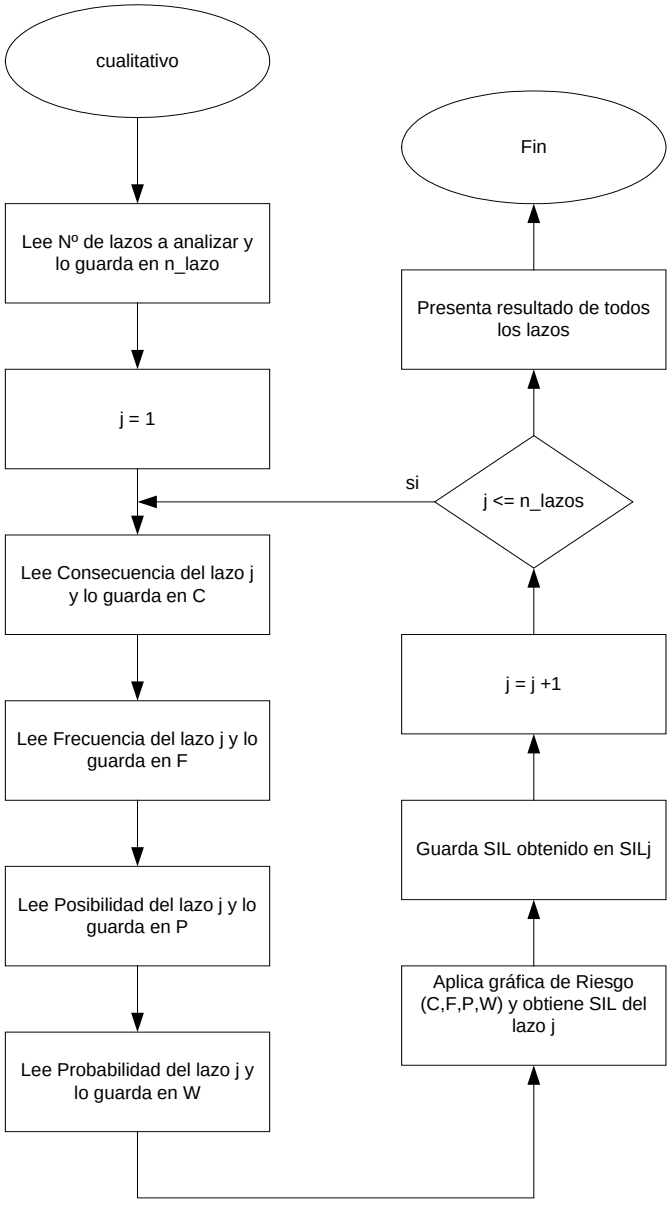

figura 4.1. Diagrama de flujo de "cualitativo"

4.5.1. Utilización de la aplicación “cualitativo”

Los pasos que se deben seguir para utilizar la aplicación “cualitativo” son los siguientes:

1. Pulsar en el botón “Análisis por Método Gráfica de Riesgo” en la interfaz principal (figura 4.1). Esto muestra una nueva ventana denominada formulario de entrada de datos (figura 4.2).
2. Introducir la siguiente información para cada uno de los lazos críticos bajo estudio en el formulario de entrada de datos:
    a. Número o identificador del lazo crítico.
    b. Descripción de lazo crítico.
    c. Nivel de severidad de consecuencia ***(C)*** de acuerdo a la tabla 2.5 del capítulo II.
    d. Nivel de frecuencia de exposición en la zona peligrosa ***(F)*** de acuerdo a la tabla 2.6 del capítulo II.
    e. Nivel de probabilidad de evitar el evento peligroso ***(P)*** de acuerdo a la tabla 2.7 del capítulo II.
    f. Nivel de probabilidad de ocurrencia del evento peligroso ***(W)*** de acuerdo a la tabla 2.8 del capítulo II.
3. Pulsar el botón “determinar SIL” en el formulario de entrada de datos (figura 4.2)

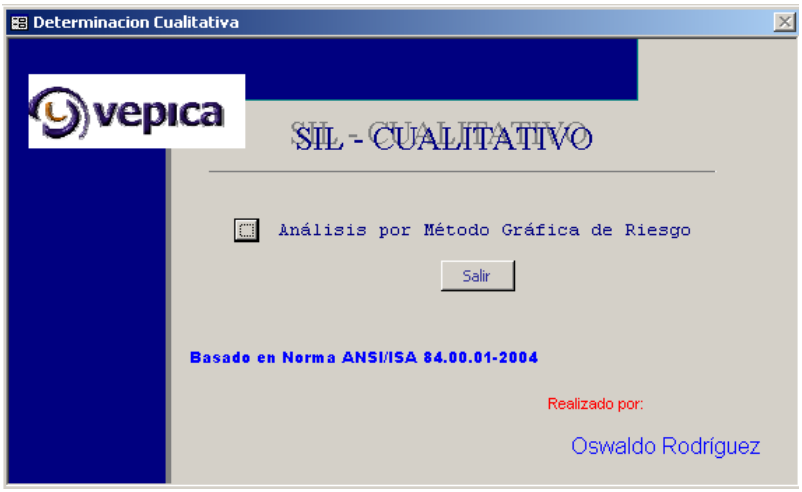

figura 4.2. Interfaz principal del programa “Cualitativo”

figura 4.3. Formulario de entrada de datos

4.5.2. Resultados obtenidos

Los resultados obtenidos de emplear el programa "cualitativo" para la determinación del SIL de forma cualitativa para cada uno de los lazos bajo estudio se muestran en la tabla 4.3.

Tabla 4.3. Resultados de determinación Cualitativa del SIL

Lazo	Evento tope	SIL	Consecuencias (C)	Frecuencia (F)	Posibilidad (P)	Probabilidad (W)
01	Avería del pozo	1	Moderada (C3)	Menor (F1)	Poco Posible (P2)	Muy Baja (W1)
02	Sobrepresión en separador de producción 0002-V-1001A/B	1	Moderada (C3)	Menor (F1)	Posible (P1)	Baja (W2)
03	Sobrenivel de liq. en separador de producción 0002-V-1001A/B	a	Baja (C2)	Menor (F1)	Posible (P1)	Baja (W2)
04	Falla bomba principal de transferencia de BHD 0002-P-1001A/B/C	2	Baja (C2)	Mayor (F2)	Posible (P1)	Moderada a Alta (W3)
05	Sobrepresión en el Tanque de BHD 0002-TK-1001	a	Baja (C2)	Menor (F1)	Posible (P1)	Baja (W2)
06	Sobrellenado de líquido en el tanque de BHD 0002-TK-1001	a	Baja (C2)	Menor (F1)	Posible (P1)	Baja (W2)
07	Sobrepresión en el depurador de gas caso gas 0002-V-1301	2	Moderada (C3)	Menor (F1)	Posible (P1)	Moderada a Alta (W3)
08	Sobre nivel de condensado en el depurador de gas 0002-V-1301	a	Baja (C2)	Menor (F1)	Posible (P1)	Baja (W2)
09	Sobrellenado de liquido en tanque amortiguador de diluente 0002-TK-1201	1	Moderada (C3)	Menor (F1)	Posible (P1)	Baja (W2)
10	Falla bomba principal de inyección de diluente 0002-P-1201A/B/C	1	Baja (C2)	Mayor (F2)	Posible (P1)	Baja (W2)
11	Sobrepresión en el tambor K.O. del mechurrio 0002-V-1801	1	Moderada (C3)	Menor (F1)	Posible (P1)	Baja (W2)
12	Sobrenivel de liq. en el tambor K.O. del mechurrio 0002-V-1801	a	Baja (C2)	Menor (F1)	Posible (P1)	Baja (W2)
13	Falla bomba principal del tambor K.O. 0002-P-1801A/B	2	Baja (C2)	Mayor (F2)	Posible (P1)	Moderada a Alta (W3)
14	Falta de agua en el tanque 0002-TK-1901	a	Moderada (C3)	Menor (F1)	Posible (P1)	Muy Baja (W1)
15	Sobrellenado de liq. en tanque de almac. de diluente 0004-TK-1201/2	1	Moderada (C3)	Menor (F1)	Posible (P1)	Baja (W2)
16	Falla bomba principal de inyección de diluente 0004-P-1201A/B/C	1	Baja (C2)	Menor (F1)	Posible (P1)	Moderada a Alta (W3)
17	Falta de agua en el tanque 0004-TK-1901	a	Moderada (C3)	Menor (F1)	Posible (P1)	Muy Baja (W1)

4.6. Determinación del SIL por método cuantitativo

Para la determinación del Nivel de Integridad de Seguridad (SIL) empleando un método cuantitativo para cada uno de los lazos críticos considerados, se empleó el método de Análisis Semi-Cuantitativo contemplado en el anexo B de la norma ANSI/ISA 84.00.01-2004 parte 3, el cual se describe en el anexo 4 del presente documento. A continuación se describen los criterios y pasos seguidos en el análisis Semi-cuantitativo.

4.6.1. Bases y criterios de los cálculos

Para realizar los cálculos correspondientes a la determinación del SIL de forma cuantitativa se tomaron en cuenta los siguientes criterios:

- Tasa de falla: La tasa de falla de los componentes es constante durante la vida del sistema.
- Redundancia: componentes redundantes tienen iguales ratas de falla y tienen el mismo comportamiento operacional.
- Independencia: se asume que las fallas de los componentes individuales es estadísticamente independiente de los otros componentes, esto es, la falla de cualquier componente no inducirá a falla a los otros componentes.
- Falla de causa común: se asume que los componentes redundantes están sujetos a fallas de causa común. Este se establece en forma de porcentaje y para los efectos de este estudio se asumió igual al 10%.
- Diámetro del orificio de descarga accidental: se utilizó una relación entre el diámetro del orificio y el diámetro de tubería (d/D) de 0,22 la cual se corresponde con una probabilidad de ocurrencia del 85% de las veces, según el documento “Hydrocarbon Leak and Ignition Data Base” del E&P Forum. [9]
- Condiciones meteorológicas del área, composición de los fluidos y condiciones de operación: estas condiciones se describen en los apartados 3.3, 3.4 y 3.5 del capítulo III.

4.6.2. Identificación del nivel de riesgo aceptable permitido

El nivel de riesgo aceptable permitido se determinó empleando la tabla 8 de la norma PDVSA IR-P-02 la cual se plasma en la tabla 4.4.

Tabla 4.4. Nivel de Riesgo Aceptable

Clasificación de la Instalación	Clasificación de la Instalación Nivel de Riesgo Aceptable (ocurrencias/año) de acuerdo a la potencialidad de daños
Normalmente atendida y no atendida con potencial de afectar a terceros	10^{-6}
Normalmente atendida con potencial de afectar a personal propio y/o al ambiente	10^{-5}
No atendida con potencial de producir pérdidas (costo reposición, pérdida de producción) > 100M $	10^{-4}
Normalmente atendida con potencial de afectar a personal propio y/o al ambiente	10^{-3}
Normalmente atendida y no atendida con potencial de afectar a terceros	10^{-2}

4.6.3. Identificación de peligros del proceso

Se describen en el apartado 4.3 del presente capítulo.

4.6.4. Identificación de capas independientes de protección

Las capas independientes de protección se describen en el punto 4.4. Por otro lado el aporte de las capas independientes de protección se muestra en la tabla 4.5.

Tabla 4.5. Aporte de las Capas Independientes de Protección

Capas Independientes de Protección	A_{IPL}
Válvula de Alivio	10^{-1}
Diques	10^{-1}
Integridad mecánica de los equipos	10^{-2}
Disco de ruptura	10^{-2}

4.6.5. Determinación de la frecuencia de ocurrencia de eventos tope

Para determinar la frecuencia de ocurrencia de los eventos topes de cada uno de los lazos críticos considerados se utilizó la técnica de Árboles de Falla. Para ello se empleó el programa Logan Fault and Event Tree Analysis v6.03 de RM Consultants Ltd. Con este software se realizó el desarrollo y cálculo de cada uno de los árboles de falla. Es importante resaltar que sólo se disponía de un demo del software antes mencionado, el cual está limitado al número de compuertas y eventos bases permitidos en cada árbol de falla. Por esta razón algunos lazos críticos tienen asociados más de un árbol de falla, de los cuales sólo uno se define como principal.

4.6.5.1. Desarrollo de árboles de falla

A cada árbol de falla se le asignó una referencia para facilitar su identificación. En la tabla 4.6 se describen cada uno de los árboles de falla desarrollados. En el anexo 7 se presentan los árboles de falla desarrollados.

Tabla 4.6. Descripción de los árboles de falla desarrollados

Ref	Descripción de evento tope	Observaciones
1_01	Avería del pozo causada por falla del control interno de la bomba o falla en el lazo de control de flujo de diluente o sobrepresión dentro del pozo, con posible derrame y pérdida de producción	Lazo principal.
1_02	Sobrepresión del pozo	Lazo secundario. La válvula del sistema de control de flujo no se ha colocado en este lazo ya que ésta falla cerrada.
2_01	Sobrepresión del separador de producción 0002-V-1001A/B debido a la ocurrencia de sobrepresión de gas causada por la falla del lazo de control de presión o por bloqueo a la descarga (sobrepresión en el depurador de gas), con posible fuga de gas asociado y avería del proceso.	Lazo principal.
2_02	Sobrenivel de líquido en el separador de producción 0002-V-1001A/B causado por la falla del lazo de control de nivel o por falla del sistema de bombeo, con posible fuga de BHD a presión y avería del proceso.	Lazo principal.
2_03	Falla sistema de bombeo de transferencia de BHD debido a la falla de las dos bombas principales en operación y de la bomba de respaldo al arrancar, con posible avería del proceso.	Lazo secundario. En este lazo se considera la probabilidad de falla de causa común de las bombas.

Tabla 4.6 (continuación). Descripción de los árboles de falla desarrollados

Ref	Descripción de evento tope	Observaciones
2_04	Falla bomba principal de transferencia de BHD 0002-P-1001A/B/C debido a falla interna o falta de flujo aguas arriba o sobrepresión a la descarga causado por falla del lazo de control de presión y bloqueo aguas abajo, con posible avería del proceso.	Lazo principal. A pesar de que las bombas 0002-P-1001A/B/C son de tornillo accionadas por motor eléctrico, en este lazo no se considera la falla eléctrica como evento base ya que de acuerdo a las bases de diseño del proceso una falla eléctrica levaría toda la planta a un estado de falla segura aunque con pérdida de producción.
2_05	Fallan lazos de control de nivel de los separadores, con posible avería del proceso	Lazo secundario. En este lazo se considera la probabilidad de falla de causa común de los lazos de control de nivel de los separadores.
2_06	Sobrepresión en el Tanque de BHD 0002-TK-1001 debido a la falla de control de presión de gas o falla en el mechurrio, con posible fuga de gas asociado y avería del proceso.	Lazo principal
2_07	Sobrellenado de líquido en el tanque de BHD 0002-TK-1001 debido a la falla de al menos uno de los lazos de control de nivel de los separadores o falla del sistema de bombeo, con posible derrame de BHD, pérdida de producción y avería del proceso.	La principal. Las válvulas de los sistemas de control de nivel no se han colocado en este lazo ya que éstas fallan abiertas.
2_08	Sobrepresión en el depurador de gas 0002-V-1301 debido a la ocurrencia de sobrepresión de gas causada por la falla del lazo de control de presión y por bloqueo a la descarga (entrada al compresor, hacia el cabezal del mechurrio y hacia el paquete HEI/FFG), con posible fuga de gas asociado y avería del proceso.	Lazo principal. En este lazo se consideran todas las vías de escape del gas.
2_09	Sobrenivel de condensado en el depurador de gas 0002-V-1301 causada por la falla de la válvula de apertura de salida o por falla del sistema de bombeo, con posible fuga de BHD a presión y avería del proceso.	Lazo principal.
2_10	Sobrellenado de líquido en el tanque amortiguador de diluente 0002-TK-1201 debido a la falla del lazo de control de nivel y falla del sistema de bombeo de inyección de diluente o falla del lazo de control de recirculación, con posible derrame de diluente y avería del proceso.	Lazo principal.
2_11	Falla sistema de bombeo de inyección de diluente debido a la falla de las dos bombas principales en operación y de la bomba de respaldo al arrancar, con posible avería del proceso.	Lazo secundario. En este lazo se considera la probabilidad de falla de causa común de las bombas.
2_12	Falla bomba principal de inyección de diluente 0002-P-1201A/B/C debido a falla interna o falta de flujo aguas arriba o sobrepresión a la descarga causado por falla del lazo de control de presión, con posible avería del proceso.	La principal. A pesar de que las bombas 0002-P-1201A/B/C son centrífugas accionadas por motor eléctrico, en este lazo no se considera la falla eléctrica como evento base ya que de acuerdo a las bases de diseño del proceso una falla eléctrica levaría toda la planta a un estado de falla segura aunque con pérdida de producción.

Tabla 4.6 (continuación). Descripción de los árboles de falla desarrollados

Ref	Descripción de evento tope	Observaciones
2_13	Falta de flujo aguas arriba de la bomba de inyección de diluente 0002-P-1201A/B/C debido a la falla del lazo de control de nivel y falla del lazo de control de flujo de recirculación, con posible avería del proceso.	Lazo secundario. La válvula del sistema de control de nivel y del sistema de control de flujo no se han colocado en este lazo ya que éstas fallan abiertas.
2_14	Sobrepresión en el tambor K.O. del mechurrio 0002-V-1801 debido a la ocurrencia de sobrepresión de gas causado por falla de la válvula de control de presión o por falla interna en el mechurrio, con posible fuga de gas asociado y avería del proceso.	Lazo principal.
2_15	Sobrenivel de líquido en el tambor K.O. del mechurrio 0002-V-1801 causado por falla del sistema de bombeo del tambor o por falla del transmisor de nivel, con posible fuga de BHD a presión y avería del proceso.	Lazo principal.
2_16	Falla bomba principal del tambor K.O. 0002-P-1801A/B debido a falla interna o falla del transmisor de nivel (provocando un arranque en falso), con posible avería del proceso.	Lazo principal.
2_17	Falta de agua en el tanque 0002-TK-1901 debido a la falla de la bomba de agua cruda con posibilidad de incendio y peligro en la Planta.	Lazo principal.
3_01	Sobrellenado de líquido en tanque de almacenamiento de diluente 0004-TK-1201/2 debido a la falla del sistema de llenado (válvula de entrada al tanque) y falla del sistema de vaciado (falla de válvula de salida o falla del sistema de bombeo de diluente), con posible derrame de diluente y avería del proceso.	Lazo principal.
3_02	Falla sistema de bombeo de diluente debido a la falla de las dos bombas principales en operación y de la bomba de respaldo al arrancar, con posible avería del proceso.	Lazo secundario. En este lazo se considera la probabilidad de falla de causa común de las bombas.
3_03	Falla bomba principal de diluente 0004-P-1201A/B/C debido a falla interna o falta de flujo aguas arriba o sobrepresión a la descarga causado por falla del lazo de control de presión, con posible avería del proceso.	Lazo principal. A pesar de que las bombas 0004-P-1201A/B/C son centrífugas accionadas por motor eléctrico, en este lazo no se considera la falla eléctrica como evento base ya que de acuerdo a las bases de diseño del proceso una falla eléctrica levaría toda la planta a un estado de falla segura aunque con pérdida de producción.
3_04	Falta de flujo aguas arriba de la bomba de inyección de diluente 0004-P-1201A/B/C debido a la falla del lazo de control de nivel y falla del lazo de control de flujo de recirculación, con posible avería del proceso.	Lazo secundario. La válvula del sistema de control de flujo no se ha colocado en este lazo ya que ésta falla abierta.
3_05	Falta de agua en el tanque 0004-TK-1901 debido a la falla de la bomba de agua cruda con posibilidad de incendio y peligro en la Planta.	Lazo principal.

4.6.5.2. Cuantificación de los árboles de falla

Los datos empleados para la determinación de la frecuencia de ocurrencia de los eventos tope de los árboles de falla se obtuvieron del anexo A de la norma PDVSA IR-S-02 y de algunos extractos de la base de datos OREDA 1997 [10]. En la tabla 4.6 se presentan los datos estadísticos e históricos empleados en el presente estudio.

Tabla 4.7. Datos Estadísticos utilizados

Elemento o Dispositivo	Tasa de Fallas (1/horas)	Modo de Falla	Fuente	Observación
Bomba	1,04E-04	durante funcionamiento	IR-S-02	accionado motor, función continua
Bomba	1,86E-05	arrancando en demanda	IR-S-02	accionado motor, alternando
Controlador	6,88E-05	pérdida de función	OREDA 97	---
Transmisor de flujo	2,76E-06	falla crítica	OREDA 97	eléctrico
Transmisor de nivel	6,09E-06	falla crítica	OREDA 97	eléctrico
Transmisor de presión	1,27E-06	falla crítica	OREDA 97	eléctrico
Transmisor de temperatura	7,73E-06	falla crítica	OREDA 97	eléctrico
Válvula autorreguladora	2,47E-05	peligroso	OREDA 97	---
Válvula ESD	1,11E-05	peligroso	OREDA 97	---
Válvula multipuerto	2,47E-05	peligroso	OREDA 97	---
Válvula neumática	2,20E-06	no cambia de posición en demanda	IR-S-02	---

4.6.6. Determinación de las consecuencias de los eventos iniciadores

Para determinar las consecuencias de los eventos iniciadores se empleó el método de Análisis de Árboles de Evento. Por otra parte se utilizó el programa de simulación FRED v4.0.0 de Shell Global Solutions. Con este software se determinó la cantidad de fluido en *kg/s* que escaparía de los diferentes recipientes del proceso (tanques de almacenamiento, depuradores de gas, separadores de producción) bajo condiciones peligrosas de sobrepresión. Este valor se utiliza para determinar la

probabilidad de ignición inmediata dada la fuga de un fluido según la tabla A.25 del anexo A de la norma PDVSA IR-S-02. El cálculo fue realizado para los lazos que se indican en la tabla 4.8, debido a que estos son los lazos que presentan como evento tope la sobrepresión debido a exceso de gas o líquido.

Tabla 4.8. Lazos críticos de sobrepresión y alto nivel de líquido

Lazo	Evento Tope
02	Sobrepresión en el separador de producción
03	Alto nivel de líquido en el separador de producción
05	Sobrepresión en el Tanque de BHD
07	Sobrepresión en el depurador de gas
08	Alto nivel de líquido en el depurador de gas
11	Sobrepresión en el tambor K.O. del mechurrio
12	Alto nivel de líquido en el tambor K.O. del mechurrio

Los datos de entrada para la realización de las simulaciones se obtuvieron de las tablas que se muestran en las secciones 3.3, 3.4 y 3.5 del capítulo III: "Descripción de la Planta y del Proceso bajo estudio" del presente documento. Los resultados obtenidos se pueden encontrar en el anexo 9 y en la tabla 4.9 se coloca el resumen de los mismos.

Tabla 4.9. Resultados obtenidos de la utilización del programa FRED

Lazo	Tipo de Fuga	Diámetro del orificio de escape (m)	Fuga (kg/s)	Probabilidad de Ignición
02	gas	0.06706	3,478	0,07
03	líquido	0.08941	104,200	0,08
05	gas	0.06706	0,219	0,01
07	gas	0.08941	4,934	0,07
08	líquido	0.02235	5,698	0,03
11	gas	0.06706	2,250	0,07
12	líquido	0.02235	4,998	0,03

4.6.6.1. Análisis de Árboles de Evento

Para cada uno de los eventos iniciadores se desarrolló un árbol de evento con la finalidad determinar la probabilidad de ocurrencia de las consecuencias o escenarios peligrosos que se pudieran presentar.

La asignación de las probabilidades de ocurrencia de las distintas ramas en los árboles de evento le agrega la característica cualitativa al análisis Semi-cuantitativo, debido a que depende principalmente de la experticia y conocimientos del proceso que tenga el equipo de trabajo que está realizando el análisis.

Los valores que se tomaron para la asignación de las probabilidades son las siguientes:

- Ignición inmediata: se toman de la tabla 4.9.
- Formación de nube de vapor: 0.5 para el caso de fuga de gas asociado y 0.2 para el caso de fuga de líquido a presión (debido a las características del Bitumen húmedo diluido).
- Nube de vapor confinada: 0.2 (debido a que la planta se encuentra al aire libre y no presenta ningún tipo de confinamiento).
- Presencia de fuentes de ignición: 0.1 (de acuerdo la tabla A.23 de la norma IR-S-02).
- Ignición retardada: 0.4 (de acuerdo al punto A.4.5 de la norma IR-S-02).

Para cada árbol de evento se tomó como frecuencia principal para la determinación del Nivel de Integridad de Seguridad la mayor frecuencia de las consecuencias o escenarios peligrosos determinados. Los árboles de evento se desarrollaron en Microsoft Excel y se presentan en el anexo 8.

4.6.7. Resultados obtenidos

En la tabla 4.10 se muestran los resultados obtenidos del cálculo cuantitativo del Nivel de Integridad de Seguridad. La descripción de los campos en dicha tabla es la siguiente:

- **Lazo**: identificador del lazo crítico.

- **Frecuencia evento tope (1/año) (*F*)**: calculada por árbol de fallas.

- **Probabilidad de ocurrencia del escenario peligroso (*P*)**: es la probabilidad de ocurrencia de la consecuencia o escenario peligroso dada la ocurrencia del evento tope. Es determinada empleando árbol de eventos.

- **Nivel de riesgo del sistema (*Rs*)**: se obtiene de multiplicar la frecuencia del evento iniciador por la probabilidad de ocurrencia de la consecuencia.

- **Aporte de IPL's (*A*$_{IPL}$)**: aporte de las capas independientes de protección de acuerdo a la tabla 4.8.

- **Nivel de riesgo final del sistema (*Rf*)**: se obtiene de multiplicar el Nivel de riesgo del sistema por el aporte de las capas independientes de protección.

- **Nivel de riesgo aceptable (1/año) (*Ra*)**: se determina de acuerdo a la tabla 4.4.

- **Probabilidad de falla en demanda promedio (*PFD*$_{AVG}$)**: se obtiene de dividir el Nivel de riesgo aceptable entre el Nivel de riesgo total del sistema.

- **Nivel de Integridad de seguridad (SIL)**: se obtiene a partir de la Probabilidad de falla en demanda promedio (*PFD*$_{AVG}$) obtenida de acuerdo a la tabla 2.9 del capítulo II del presente documento.

Tabla 4.10. Determinación Cuantitativa del SIL

Lazo	Frecuencia evento tope (1/año) (*F*)	Probabilidad de ocurrencia del escenario peligroso (*P*)	Nivel de riesgo del sistema (*Rs*)	Aporte de IPL's (*AIPL*)	Nivel de riesgo final del sistema (*Rf*)	Nivel de riesgo aceptable (1/año) (*Ra*)	*PFDAVG*	Nivel de Integridad de seguridad (SIL)
01	1,272965676	0,9	1,145669108	1,00E-02	1,15E-02	1,00E-04	8,73E-03	SIL 2
02	0,634878272	0,465	0,295218397	1,00E-02	2,95E-03	1,00E-05	3,39E-03	SIL 2
03	0,800732391	0,4416	0,353603424	1,00E-02	3,54E-03	1,00E-05	2,83E-03	SIL 2
04	0,980829253	0,9	0,882746328	1,00E-01	8,83E-02	1,00E-03	1,13E-02	SIL 1
05	1,217395825	0,495	0,602610933	1,00E-01	6,03E-02	1,00E-04	1,66E-03	SIL 2
06	0,085557888	0,9	0,0770021	1,00E-01	7,70E-03	1,00E-04	1,30E-02	SIL 1
07	0,001651363	0,465	0,000767884	1,00E-02	7,68E-06	1,00E-04	1,30E+01	no necesario
08	0,223143551	0,4656	0,103895637	1,00E-02	1,04E-03	1,00E-05	9,63E-03	SIL 2
09	0,358104537	0,9	0,322294083	1,00E-01	3,22E-02	1,00E-04	3,10E-03	SIL 2
10	1,795767491	0,9	1,616190742	1	1,62E+00	1,00E-03	6,19E-04	SIL 3
11	0,818710404	0,465	0,380700338	1	3,81E-01	1,00E-04	2,63E-04	SIL 3
12	0,215671536	0,4656	0,100416667	1	1,00E-01	1,00E-04	9,96E-04	SIL 3
13	0,964955904	0,9	0,868460313	1	8,68E-01	1,00E-03	1,15E-03	SIL 2
14	0,162518929	0,03	0,004875568	1	4,88E-03	1,00E-03	2,05E-01	no necesario
15	0,023166278	0,9	0,02084965	1,00E-01	2,08E-03	1,00E-05	4,80E-03	SIL 2
16	1,62964062	0,9	1,466676558	1	1,47E+00	1,00E-03	6,82E-04	SIL 3
17	0,162518929	0,03	0,004875568	1	4,88E-03	1,00E-03	2,05E-01	no necesario

4.7. Análisis de Resultados

En la tabla 4.11 se muestra el SIL resultante para cada lazo crítico por los dos métodos empleados.

Tabla 4.11. Resultados Obtenidos del SIL

	SIL	
Lazo	**Cualitativo**	**Cuantitativo**
01	1	SIL 2
02	1	SIL 2
03	a	SIL 2
04	2	SIL 1
05	a	SIL 2
06	a	SIL 1
07	2	no necesario
08	a	SIL 2
09	1	SIL 2
10	1	SIL 3
11	1	SIL 3
12	a	SIL 3
13	2	SIL 2
14	a	no necesario
15	1	SIL 2
16	1	SIL 3
17	a	no necesario

Como se pude apreciar en la tabla 4.11, el SIL obtenido por los dos métodos empleados coincide solamente para los lazos 13, 14 y 17, mientras que para los otros lazos difieren sin ningún patrón constante.

Esto es debido a que el método de Gráfica de Riesgo, como todo método cualitativo, depende de la experiencia y conocimientos previos sobre el proceso bajo estudio que posea la persona encargada del análisis; es decir, sus resultados son subjetivos y no reproducibles (diferentes personas u organizaciones pueden revisar el mismo proceso y proporcionar requerimientos de SIL muy diferentes entre sí). Basado en lo expuesto anteriormente se pude decir que, para los efectos del presente trabajo de grado, los resultados obtenidos por el método cualitativo empleado en la determinación del SIL carecen de validez.

Por lo tanto, para el desarrollo de las especificaciones y diseño del SIS se toman como válidos los resultados del SIL que se obtuvieron por el método cuantitativo empleado.

CAPÍTULO V

DISEÑO DEL SISTEMA INSTRUMENTADO DE SEGURIDAD (SIS)

El diseño de un sistema instrumentado de seguridad consta de varia fases de acuerdo a lo establecido en la norma ANSI/ISA-84.00.01-2004. Las fases consideradas en el presente capítulo son las siguientes:

- Desarrollo de las especificaciones de los requerimientos de seguridad.
- Diseño conceptual del SIS.
- Diseño detallado del SIS.

5.1. Desarrollo de las especificaciones de requerimientos de seguridad

A continuación se describen los aspectos considerados de acuerdo a la norma ANSI/ISA-84.00.01-2004.

5.1.1. Requerimientos de entrada

Como requerimientos de entrada se tienen los siguientes:

a) Lista de las Funciones Instrumentadas de Seguridad (SIF) y su respectivo Nivel de Integridad de Seguridad (SIL)

En la tabla 5.1 se muestran las Funciones Instrumentadas de Seguridad (SIF) que se dedujeron a partir del los resultados cuantitativos obtenidos en el capítulo IV "Determinación del Nivel de Integridad de Seguridad" del presente documento. Cabe destacar que en referencia a algunos lazos críticos se plantea más de una SIF, lo cual obedece a lo establecido en el punto 4.3 del capítulo IV.

Tabla 5.1. Funciones Instrumentadas de Seguridad

Lazo	SIF	SIL	Función Instrumentada de Seguridad	Descripción de disparo
01	S-01	SIL 2	Alto flujo de diluente o Alta presión en el pozo	Si la presión en el pozo alcanza 145 psig
02	S-02	SIL 2	Alta - Alta presión en separador de producción 0002-V-1001A	Si la presión en el separador alcanza 83 psig
	S-03	SIL 2	Alta - Alta presión en separador de producción 0002-V-1001B	Si la presión en el separador alcanza 83 psig
03	S-04	SIL 2	Alto - Alto nivel de líquido en separador de producción 0002-V-1001A	Si el nivel de líquido en el separador alcanza 6'-0"
	S-05	SIL 2	Alto - Alto nivel de líquido en separador de producción 0002-V-1001B	Si el nivel de líquido en el separador alcanza 6'-0"
04	S-06	SIL 1	Alta - Alta presión aguas abajo o Baja presión aguas arriba de la bomba 0002-P-1001A	Si la presión a la succión disminuye de -2 psig o la presión a la descarga alcanza 305 psig
	S-07	SIL 1	Alta - Alta presión aguas abajo o Baja presión aguas arriba de la bomba 0002-P-1001B	Si la presión a la succión disminuye de -2 psig o la presión a la descarga alcanza 305 psig
	S-08	SIL 1	Alta - Alta presión aguas abajo o Baja presión aguas arriba de la bomba 0002-P-1001C	Si la presión a la succión disminuye de -2 psig o la presión a la descarga alcanza 305 psig
05	S-09	SIL 2	Alta - Alta presión en tanque de BHD 0002-TK-1001	Si la presión en el tanque alcanza 7" H2O
06	S-10	SIL 1	Alto - Alto nivel de líquido en tanque de BHD 0002-TK-1001	Si el nivel de líquido en el tanque alcanza 35'-0"
07	---	no necesario	---	---
08	S-11	SIL 2	Alto - Alto nivel de líquido en el depurador de gas 0002-V-1301	Si el nivel de líquido en el depurador alcanza 4'-4"
09	S-12	SIL 2	Alto - Alto nivel de líquido en tanque amortiguador de diluente 0002-TK-1201	Si el nivel de líquido en el tanque alcanza 29'-0"

Tabla 5.1 (continuación). Funciones Instrumentadas de Seguridad

Lazo	SIF	SIL	Función Instrumentada de Seguridad	Descripción
10	S-13	SIL 3	Alta - Alta presión aguas abajo o Baja presión aguas arriba de la bomba 0002-P-1201A	Si la presión a la succión disminuye de -1 psig o la presión a la descarga excede 525 psig
	S-14	SIL 3	Alta - Alta presión aguas abajo o Baja presión aguas arriba de la bomba 0002-P-1201B	Si la presión a la succión disminuye de -1 psig o la presión a la descarga excede 525 psig
	S-15	SIL 3	Alta - Alta presión aguas abajo o Baja presión aguas arriba de la bomba 0002-P-1201C	Si la presión a la succión disminuye de -1 psig o la presión a la descarga excede 525 psig
11	S-16	SIL 3	Alta - Alta presión en tambor K.O. del mechurrio 0002-V-1801	Si la presión en el tambor K.O alcanza 48 psig
12	S-17	SIL 3	Alto - Alto nivel de líquido en tambor K.O. del mechurrio 0002-V-1801	Si el nivel de líquido en el tambor K.O alcanza 3'-5"
13	S-18	SIL 2	Alta - Alta presión aguas abajo o Baja presión aguas arriba de la bomba 0002-P-1801A	Si la presión a la succión disminuye de -2,8 psig o la presión a la descarga alcanza 20 psig
	S-19	SIL 2	Alta - Alta presión aguas abajo o Baja presión aguas arriba de la bomba 0002-P-1801B	Si la presión a la succión disminuye de -2,8 psig o la presión a la descarga alcanza 20 psig
14	---	no necesario	---	---
15	S-20	SIL 2	Alto - Alto nivel de líquido en tanque de almacenamiento de diluente 0004-TK-1201	Si el nivel de líquido alcanza 45'-0"
	S-21	SIL 2	Alto - Alto nivel de líquido en tanque de almacenamiento de diluente 0004-TK-1202	Si el nivel de líquido alcanza 45'-0"
16	S-22	SIL 3	Alta - Alta presión aguas abajo o Baja presión aguas arriba de la bomba 0004-P-1201A	Si la presión a la succión disminuye de -1 psig o la presión a la descarga alcanza 175 psig
	S-23	SIL 3	Alta - Alta presión aguas abajo o Baja presión aguas arriba de la bomba 0004-P-1201B	Si la presión a la succión disminuye de -1 psig o la presión a la descarga alcanza 175 psig
	S-24	SIL 3	Alta - Alta presión aguas abajo o Baja presión aguas arriba de la bomba 0004-P-1201C	Si la presión a la succión disminuye de -1 psig o la presión a la descarga alcanza 175 psig
17	---	no necesario	---	---

b) Consideraciones de fallas de Causa Común del Proceso

Entre los factores de causa común se pueden citar la temperatura, la vibración, la calidad del aire de instrumentos, la corrosión, etc. De acuerdo al punto 4.6.1 del capítulo IV y para efectos de la determinación de la arquitectura más óptima para cada SIF, se tomó el porcentaje de causa común para elementos redundantes igual al 10%.

5.1.2. Requerimientos Funcionales de Seguridad

Los requerimientos funcionales de seguridad son los siguientes:

a) Estado seguro del proceso

El SIS logra colocar el proceso en un estado seguro bloqueando las entradas y salidas de energía y/o masa de las diferentes unidades y/o equipos del proceso.

b) Entradas del proceso al SIS y sus puntos de disparo

En la tabla 5.2 se presentan las entradas del proceso al SIS y sus respectivos puntos de disparo.

Tabla 5.2. Entradas del proceso al SIS y sus puntos de disparo

SIF	SIL	Función Instrumentada de Seguridad	Entrada del proceso al SIS	Punto de disparo
S-01	SIL 2	Alto flujo de diluente o Alta presión en el pozo	presión en el pozo	145 psig (inc)
S-02	SIL 2	Alta - Alta presión en separador de producción 0002-V-1001A	presión en 0002-V-1001A	83 psig (inc)
S-03	SIL 2	Alta - Alta presión en separador de producción 0002-V-1001B	presión en 0002-V-1001B	83 psig (inc)
S-04	SIL 2	Alto - Alto nivel de líquido en separador de producción 0002-V-1001A	nivel de líquido en 0002-V-1001A	6'-0" (inc)
S-05	SIL 2	Alto - Alto nivel de líquido en separador de producción 0002-V-1001B	nivel de líquido en 0002-V-1001B	6'-0" (inc)

Tabla 5.2 (continuación). Entradas del proceso al SIS y sus puntos de disparo

SIF	SIL	Función Instrumentada de Seguridad	Entrada del proceso al SIS	Punto de disparo
S-06	SIL 1	Alta - Alta presión aguas abajo o Baja presión aguas arriba de la bomba 0002-P-1001A	presión aguas abajo y presión aguas arriba de 0002-P-1001A	-2 psig (dec) y 305 psig (inc) respectivamente
S-07	SIL 1	Alta - Alta presión aguas abajo o Baja presión aguas arriba de la bomba 0002-P-1001B	presión aguas abajo y presión aguas arriba de 0002-P-1001B	-2 psig (dec) y 305 psig (inc) respectivamente
S-08	SIL 1	Alta - Alta presión aguas abajo o Baja presión aguas arriba de la bomba 0002-P-1001C	presión aguas abajo y presión aguas arriba de 0002-P-1001C	-2 psig (dec) y 305 psig (inc) respectivamente
S-09	SIL 2	Alta - Alta presión en tanque de BHD 0002-TK-1001	presión en 0002-TK-1001	7" H2O (inc)
S-10	SIL 1	Alto - Alto nivel de líquido en tanque de BHD 0002-TK-1001	nivel de líquido en 0002-TK-1001	35'-0" (inc)
S-11	SIL 2	Alto - Alto nivel de líquido en el depurador de gas 0002-V-1301	nivel de líquido en 0002-V-1301	4'-4" (inc)
S-12	SIL 2	Alto - Alto nivel de líquido en tanque amortiguador de diluente 0002-TK-1201	nivel de líquido en 0002-TK-1201	29'-0" (inc)
S-13	SIL 3	Alta - Alta presión aguas abajo o Baja presión aguas arriba de la bomba 0002-P-1201A	presión aguas abajo y presión aguas arriba de 0002-P-1201A	-1 psig (dec) y 525 psig (inc) respectivamente
S-14	SIL 3	Alta - Alta presión aguas abajo o Baja presión aguas arriba de la bomba 0002-P-1201B	presión aguas abajo y presión aguas arriba de 0002-P-1201B	-1 psig (dec) y 525 psig (inc) respectivamente
S-15	SIL 3	Alta - Alta presión aguas abajo o Baja presión aguas arriba de la bomba 0002-P-1201C	presión aguas abajo y presión aguas arriba de 0002-P-1201C	-1 psig (dec) y 525 psig (inc) respectivamente
S-16	SIL 3	Alta - Alta presión en tambor K.O. del mechurrio 0002-V-1801	presión en 0002-V-1801	48 psig (inc)
S-17	SIL 3	Alto - Alto nivel de líquido en tambor K.O. del mechurrio 0002-V-1801	nivel de líquido en 0002-V-1801	3'-5" (inc)
S-18	SIL 2	Alta - Alta presión aguas abajo o Baja presión aguas arriba de la bomba 0002-P-1801A	presión aguas abajo y presión aguas arriba de 0002-P-1801A	-2,8 psig (dec) y 20 psig (inc) respectivamente

Tabla 5.2 (continuación). Entradas del proceso al SIS y sus puntos de disparo

SIF	SIL	Función Instrumentada de Seguridad	Entrada del proceso al SIS	Punto de disparo
S-19	SIL 2	Alta - Alta presión aguas abajo o Baja presión aguas arriba de la bomba 0002-P-1801B	presión aguas abajo y presión aguas arriba de 0002-P-1801B	-2,8 psig (dec) y 20 psig (inc) respectivamente
S-20	SIL 2	Alto - Alto nivel de líquido en tanque de almacenamiento de diluente 0004-TK-1201	nivel de líquido en 0004-TK-1201	45'-0" (inc)
S-21	SIL 2	Alto - Alto nivel de líquido en tanque de almacenamiento de diluente 0004-TK-1202	nivel de líquido en 0004-TK-1202	45'-0" (inc)
S-22	SIL 3	Alta - Alta presión aguas abajo o Baja presión aguas arriba de la bomba 0004-P-1201A	presión aguas abajo y presión aguas arriba de 0004-P-1201A	-1 psig (dec) y 175 psig (inc) respectivamente
S-23	SIL 3	Alta - Alta presión aguas abajo o Baja presión aguas arriba de la bomba 0004-P-1201B	presión aguas abajo y presión aguas arriba de 0004-P-1201B	-1 psig (dec) y 175 psig (inc) respectivamente
S-24	SIL 3	Alta - Alta presión aguas abajo o Baja presión aguas arriba de la bomba 0004-P-1201C	presión aguas abajo y presión aguas arriba de 0004-P-1201C	-1 psig (dec) y 175 psig (inc) respectivamente

En la tabla anterior la abreviatura (inc) y (dec) significan incrementando y decrementando respectivamente.

c) Rango de operación normal

Esta información se presenta en el capítulo III “Descripción de la planta y proceso bajo estudio” del presente documento.

d) Salidas del SIS al proceso y sus acciones

El SIS actúa sobre contactores y válvulas solenoides que operan sobre válvulas de bloqueo (shutdown). Las salidas del SIS y su acción se presentan en la tabla 5.3.

Tabla 5.3. Salidas del SIS al proceso

SIF	SIL	Función Instrumentada de Seguridad	Acción de las salidas del SIS al proceso
S-01	SIL 2	Alto flujo de diluente o Alta presión en el pozo	detener entrada de diluente al pozo y apagar la bomba
S-02	SIL 2	Alta - Alta presión en separador de producción 0002-V-1001A	detener el flujo de entrada de BHD al 0002-V-1001A
S-03	SIL 2	Alta - Alta presión en separador de producción 0002-V-1001B	detener el flujo de entrada de BHD al 0002-V-1001B
S-04	SIL 2	Alto - Alto nivel de líquido en separador de producción 0002-V-1001A	detener el flujo de entrada de BHD al 0002-V-1001A
S-05	SIL 2	Alto - Alto nivel de líquido en separador de producción 0002-V-1001B	detener el flujo de entrada de BHD al 0002-V-1001B
S-06	SIL 1	Alta - Alta presión aguas abajo o Baja presión aguas arriba de la bomba 0002-P-1001A	detener el flujo de BHD hacia sistema de bombeo y apagar 0002-P-1001A
S-07	SIL 1	Alta - Alta presión aguas abajo o Baja presión aguas arriba de la bomba 0002-P-1001B	detener el flujo de BHD hacia sistema de bombeo y apagar 0002-P-1001B
S-08	SIL 1	Alta - Alta presión aguas abajo o Baja presión aguas arriba de la bomba 0002-P-1001C	detener el flujo de BHD hacia sistema de bombeo y apagar 0002-P-1001C
S-09	SIL 2	Alta - Alta presión en tanque de BHD 0002-TK-1001	detener el flujo de entrada de BHD hacia 0002-TK-1001
S-10	SIL 1	Alto - Alto nivel de líquido en tanque de BHD 0002-TK-1001	detener el flujo de entrada de BHD hacia 0002-TK-1001
S-11	SIL 2	Alto - Alto nivel de líquido en el depurador de gas 0002-V-1301	detener el flujo de entrada/salida de gas asociado hacia/desde 0002-V-1301
S-12	SIL 2	Alto - Alto nivel de líquido en tanque amortiguador de diluente 0002-TK-1201	detener el flujo de entrada de diluente hacia 0002-TK-1201
S-13	SIL 3	Alta - Alta presión aguas abajo o Baja presión aguas arriba de la bomba 0002-P-1201A	detener el flujo de diluente hacia sistema de bombeo y apagar 0002-P-1201A
S-14	SIL 3	Alta - Alta presión aguas abajo o Baja presión aguas arriba de la bomba 0002-P-1201B	detener el flujo de diluente hacia sistema de bombeo y apagar 0002-P-1201B
S-15	SIL 3	Alta - Alta presión aguas abajo o Baja presión aguas arriba de la bomba 0002-P-1201C	detener el flujo de diluente hacia sistema de bombeo y apagar 0002-P-1201C

Tabla 5.3 (continuación). Salidas del SIS al proceso

SIF	SIL	Función Instrumentada de Seguridad	Acción de las salidas del SIS al proceso
S-16	SIL 3	Alta - Alta presión en tambor K.O. del mechurrio 0002-V-1801	detener el flujo de entrada de gas hacia el 0002-V-1801
S-17	SIL 3	Alto - Alto nivel de líquido en tambor K.O. del mechurrio 0002-V-1801	detener el flujo de entrada de condensado hacia el 0002-V-1801
S-18	SIL 2	Alta - Alta presión aguas abajo o Baja presión aguas arriba de la bomba 0002-P-1801A	detener el flujo de condensado hacia sistema de bombeo y apagar 0002-P-1801A
S-19	SIL 2	Alta - Alta presión aguas abajo o Baja presión aguas arriba de la bomba 0002-P-1801B	detener el flujo de condensado hacia sistema de bombeo y apagar 0002-P-1801B
S-20	SIL 2	Alto - Alto nivel de líquido en tanque de almacenamiento de diluente 0004-TK-1201	detener el flujo de entrada de diluente hacia 0004-TK-1201
S-21	SIL 2	Alto - Alto nivel de líquido en tanque de almacenamiento de diluente 0004-TK-1202	detener el flujo de entrada de diluente hacia 0004-TK-1202
S-22	SIL 3	Alta - Alta presión aguas abajo o Baja presión aguas arriba de la bomba 0004-P-1201A	detener el flujo de diluente hacia sistema de bombeo y apagar 0004-P-1201C
S-23	SIL 3	Alta - Alta presión aguas abajo o Baja presión aguas arriba de la bomba 0004-P-1201B	detener el flujo de diluente hacia sistema de bombeo y apagar 0004-P-1201B
S-24	SIL 3	Alta - Alta presión aguas abajo o Baja presión aguas arriba de la bomba 0004-P-1201C	detener el flujo de diluente hacia sistema de bombeo y apagar 0004-P-1201C

e) Selección de Disparo Energizado / Desenergizado

El SIS debe ser des-energizado para generar una parada segura.

f) Condiciones para parada manual

Se deben colocar “push button” manuales y un panel de alarmas con la finalidad de que los operadores puedan llevar el proceso a su condición segura en el caso de que el SIS falle o el operador observe alguna otra condición inusual.

El o los pulsadores, se deben cablear directamente a una entrada discreta del "Logic Solver".

g) Acción a ser tomada bajo pérdida de la fuente de energía al SIS

La pérdida de electricidad o suministro de aire resulta en el cierre de todas válvulas asociadas al SIS, de acuerdo a lo definido en los estados seguros del proceso, y apagado de los motores de las bombas.

h) Requerimientos de Tiempo de Respuesta para que el SIS lleve el proceso a un Estado Seguro

No existe ningún requerimiento de velocidad de respuesta especial.

i) Acción de Respuesta a cualquier fallo detectado en el sistema.

Si el operador observa cualquier falla en el SIS, debe hacer una parada manual mediante el pulsador a ser incluido.

j) Requerimientos de Interfaz Humano – Máquina (HMI)

El BPCS servirá como HMI primaria para el SIS. Todas las funciones de visualización de alarmas serán implementadas en el BPCS.

k) Función de Interruptor de Reposición (RESET)

En el evento de que el SIS haga una parada, es necesario que el operador presione un interruptor de reposición (reset) antes de recomenzar el nuevo arranque.

5.1.3. Requerimientos de Integridad de Seguridad

Los requerimientos de integridad de seguridad se plantean a continuación:

a) SIL requerido para cada función de seguridad

Están definidos en la tabla 5.1.

b) Requerimientos de diagnóstico

- Sensores de posición en las válvulas de bloqueo.
- Transmisores con capacidad de diagnóstico.

c) Mantenimiento y Pruebas

Este SIS será inspeccionado y probado una vez por año. Adicionalmente si se detecta cualquier problema en el SIS, se ejecutará una acción inmediatamente y el trabajo será continuo hasta que la reparación se culmine exitosamente.

d) Paradas Indeseadas (Falsas)

Las paradas falsas no causarán problemas relacionados con seguridad.

5.2. Diseño conceptual del SIS

El SIS a implantar debe cumplir con las siguientes consideraciones de diseño:

5.2.1. Separación

El SIS debe ser separado e independiente del BPCS. La separación del sistema de control básico de proceso y las funciones del Sistema Instrumentado de Seguridad reducen la probabilidad de que el control y las funciones de seguridad no estén disponibles al mismo tiempo, ya que cambios inadvertidos afectarían la funcionalidad de seguridad del SIS.

5.2.2. Redundancia

Se requiere en algunos elementos del sistema de manera de lograr el SIL requerido. El esquema de redundancia y votación a seguir en los elementos sensores/transmisores, logic solvers y elementos finales de control, de modo de cumplir con el SIL requerido de cada lazo, se definen en la sección 5.3.

5.2.3. Consideraciones de diseño del software

El programa de aplicación de seguridad deberá ser diseñado empleando bloques de funciones o diagramas de escaleras.

5.2.4. Selección de tecnología

El SIS será implantado haciendo uso de un Logic Solver Electrónico Programable.

5.2.5. Requerimientos de arquitectura

Inicialmente no existe ningún requerimiento especial de arquitectura (la arquitectura de votación de los diferentes elementos que componen cada una de las SIF se define en la sección 5.3.

5.2.6. Fuentes de Poder

Las fuentes de poder eléctricas y neumáticas se deben proveer usando buenas prácticas de ingeniería. Estas deben incluir:

- Fuente de Poder dedicada, derivada separadamente de un sistema de alimentación ininterrumpida.
- Se debe utilizar fuentes redundantes (2 como mínimo) y las mismas se deben poder mantener individualmente, sin necesidad de poner fuera de servicio ni total ni parcialmente la alimentación del SIS.
- Se requiere revisar el sistema de suministro de aire a las válvulas y la alimentación eléctrica a los motores de las bombas.
- Aterramiento usando buenas prácticas de ingeniería.

5.2.7. Diagnóstico

Al emplear transmisores inteligentes y válvulas con diagnóstico, se dispone de una mejor capacidad de detección y predicción de fallas.

5.2.8. Dispositivos de campo

Se deben emplear sensores inteligentes para todas las mediciones del proceso.

5.2.9. Tasas de Falla y Modos de Falla

Estos datos han sido tomados de los reportes FMEDA aportados por los fabricantes

5.2.10. Interfaz con el usuario

La interfaz con el usuario debe constar de un panel de alarmas, interruptores de reset y de apagado (shut down).

5.2.11. Seguridad

Debido a las características de la instalación de la planta y del proceso ésta se considera segura. El Logic Solver del SIS está ubicado en la Sala de Control. Los sensores y elementos finales de campo del SIS tendrán indicativos de seguridad para advertir su status funcional de seguridad al personal de la planta. El enlace de comunicación entre el BPCS y el Logic Solver estará protegido contra escritura para prevenir cambios inadvertidos en el programa del SIS desde el BPCS.

5.2.12. Prácticas de cableado

El cableado debe ser hecho de acuerdo con el Código Eléctrico Nacional, las regulaciones locales y los lineamientos del fabricante de los componentes del SIS. Se deben instalar dos sistemas separados de cableado, uno para la potencia eléctrica (120/240V, etc.) y otro para la señal de instrumentos (4 – 20 mA, etc.). El cableado del SIS puede utilizar el misma caja terminal que el cableado del BPCS, pero empleando terminales separados y claramente identificados.

5.2.13. Intervalo de Pruebas Funcionales

El SIS debe ser probado integralmente una vez al año, ya que en la realización de los cálculos del SIL de cada SIF se tomó como intervalo de pruebas 1 año (8760 horas).

5.3. Diseño detallado del SIS

Para realizar el diseño detallado del SIS se elaboró una aplicación (“diseño”) desarrollado en Microsoft Access empleando como plataforma de programación Microsoft Visual Basic para Aplicaciones. Con esta aplicación se realiza el análisis de desempeño y diseño de cada SIFs que conforman el SIS. En la figura 5.1 se muestra la interfaz de entrada del programa desarrollado.

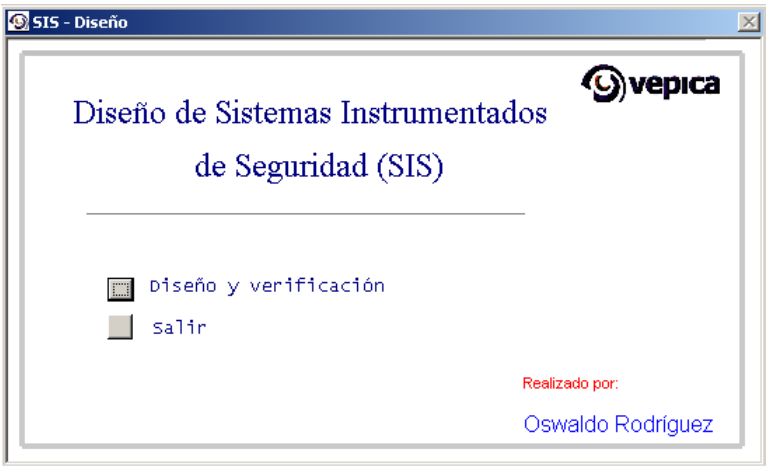

figura 5.1. Interfaz gráfica del programa “diseño”

5.3.1. Descripción de la aplicación “diseño”

La aplicación “diseño” consta de tres partes:

- Módulo genético.
- Módulo de verificación.
- Base de Datos.

En la figura 5.2 se muestra el diagrama de flujo general de “diseño”.

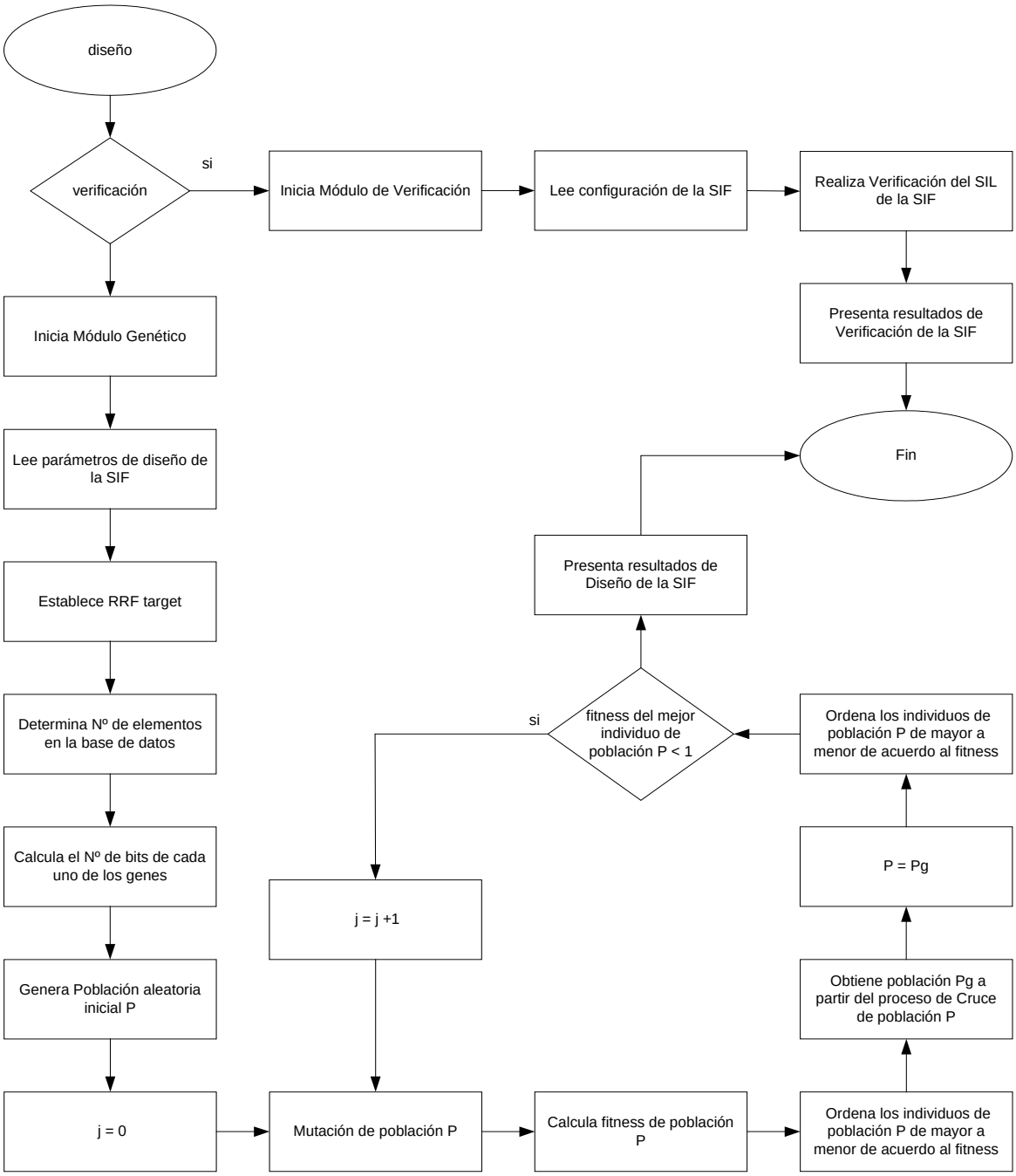

figura 5.2. Diagrama de flujo de “diseño”

5.3.1.1. Módulo genético

Se desarrolló un algoritmo genético con la finalidad de optimizar el proceso de diseño de cada SIF. Este algoritmo genético se encarga de determinar, para cada SIF, el (los) mejor(es) elemento(s) sensor/transmisor y su(s) arquitectura(s) de votación, el mejor logic solver y su arquitectura de votación y el (los) mejor(es) elemento(s) final(es) de control y su(s) arquitectura(s) de votación, en términos de menor probabilidad de falla en demanda promedio (PFD_{AVG}) y de menor complejidad de arquitectura de votación.

Como se observa en la ecuación 5.1, una menor probabilidad de falla en demanda promedio implica un mayor factor de reducción de riesgo (*RRF*), el cual garantiza mayor confiabilidad de la SIF y por lo tanto del SIS.

$$RRF = \frac{1}{PFD_{AVG}} \qquad \text{Ec. 5.1}$$

Una menor complejidad de la arquitectura de votación de los elementos que componen cada SIF garantiza un menor costo de instalación del SIS. Esto es debido a que, obviamente, es mucho más costoso instalar un sistema con votación 2oo3 que uno con votación 1oo1.

Para realizar el diseño de cada SIF empleando el módulo genético, se deben introducir los siguientes parámetros empleando la interfaz gráfica del módulo genético (figura 5.3):

- SIL requerido. Representa el SIL requerido por la SIF. Se escoge uno de los siguientes valores: 1, 2, 3.
- Tipo del 1^{er} elemento sensor/transmisor. Se coloca el tipo de sensor/transmisor de acuerdo a la variable a medir. Se escoge uno de los siguientes: Flujo, Nivel, Presión, Temperatura.
- Tipo del 2^{do} elemento sensor/transmisor (opcional). Este parámetro se coloca en caso de que la SIF necesite un segundo elemento sensor/transmisor distinto al escogido anteriormente (1^{er} elemento sensor/transmisor).

- Tipo del 1^{er} elemento final de control. Se coloca el tipo de elemento final de control de acuerdo a la acción a realizar. Se escoge uno de los siguientes: Contactor, Controlador/posicionador, Válvula, Válvula shutdown.
- Tipo del 2^{do} elemento final de control (opcional). Este parámetro se coloca en caso de que la SIF necesite un segundo elemento final de control distinto al escogido anteriormente (1^{er} elemento final de control).
- Cantidad del 1^{er} y 2^{do} elemento sensor/transmisor y del 1^{er} y 2^{do} elemento final de control. Se coloca la cantidad de elementos (sensor/transmisor, final de control) del tipo escogido que requiere la SIF. Este número puede variar de 1 a 9.

No se coloca ninguna información referente al logic solver a emplear, debido a que el algoritmo genético determina el más apropiado de entre todos los logic solvers existentes en la base de datos.

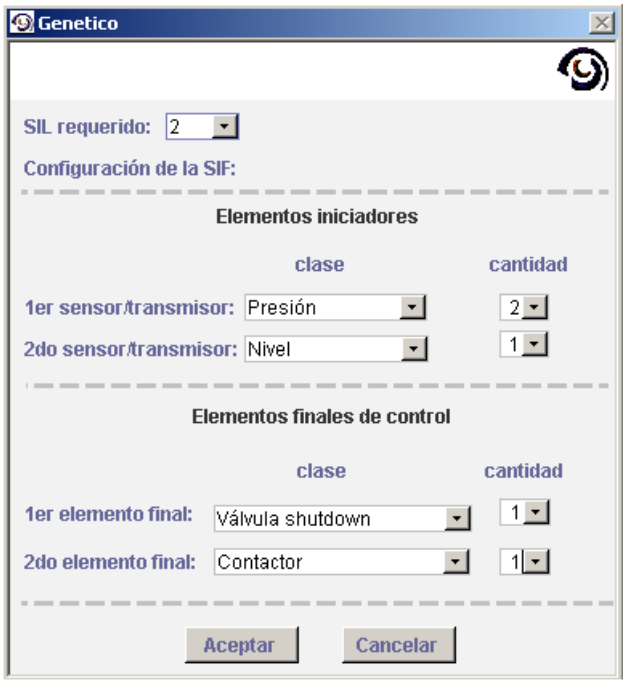

figura 5.3. Interfaz gráfica del módulo genético

El algoritmo genético trabaja con una población cuyos individuos presentan el cromosoma que se muestra en la figura 5.4.

gen 1	gen 2	gen 3	gen 4	gen 5	gen 6	gen 7	gen 8

figura 5.4. Cromosoma

La información genética es la siguiente:

gen 1: representa el 1^{er} elemento sensor/transmisor.

gen 2: representa el 2^{do} elemento sensor/transmisor.

gen 3: representa la arquitectura de votación de los elementos sensor/transmisor.

gen 4: representa el logic solver.

gen 5: representa la arquitectura de votación del logic solver.

gen 6: representa el 1^{er} elemento final de control.

gen 7: representa el 2^{do} elemento final de control.

gen 8: representa la arquitectura de votación de los elementos finales de control.

El número de bits de los genes 1, 2 , 4, 6 y 7 depende del número de elementos del tipo seleccionado que existan en la base datos de la aplicaciòn. Este valor viene dado la ecuación 5.2:

$$nº\ de\ bits = parte\ entera\left[\frac{\ln(nº\ de\ elementos\ en\ la\ base\ de\ datos)}{\ln(2)} + 1\right] \qquad \text{Ec.5.2}$$

El número de bits de los genes 3, 5 y 8 es tres (ecuación 5.3), debido a que se trabajan con 7 arquitecturas de votación.

$$nº\ de\ bits = parte\ entera\left[\frac{\ln(7)}{\ln(2)} + 1\right] = 3 \qquad \text{Ec. 5.3}$$

El algoritmo genético desarrollado emplea un fitness compuesto descrito por la ecuación 5.4:

$$fit = \alpha \cdot fit\_PFD + \varphi \cdot fit\_arq \qquad \text{Ec. 5.4}$$

con,

fit_PFD : fitness de menor probabilidad de falla en demanda promedio.

fit_arq : fitness de menor complejidad de arquitectura de votación.

α : presión evolutiva de menor probabilidad de falla en demanda promedio.

φ: presión evolutiva de menor complejidad de arquitectura de votación.

Las presiones evolutivas están relacionadas por la ecuación 5.5:

$$\alpha + \varphi = 1 \qquad \text{Ec. 5.5}$$

Según el nivel SIL requerido de cada SIF, se asigna un factor de reducción de riesgo target (*RRF_tg*) de acuerdo a la siguiente tabla:

Tabla 5.4. Factor de reducción de riesgo target

SIL requerido	***RRF_tg***
1	100
2	1000
3	10000

El *fit_PFD* de cada individuo se calcula empleando la siguiente ecuación:

$$fit\_PFD = \frac{1}{1+\mathcal{E}} \qquad \text{Ec. 5.6}$$

donde $\mathcal{E}$ viene dado por:

$$\mathcal{E} = \left| RRF\_tg - RRF \right| \qquad \text{Ec. 5.7}$$

RRF se obtiene de la ecuación Ec.5.1 y PFD_{AVG} se obtiene a partir de:

$$PFD_{AVG} = PFD_{AVG}\_1^{er}\,es + PFD_{AVG}\_2^{do}\,es + PFD_{AVG}\_ls + \\ + PFD_{AVG}\_1^{er}\,ef + PFD_{AVG}\_2^{do}\,ef \qquad \text{Ec. 5.9}$$

en la cual,

$PFD_{AVG}\_1^{er}\,es$: probabilidad de falla en demanda del 1^{er} elemento sensor/transmisor.

$PFD_{AVG}\_2^{do}\,es$: probabilidad de falla en demanda del 2^{do} elemento sensor/transmisor.

PFD_{AVG}_ls : probabilidad de falla en demanda del logic solver.

$PFD_{AVG}\_1^{er}\,ef$: probabilidad de falla en demanda del 1^{er} elemento final de control.

$PFD_{AVG}\_2^{do}\,ef$: probabilidad de falla en demanda del 2^{do} elemento final de control.

Estos valores dependen de la arquitectura de votación de los elementos respectivos y las ecuaciones para su determinación se presentan en la tabla 5.5.

El *fit_arq* de cada individuo se determina empleando la siguiente expresión:

$$fit\_arq = fit\_arq1^{er}\,es + fit\_arq2^{do}\,es + fit\_arqls + \\ + fit\_arq1^{er}\,ef + fit\_arq2^{do}\,ef \qquad \text{Ec. 5.10}$$

donde,

$fit\_arq1^{er}\,es$: fitness de arquitectura del 1^{er} elemento sensor/transmisor.

$fit\_arq2^{do}\,es$: fitness de arquitectura del 2^{do} elemento sensor/transmisor.

fit_arqls : fitness de arquitectura del logic solver.

$fit\_arq1^{er}\,ef$: fitness de arquitectura del 1^{er} elemento final de control.

$fit\_arq2^{do}\,ef$: fitness de arquitectura del 2^{do} elemento final de control.

Cada uno de estos valores se determinan empleando la tabla 5.5, en la cual se puede apreciar que la arquitectura más simple (1oo1) presenta el mayor fitness, mientras que la arquitectura más compleja (2oo3) se le asigna el menor fitness.

El valor ***a*** que aparece en la tabla 5.5 se calcula como:

$$a = \frac{1}{n^{o}\ de\ arquitecturas} = \frac{1}{7} = 0{,}1428571 \qquad \text{Ec. 5.11}$$

Tabla 5.5. Asignación de fitness de arquitectura.

Arquitectura	***fit_arq***
1oo1	1
1oo2	$1-a$
1oo1D	$1-2\cdot a$
1oo2D	$1-3\cdot a$
2oo2	$1-4\cdot a$
2oo2D	$1-5\cdot a$
2oo3	$1-6\cdot a$

Los valores de las presiones evolutivas (α y β), que se muestran en la tabla 5.6, dependen de el SIL requerido por la SIF. Estos valores se determinaron empíricamente.

Tabla 5.6. Presiones evolutivas

SIL requerido	**α**	**φ**
1	0,7	0,7
2	0,7	0,7
3	0,999	0,001

Cabe destacar que en el algoritmo genético desarrollado la selección de los individuos se realiza empleando el método de ventana deslizante exponencial, se emplea cruce multipunto y se trabaja con mutación de 10%. En el punto 1 del anexo 13 se coloca el listado del programa con los comentarios y explicaciones de la funcionalidad de cada una de las subrutinas desarrolladas en este módulo.

5.3.1.2. Módulo de verificación

Este módulo se desarrolló con la finalidad de poder verificar el desempeño, en términos de la probabilidad de falla en demanda promedio (PFD_{AVG}), de cada una de las SIF, teniendo como datos de entrada alguna de las siguientes combinaciones:

- Los elementos empleados (elementos sensor/transmisor, logic solver, elementos final de control) y el SIL requerido.
- Los elementos empleados (elementos sensor/transmisor, logic solver, elementos final de control) y sus arquitecturas.

En el primer caso, se determinan las arquitecturas de votación de los elementos empleados, que se necesitan para alcanzar el SIL requerido. En el segundo caso, se determina el nivel SIL que alcanza la SIF con los elementos empleados y su respectiva arquitectura de votación seleccionada.

En la figura 5.5 se muestra la interfaz gráfica del Módulo de Verificación.

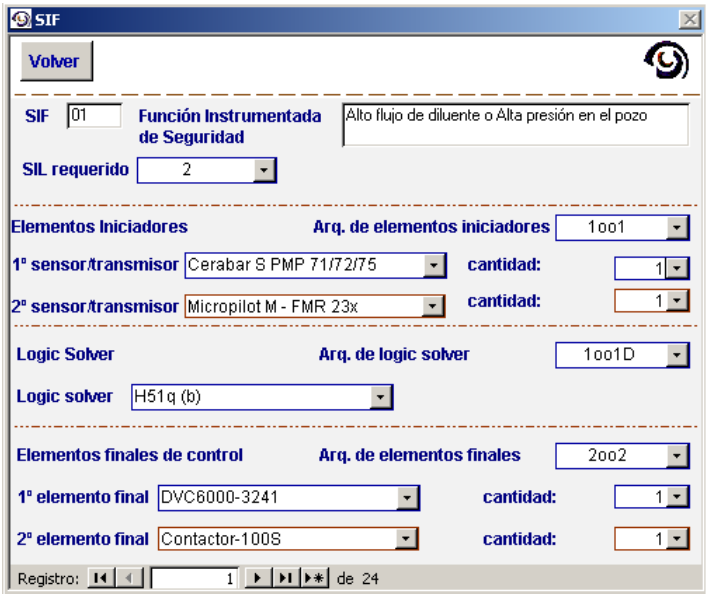

figura 5.5. Interfaz gráfica del módulo de verificación

En el punto 2 parte del anexo 13 se coloca el listado del programa con los comentarios y explicaciones de la funcionalidad de cada una de las subrutinas desarrolladas en este módulo.

5.3.2.3. Base de Datos

El programa "diseño" cuenta con una base de datos de equipos (elementos sensor/transmisor, logic solver y elementos finales de control) certificados por TÜV y/o ***exida.com*** para trabajar en sistemas instrumentados de seguridad. De esta base de datos, empleando comandos SQL, se extrae toda la información necesaria para que los módulos genético y de verificación puedan ejecutarse. La información contenida en esta base de datos es obtenida de los reportes FMEDA (Failure Modes, Effects and Diagnostic Analysis) generados por ***exida.com***, los cuales fueron proporcionados por los fabricantes.

En las figuras 5.6, 5.7 y 5.8 se muestra la interfaz gráfica para introducir la información de los elementos logic solver, sensor/transmisor y elementos finales de control a la base de datos respectivamente.

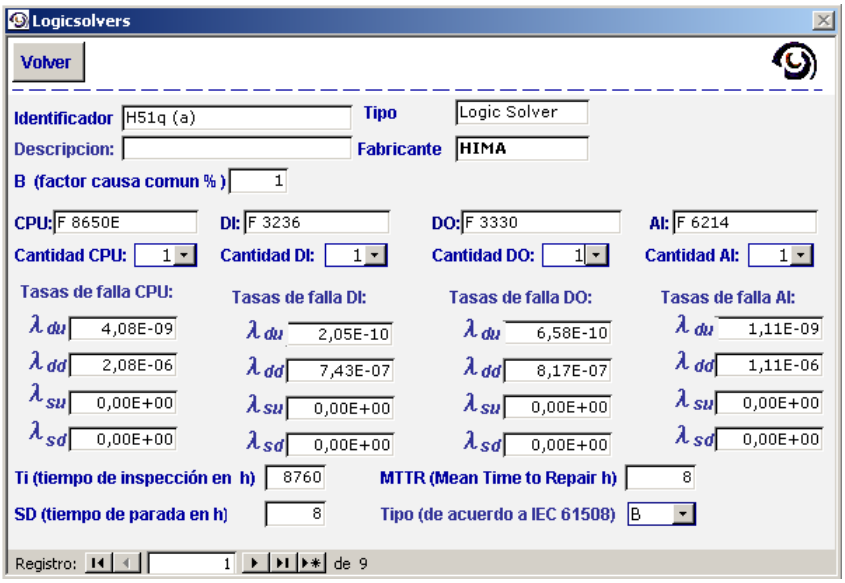

figura 5.6. Interfaz de base de datos Logic solver

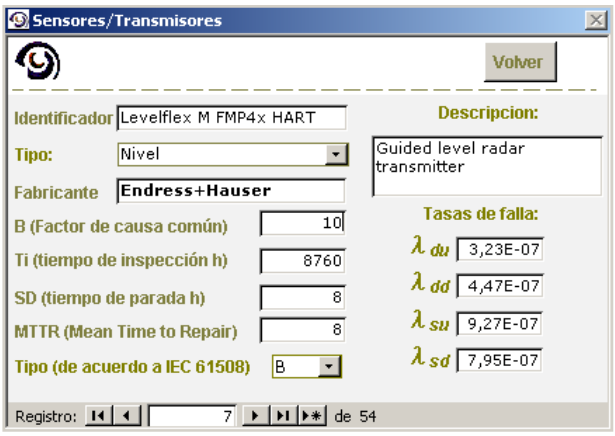

figura 5.7. Interfaz de base de datos Sensor/Transmisor

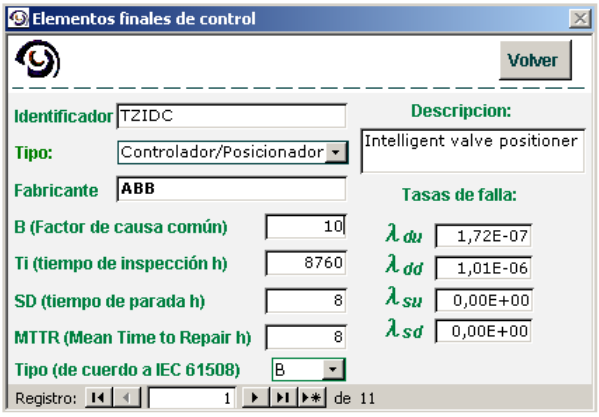

figura 5.8. Interfaz de base de datos Elementos finales de control

En general, los valores que se almacenan dentro de la base de datos, para cada uno de los equipos, son los siguientes:

- λ*du*: tasa de falla peligrosa no detectada (dangerous undetected).
- λ*dd*: tasa de falla peligrosa detectada (dangerous detected).
- λ*su*: tasa de falla segura no detectada (safe undetected).
- λ*sd*: tasa de falla segura detectada (safe detected).
- β: factor de causa común (en porcentaje).
- *MTTR*: tiempo medio de reparación (mean time to repair).

- Ti: tiempo de inspección.
- SD: tiempo de parada (shutdown time).
- Tipo (según clasificación IEC 61508).

5.3.2. Ecuaciones empleadas

Las ecuaciones empleadas en "diseño" se derivan del método de Análisis de Árboles de Falla y se extraen de la guía de ingeniería PDVSA 90620.1.117.

A partir de los valores que se encuentran en la base de datos, se calculan los siguientes parámetros:

- λdun: tasa de falla peligrosa no detectada normal.

$$\lambda dun = (1 - \beta) \cdot \lambda du \qquad \text{Ec. 5.12}$$

- λduc: tasa de falla peligrosa no detectada de causa común.

$$\lambda duc = \beta \cdot \lambda du \qquad \text{Ec. 5.13}$$

- λddn: tasa de falla peligrosa detectada normal.

$$\lambda ddn = (1 - \beta) \cdot \lambda dd \qquad \text{Ec. 5.14}$$

- λddc: tasa de falla peligrosa detectada de causa común

$$\lambda ddc = \beta \cdot \lambda dd \qquad \text{Ec. 5.15}$$

- λsun: tasa de falla segura no detectada normal.

$$\lambda sun = (1 - \beta) \cdot \lambda su \qquad \text{Ec. 5.16}$$

- λsuc: tasa de falla segura no detectada de causa común.

$$\lambda suc = \beta \cdot \lambda su \qquad \text{Ec. 5.17}$$

- λsdn: tasa de falla segura detectada normal.

$$\lambda sdn = (1 - \beta) \cdot \lambda sd \qquad \text{Ec. 5.18}$$

- λsdc: tasa de falla segura detectada de causa común.

$$\lambda sdc = \beta \cdot \lambda sd \qquad \text{Ec. 5.19}$$

- SFF: fracción de falla segura (safe failure fraction).

$$SFF = 1 - \frac{\lambda du}{\lambda du + \lambda dd + \lambda su + \lambda sd} \qquad \text{Ec. 5.20}$$

Empleando el SFF y el SIL requerido por la SIF con la que se esté trabajando, se determina el parámetro de tolerancia de falla de hardware (HFT: hardware failure tolerance) mínimo que debe tener el(los) elemento(s) (sensor/transmisor, logic solver y final de control) que integran la SIF de acuerdo la tabla 5.7, la cual se extrae de la norma IEC 61508.

Tabla 5.7. Tolerancia de Falla de Hardware (*HFT*) mínimo.

	Tipo A			**Tipo B**		
Safe Failure Fraction	**HFT**			**HFT**		
	0	**1**	**2**	**0**	**1**	**2**
< 60%	SIL 1	SIL 2	SIL 3	no permitido	SIL 1	SIL 2
60% a 90%	SIL 2	SIL 3	SIL 4	SIL 1	SIL 2	SIL 3
90% a 99%	SIL 3	SIL 4	SIL 4	SIL 2	SIL 3	SIL 4
≥ 99%	SIL 3	SIL 4	SIL 4	SIL 3	SIL 4	SIL 4

El HFT es empleado en los dos módulos del programa diseño para identificar cuáles arquitecturas de votación son válidas y cuáles no para un determinado elemento o conjunto de elementos en una SIF específica según la siguiente tabla:

Tabla 5.8. Arquitecturas permitidas según el HFT mínimo

HFT mínimo	**Arquitecturas Permitidas**
0	1oo1, 1oo1D, 1oo2, 1oo2D, 2oo2, 2oo2D, 2oo3
1	1oo2, 1oo2D, 2oo2, 2oo2D, 2oo3
2	2oo3

5.3.2.1. Ecuaciones para el cálculo de *PFD*$_{AVG}$

Las ecuaciones para el cálculo de la probabilidad de falla en demanda promedio (*PFD*$_{AVG}$) para cada una de las arquitecturas son las siguientes:

Tabla 5.9. Ecuaciones PFD_{AVG}.

1oo1	$\lambda dd \cdot MTTR + (\lambda du \cdot Ti)/2$
1oo2	$\frac{\lambda duc \cdot Ti}{2} + \lambda ddc \cdot MTTR + (\lambda ddn \cdot MTTR)^2 + \frac{(\lambda ddn \cdot MTTR \cdot \lambda dun \cdot Ti)^2}{2} + \frac{(\lambda dun \cdot Ti)^2}{3}$
2oo2	$\lambda ddc \cdot MTTR + \frac{\lambda duc \cdot Ti}{2} + 2 \cdot \lambda ddn \cdot MTTR + \lambda dun \cdot Ti$
2oo3	$3 \cdot \left(\frac{\lambda duc \cdot Ti}{2} + \lambda ddc \cdot MTTR + (\lambda ddn \cdot MTTR)^2 + \frac{\lambda ddn \cdot MTTR \cdot \lambda dun \cdot Ti}{2} + \frac{(\lambda dun \cdot Ti)^2}{3} \right)$
1oo1D	$\frac{\lambda du \cdot Ti}{2}$
2oo2D	$\frac{\lambda duc \cdot Ti}{2} + \lambda dun \cdot Ti$
1oo2D	$\frac{\lambda duc \cdot Ti}{2} + \frac{(\lambda dun \cdot Ti)^2}{3}$

5.3.2.2. Ecuaciones para el cálculo de *PFS*

Las ecuaciones para el cálculo de la probabilidad de falla segura (*PFS*) para cada una de las arquitecturas son las siguientes:

Tabla 5.10. Ecuaciones de *PFS*

1oo1	$\lambda sd \cdot SD + \lambda su \cdot SD$
1oo2	$(\lambda sdc + \lambda suc + 2 \cdot \lambda sdn + 2 \cdot \lambda sun) \cdot SD$
2oo2	$2 \cdot \left(\frac{\lambda sdc + \lambda suc}{2} + \lambda sdn^2 \cdot MTTR + \lambda sun \cdot Ti \cdot \lambda sdn + \lambda sdn \cdot MTTR \cdot \lambda sun + \lambda sun^2 \cdot Ti \right) \cdot SD$

2oo3	$6 \cdot \left(\frac{\lambda sdc + \lambda suc}{2} + \lambda sdn^2 \cdot MTTR + \lambda sun \cdot Ti \cdot \lambda sdn + \right.$ $\left. + \lambda sdn \cdot MTTR \cdot \lambda sun + \lambda sun^2 \cdot Ti \right) \cdot SD$
1oo1D	$(\lambda sd + \lambda su + \lambda dd) \cdot SD$
2oo2D	$2 \cdot \left(\frac{\lambda suc + \lambda sdc + \lambda ddc}{2} + (\lambda sdn + \lambda ddn)^2 \cdot MTTR + \right.$ $+ \lambda sun \cdot Ti \cdot (\lambda sdn + \lambda ddn) +$ $\left. + \lambda sun \cdot MTTR \cdot (\lambda sdn + \lambda ddn) + \lambda sun^2 \cdot Ti \right) \cdot SD$
1oo2D	$(\lambda sdc + \lambda suc + \lambda ddc) \cdot SD +$ $+ (\lambda sdn \cdot MTTR + \lambda ddn \cdot MTTR)^2 + (\lambda sun \cdot Ti)^2$

5.3.2.3. Ecuaciones para el cálculo de *MTTFs*

Las ecuaciones para el cálculo del tiempo medio de falla segura (MTTFs) para cada una de las arquitecturas son las siguientes:

Tabla 5.11. Ecuaciones de *MTTFs*

1oo1	$1/(\lambda sd + \lambda su)$
1oo2	$1/(\lambda \text{sdc} + \lambda \text{suc} + 2 \cdot \lambda \text{sdn} + 2 \cdot \lambda \text{sun})$
2oo2	$1 \Big/ \left(\lambda suc + \lambda sdc + \right.$ $\left. + 2 \cdot (\lambda \lambda dn^2 \cdot MTTR + \lambda sun \cdot Ti \cdot \lambda sdn + \lambda sdn \cdot MTTR \cdot \lambda sun + \lambda sun^2 \cdot Ti) \right)$
2oo3	$1 \Big/ \left(3 \cdot (\lambda suc + \lambda sdc) + \right.$ $\left. + 6 \cdot (\lambda \lambda dn^2 \cdot MTTR + \lambda sun \cdot Ti \cdot \lambda sdn + \lambda sdn \cdot MTTR \cdot \lambda sun + \lambda sun^2 \cdot Ti) \right)$
1oo1D	$1/(\lambda sd + \lambda su + \lambda dd)$
2oo2D	$1 \Big/ \left(\lambda suc + \lambda sdc + \lambda ddc + 2 \cdot \left(\begin{array}{l} (\lambda sdn + \lambda ddn)^2 \cdot MTTR + \lambda sun \cdot Ti \cdot (\lambda sdn + \lambda ddn) + \\ (\lambda sdn + \lambda ddn) \cdot MTTR \cdot \lambda sun + \lambda sun^2 \cdot Ti \end{array} \right) \right)$
1oo2D	$1/(\lambda sdc + \lambda suc + \lambda ddc + (\lambda sdn \cdot MTTR + \lambda ddn \cdot MTTR)^2 + (\lambda sun \cdot Ti)^2)$

5.3.3. Criterios utilizados en los cálculos

Los criterios en los que se basa el cálculo de los índices de seguridad PFD, PFS y MTTFs son los siguientes:

- La tasa de falla de los componentes es constante durante la vida del sistema.
- Componentes redundantes tienen iguales ratas de falla y tienen el mismo comportamiento operacional.
- Se asume que las fallas de los componentes individuales es estadísticamente independiente de los otros componentes, esto es, la falla de cualquier componente no inducirá falla a los otros componentes.
- El Tiempo de Reparación de los componentes es constante durante la vida del Sistema.
- Se asumen dos modos de falla: "Falla Segura" (S: Safe) y "Falla Peligrosa" (D: Dangerous) para un sistema inherentemente seguro (desenergizar para disparar).
- La aproximación ($MTTF = 1/\lambda$) es utilizada dado que se asume tasas de fallas constantes, es decir, que la distribución es exponencial. Igualmente las ecuaciones son válidas cuando la rata de reparación es mucho mayor que la rata de falla (1/MTTR>> λ, 10 a 1).

5.3.4. Pasos seguidos en el Diseño Detallado del SIS

Las SIF se agruparon de acuerdo a su configuración y SIL requeridos, como se indica en la tabla 5.12, con la finalidad de optimizar el proceso de diseño del SIS. Los pasos seguidos en el proceso de diseño son los siguientes:

- Para cada una de los grupos de SIF's (tabla 5.11) se introdujo la información correspondiente a su configuración y SIL requerido en la interfaz gráfica que se muestra en la figura 5.2., luego se ejecutó el módulo genético del programa diseño.
- De los resultados que arroja el algoritmo genético se tomó el que presentaba mayor fitness.

- Este último resultado (para cada SIF) se llevó al módulo de verificación, empleando la interfaz gráfica que se muestra en la figura 5.3, para corroborar la veracidad del resultado obtenido empleando el algoritmo genético y observar gráficamente el aporte (en porcentaje) de los distintos elementos de la SIF a la probabilidad de falla en demanda promedio (PFD_{AVG}) de la misma.

Tabla 5.12. Agrupación de las SIF's de acuerdo a sus requerimientos

SIF(s)	SIL	Elemento(s) iniciador(es)	Cantidad	Elemento(s) final(es)	Cantidad
13, 14, 15	3	Transmisor de Presión	2	Válvula shutdown	1
				Contactor	1
22, 23, 24	3	Transmisor de Presión	2	Válvula shutdown	2
				Contactor	1
17	3	Transmisor de Nivel	1	Válvula shutdown	2
16	3	Transmisor de Presión	1	Válvula shutdown	2
18, 19	2	Transmisor de Presión	2	Válvula shutdown	1
				Contactor	1
01	2	Transmisor de Presión	1	Válvula shutdown	1
				Contactor	1
11	2	Transmisor de Nivel	1	Válvula shutdown	2
09	2	Transmisor de Presión	1	Válvula shutdown	2
04, 05, 12, 20, 21	2	Transmisor de Nivel	1	Válvula shutdown	1
02, 03	2	Transmisor de Presión	1	Válvula shutdown	1
06, 07, 08	1	Transmisor de Presión	2	Válvula shutdown	1
				Contactor	1
10	1	Transmisor de Nivel	1	Válvula shutdown	2

Este procedimiento se realizó comenzando con las SIF con mayores requerimientos (SIF 13,14, 15) hasta las SIF con menores requerimientos (SIF 10); es decir, diseñando primero las SIF más exigentes. Esto se realizó de forma tal que si alguno de los elementos de una SIF con altos requerimientos forma parte de otra SIF con bajos requerimientos, ya la primera SIF esté bien definida y se asegure la confiabilidad y seguridad del diseño.

En el diseño de la SIF más exigente (SIF 13, 14, 15) se obtuvo como elemento logic solver el indicado en la tabla 5.13.

Tabla 5.13. Logic solver empleado

Logic solver	Arquitectura	Fabricante
H51q (b)	1oo1D	HIMA

Debido a que se emplea el mismo logic solver para todas las SIF y de acuerdo a lo planteado anteriormente, para el diseño definitivo de cada una de las SIF se tomó como elemento logic solver el indicado en la tabla 5.13; es decir, que de los resultados obtenidos del algoritmo genético se tomaron los referentes a los elementos sensor/transmisor y elementos finales de control pero manteniendo siempre el mismo logic solver con su respectiva arquitectura.

5.3.5. Resultados obtenidos

Los resultados obtenidos del empleo del módulo genético para cada una de los grupos de SIFs (tabla 5.12) se muestran en el anexo 10. Los resultados obtenidos del empleo del módulo de verificación para cada una de las SIFs se muestran en el anexo 11.

En la tabla 5.14 se muestra la descripción de cada una de las SIF diseñadas que conforman el SIS. Este diseño se refleja en los Diagramas de Tuberías e Instrumentación (P&ID) que se colocan en el anexo 5.

En la tabla 5.15 se presentan los equipos empleados como resultado del proceso de diseño. En el anexo 14 se presenta un resumen de las hojas de datos de cada uno de los equipos empleados

Tabla 5.14. SIFs del SIS

SIF	SIL	Función Instrumentada de Seguridad	Descripción de disparo	Sensor/transmisor	Punto de disparo	Arq.	Elemento final	(acción)	Arq.
S-01	SIL 2	Alto flujo de diluente o Alta presión en el pozo	Si la presión en el pozo alcanza 145 psig	0001-PT-1014	145 psig (inc)	1oo1	0001-SDV-1200A/B 0001-XY-1014A/B	cerrar abrir	2oo2
S-02	SIL 2	Alta - Alta presión en separador de producción 0002-V-1001A	Si la presión en el separador alcanza 83 psig	0002-PT-1306	83 psig (inc)	1oo1	0002-SDV-1004	cerrar	1oo1
S-03	SIL 2	Alta - Alta presión en separador de producción 0002-V-1001B	Si la presión en el separador alcanza 83 psig	0002-PT-1307	83 psig (inc)	1oo1	0002-SDV-1014	cerrar	1oo1
S-04	SIL 2	Alto - Alto nivel de líquido en separador de producción 0002-V-1001A	Si el nivel de líquido en el separador alcanza 6'-0"	0002-LT-1007A/B	6'-0" (inc)	2oo2	0002-SDV-1004	cerrar	1oo1
S-05	SIL 2	Alto - Alto nivel de líquido en separador de producción 0002-V-1001B	Si el nivel de líquido en el separador alcanza 6'-0"	0002-LT-1017A/B	6'-0" (inc)	2oo2	0002-SDV-1014	cerrar	1oo1
S-06	SIL 1	Alta - Alta presión aguas abajo o Baja presión aguas arriba de la bomba 0002-P-1001A	Si la presión a la succión disminuye de -2 psig o la presión a la descarga alcanza 305 psig	0002-PT-1009	-2 psig (dec)	1oo1	0002-SDV-1034A/B 0002-XY-1009A/B	cerrar abrir	2oo2
				0002-PT-1010	305 psig (inc)				
S-07	SIL 1	Alta - Alta presión aguas abajo o Baja presión aguas arriba de la bomba 0002-P-1001B	Si la presión a la succión disminuye de -2 psig o la presión a la descarga alcanza 305 psig	0002-PT-1019	-2 psig (dec)	1oo1	0002-SDV-1034A/B 0002-XY-1019A/B	cerrar abrir	2oo2
				0002-PT-1020	305 psig (inc)				

Tabla 5.14 (continuación). SIFs del SIS

SIF	SIL	Función Instrumentada de Seguridad	Descripción de disparo	Sensor/transmisor	Punto de disparo	Arq.	Elemento final	(acción)	Arq.
S-08	SIL 1	Alta - Alta presión aguas abajo o Baja presión aguas arriba de la bomba 0002-P-1001C	Si la presión a la succión disminuye de -2 psig o la presión a la descarga alcanza 305 psig	0002-PT-1025	-2 psig (dec)	1oo1	0002-SDV-1034A/B 0002-XY-1025A/B	cerrar abrir	2oo2
				0002-PT-1026	305 psig (inc)				
S-09	SIL 2	Alta - Alta presión en tanque de BHD 0002-TK-1001	Si la presión en el tanque alcanza 7" H2O	0002-PT-1322	7" H2O (inc)	1oo1	0002-SDV-1006A/B 0002-SDV-1016A/B	cerrar cerrar	2oo2
S-10	SIL 1	Alto - Alto nivel de líquido en tanque de BHD 0002-TK-1001	Si el nivel de líquido en el tanque alcanza 35'-0"	0002-LT-1035	35'-0" (inc)	1oo1	0002-SDV-1006A/B 0002-SDV-1016A/B	cerrar cerrar	2oo2
S-11	SIL 2	Alto - Alto nivel de líquido en el depurador de gas 0002-V-1301	Si el nivel de líquido en el depurador alcanza 4'-4"	0002-LT-1831A/B	4'-4" (inc)	2oo2	0002-SDV-1312 0002-SDV-1313	cerrar cerrar	1oo1
S-12	SIL 2	Alto - Alto nivel de líquido en tanque amortiguador de diluente 0002-TK-1201	Si el nivel de líquido en el tanque alcanza 29'-0"	0002-LT-1202A/B	29'-0" (inc)	2oo2	0002-SDV-1200	cerrar	1oo1
S-13	SIL 3	Alta - Alta presión aguas abajo o Baja presión aguas arriba de la bomba 0002-P-1201A	Si la presión a la succión disminuye de -1 psig o la presión a la descarga excede 525 psig	0002-PT-1206A/B	-1 psig (dec)	1oo2	0002-SDV-1203A/B/C 0002-XY-1206A/B/C	cerrar abrir	2oo3
				0002-PT-1207A/B	525 psig (inc)				
S-14	SIL 3	Alta - Alta presión aguas abajo o Baja presión aguas arriba de la bomba 0002-P-1201B	Si la presión a la succión disminuye de -1 psig o la presión a la descarga excede 525 psig	0002-PT-1212A/B	-1 psig (dec)	1oo2	0002-SDV-1203A/B/C 0002-XY-1212A/B/C	cerrar abrir	2oo3
				0002-PT-1213A/B	525 psig (inc)				

Tabla 5.14 (continuación). SIFs del SIS

SIF	SIL	Función Instrumentada de Seguridad	Descripción de disparo	Sensor/transmisor	Punto de disparo	Arq.	Elemento final	(acción)	Arq.
S-15	SIL 3	Alta - Alta presión aguas abajo o Baja presión aguas arriba de la bomba 0002-P-1201C	Si la presión a la succión disminuye de -1 psig o la presión a la descarga excede 525 psig	0002-PT-1218A/B	-1 psig (dec)	1oo2	0002-SDV-1203A/B/C 0002-XY-1218A/B/C	cerrar abrir	2oo3
				0002-PT-1219A/B	525 psig (inc)				
S-16	SIL 3	Alta - Alta presión en tambor K.O. del mechurrio 0002-V-1801	Si la presión en el tambor K.O alcanza 48 psig	0002-PT-1819A/B	48 psig (inc)	1oo2	0002-SDV-1821A/B 0002-SDV-1822A/B	cerrar	1oo2
S-17	SIL 3	Alto - Alto nivel de líquido en tambor K.O. del mechurrio 0002-V-1801	Si el nivel de líquido en el tambor K.O alcanza 3'-5"	0002-LT-1805A/B/C	3'-5" (inc)	2oo3	0002-SDV-1821A/B 0002-SDV-1822A/B	cerrar	1oo2
S-18	SIL 2	Alta - Alta presión aguas abajo o Baja presión aguas arriba de la bomba 0002-P-1801A	Si la presión a la succión disminuye de -2,8 psig o la presión a la descarga excede 20 psig	0002-PT-1806	-2,8 psig (dec)	1oo1	0002-SDV-1823A/B 0002-XY-1806A/B	cerrar abrir	2oo2
				0002-PT-1807	20 psig (inc)				
S-19	SIL 2	Alta - Alta presión aguas abajo o Baja presión aguas arriba de la bomba 0002-P-1801B	Si la presión a la succión disminuye de -2,8 psig o la presión a la descarga excede 20 psig	0002-PT-1811	-2,8 psig (dec)	1oo1	0002-SDV-1823A/B 0002-XY-1811A/B	cerrar abrir	2oo2
				0002-PT-1812	20 psig (inc)				
S-20	SIL 2	Alto - Alto nivel de líquido en tanque de almacenamiento de diluente 0004-TK-1201	Si el nivel de líquido alcanza 45'-0"	0004-LT-1202A/B	45'-0" (inc)	2oo2	0004-SDV-1200	cerrar	1oo1
S-21	SIL 2	Alto - Alto nivel de líquido en tanque de almacenamiento de diluente 0004-TK-1202	Si el nivel de líquido alcanza 45'-0"	0004-LT-1262A/B	45'-0" (inc)	2oo2	0004-SDV-1200	cerrar	1oo1

Tabla 5.14 (continuación). SIFs del SIS

SIF	SIL	Función Instrumentada de Seguridad	Descripción de disparo	Sensor/transmisor	Punto de disparo	Arq.	Elemento final	(acción)	Arq.
S-22	SIL 3	Alta - Alta presión aguas abajo o Baja presión aguas arriba de la bomba 0004-P-1201A	Si la presión a la succión disminuye de -1 psig o la presión a la descarga alcanza 175 psig	0004-PT-1205A/B	-1 psig (dec)	1oo2	0004-SDV-1203A/B/C 0004-SDV-1262A/B/C 0004-XY-1205A/B/C	cerrar cerrar abrir	2oo3
				0004-PT-1207A/B	175 psig (inc)				
S-23	SIL 3	Alta - Alta presión aguas abajo o Baja presión aguas arriba de la bomba 0004-P-1201B	Si la presión a la succión disminuye de -1 psig o la presión a la descarga alcanza 175 psig	0004-PT-1212A/B	-1 psig (dec)	1oo2	0004-SDV-1203A/B/C 0004-SDV-1262A/B/C 0004-XY-1212A/B/C	cerrar cerrar abrir	2oo3
				0004-PT-1214A/B	175 psig (inc)				
S-24	SIL 3	Alta - Alta presión aguas abajo o Baja presión aguas arriba de la bomba 0004-P-1201C	Si la presión a la succión disminuye de -1 psig o la presión a la descarga alcanza 175 psig	0004-PT-1219A/B	-1 psig (dec)	1oo2	0004-SDV-1203A/B/C 0004-SDV-1262A/B/C 0004-XY-1219A/B/C	cerrar cerrar abrir	2oo3
				0004-PT-1221A/B	175 psig (inc)				

Tabla 5.15. Equipos empleados

tag	Equipo	Modelo	Fabricante
0002-LT-1007A/B	Transmisor de Nivel	144LD / 244LD	Foxboro Eckardt GmbH
0002-LT-1017A/B	Transmisor de Nivel	144LD / 244LD	Foxboro Eckardt GmbH
0002-LT-1035	Transmisor de Nivel	144LD / 244LD	Foxboro Eckardt GmbH
0002-LT-1831A/B	Transmisor de Nivel	144LD / 244LD	Foxboro Eckardt GmbH
0002-LT-1202A/B	Transmisor de Nivel	144LD / 244LD	Foxboro Eckardt GmbH
0002-LT-1805A/B/C	Transmisor de Nivel	144LD / 244LD	Foxboro Eckardt GmbH
0004-LT-1202A/B	Transmisor de Nivel	144LD / 244LD	Foxboro Eckardt GmbH
0004-LT-1262A/B	Transmisor de Nivel	144LD / 244LD	Foxboro Eckardt GmbH
0001-PT-1014	Transmisor de Presión	Cerabar S PMP 71/72/75	Endress+Hauser
0002-PT-1306	Transmisor de Presión	Cerabar S PMP 71/72/75	Endress+Hauser
0002-PT-1307	Transmisor de Presión	Cerabar S PMP 71/72/75	Endress+Hauser
0002-PT-1009	Transmisor de Presión	Cerabar T PMP131	Endress+Hauser
0002-PT-1010	Transmisor de Presión	Cerabar T PMP131	Endress+Hauser
0002-PT-1019	Transmisor de Presión	Cerabar T PMP131	Endress+Hauser
0002-PT-1020	Transmisor de Presión	Cerabar T PMP131	Endress+Hauser
0002-PT-1025	Transmisor de Presión	Cerabar T PMP131	Endress+Hauser
0002-PT-1026	Transmisor de Presión	Cerabar T PMP131	Endress+Hauser
0002-PT-1322	Transmisor de Presión	Cerabar S PMP 71/72/75	Endress+Hauser
0002-PT-1206A/B	Transmisor de Presión	Cerabar T PMP131	Endress+Hauser
0002-PT-1207A/B	Transmisor de Presión	Cerabar T PMP131	Endress+Hauser
0002-PT-1212A/B	Transmisor de Presión	Cerabar T PMP131	Endress+Hauser
0002-PT-1213A/B	Transmisor de Presión	Cerabar T PMP131	Endress+Hauser
0002-PT-1218A/B	Transmisor de Presión	Cerabar T PMP131	Endress+Hauser
0002-PT-1219A/B	Transmisor de Presión	Cerabar T PMP131	Endress+Hauser
0002-PT-1819A/B	Transmisor de Presión	Cerabar T PMP131	Endress+Hauser
0002-PT-1806	Transmisor de Presión	Cerabar S PMP 71/72/75	Endress+Hauser
0002-PT-1807	Transmisor de Presión	Cerabar S PMP 71/72/75	Endress+Hauser
0002-PT-1811	Transmisor de Presión	Cerabar S PMP 71/72/75	Endress+Hauser
0002-PT-1812	Transmisor de Presión	Cerabar S PMP 71/72/75	Endress+Hauser
0004-PT-1205A/B	Transmisor de Presión	Cerabar T PMP131	Endress+Hauser
0004-PT-1207A/B	Transmisor de Presión	Cerabar T PMP131	Endress+Hauser
0004-PT-1212A/B	Transmisor de Presión	Cerabar T PMP131	Endress+Hauser
0004-PT-1214A/B	Transmisor de Presión	Cerabar T PMP131	Endress+Hauser
0004-PT-1219A/B	Transmisor de Presión	Cerabar T PMP131	Endress+Hauser
0004-PT-1221A/B	Transmisor de Presión	Cerabar T PMP131	Endress+Hauser
0001-SDV-1200A/B	Válvula shutdown	DVC6000 - 3241	Fisher - Samson
0002-SDV-1004	Válvula shutdown	SVM - 3241	Drallim - Samson
0002-SDV-1014	Válvula shutdown	SVM - 3241	Drallim - Samson
0002-SDV-1034A/B	Válvula shutdown	ESD	---
0002-SDV-1006A/B	Válvula shutdown	SVM - 3241	Drallim - Samson
0002-SDV-1016A/B	Válvula shutdown	SVM - 3241	Drallim - Samson
0002-SDV-1312	Válvula shutdown	SVM - 3241	Drallim - Samson
0002-SDV-1313	Válvula shutdown	SVM - 3241	Drallim - Samson

Tabla 5.15 (continuación). Equipos empleados

tag	Equipo	Modelo	Fabricante
0002-SDV-1200	Válvula shutdown	SVM – 3241	Drallim – Samson
0002-SDV-1203A/B/C	Válvula shutdown	SVM – 3241	Drallim - Samson
0002-SDV-1821A/B	Válvula shutdown	SVM - 3241	Drallim - Samson
0002-SDV-1822A/B	Válvula shutdown	SVM - 3241	Drallim - Samson
0002-SDV-1823A/B	Válvula shutdown	SVM - 3241	Drallim - Samson
0004-SDV-1200	Válvula shutdown	SVM - 3241	Drallim - Samson
0004-SDV-1203A/B/C	Válvula shutdown	SVM - 3241	Drallim - Samson
0004-SDV-1262A/B/C	Válvula shutdown	SVM - 3241	Drallim - Samson
0001-XY-1014A/B	Contactor	100S	Rockwell Automation
0002-XY-1009A/B	Contactor	100S	Rockwell Automation
0002-XY-1019A/B	Contactor	100S	Rockwell Automation
0002-XY-1025A/B	Contactor	100S	Rockwell Automation
0002-XY-1206A/B/C	Contactor	100S	Rockwell Automation
0002-XY-1212A//C	Contactor	100S	Rockwell Automation
0002-XY-1218A/B/C	Contactor	100S	Rockwell Automation
0002-XY-1806A/B	Contactor	100S	Rockwell Automation
0002-XY-1811A/B	Contactor	100S	Rockwell Automation
0004-XY-1205A/B/C	Contactor	100S	Rockwell Automation
0004-XY-1212A/B/C	Contactor	100S	Rockwell Automation
0004-XY-1219A/B/C	Contactor	100S	Rockwell Automation

5.4. Matriz Causa – Efecto del SIS

Los resultados obtenidos del diseño del SIS se resumen en la matriz Causa – Efecto que se presenta a continuación. Por otro lado la narrativa lógica del SIS diseñado se presenta en el anexo 6.

CONCLUSIONES

Se logró la determinación del Nivel de Integridad de Seguridad (SIL) y el diseño del Sistema Instrumentado de Seguridad (SIS) para las facilidades de proceso de una planta de extracción de crudo pesado y su planta de tratamiento asociada, cumpliendo con las normas ISA e IEC relacionadas con el tema.

La determinación del Nivel de Integridad de Seguridad (SIL) por el método cualitativo de Gráfica de Riesgo depende principalmente de la experiencia y conocimientos previos acerca del proceso bajo estudio de la persona que realiza el análisis, por lo tanto su resultado es subjetivo y no es reproducible.

La determinación del Nivel de Integridad de Seguridad (SIL) por el método Semi-Cuantitativo empleado establece una metodología en la que los aspectos cualitativos influyen en un porcentaje mínimo, por lo cual se obtienen resultados objetivos, confiables y reproducibles.

El método cualitativo de Gráfica de Riesgo es fácil de implementar en comparación con el método Semi-Cuantitativo, el cual requiere de mayor esfuerzo y horas hombre de trabajo.

Se desarrolló el programa “cualitativo” para minimizar el tiempo empleado en la determinación cualitativa del Nivel de Integridad de Seguridad (SIL) con el método de Gráfica de Riesgo. Esta aplicación se desarrolló en Microsoft Access empleando como plataforma de programación Microsoft Visual Basic para Aplicaciones y consultas SQL.

Se desarrolló el programa “diseño” para realizar el análisis de desempeño y diseño de cada una de las Funciones Instrumentadas de Seguridad (SIF) que conforman el SIS. Con la finalidad de optimizar el proceso de diseño de cada SIF se implementó un algoritmo genético, el cual determina la mejor configuración de la misma en términos de menor probabilidad de falla en demanda promedio (PFD_{AVG}) y de menor complejidad de arquitectura de votación de los elementos que la componen.

Esta apliación se desarrolló en Microsoft Access empleando como plataforma de programación Microsoft Visual Basic para Aplicaciones.

A partir de los resultados obtenidos de la realización de este trabajo, el personal de ingeniería del área de instrumentación y control de la empresa VEPICA logró afirmar los conocimientos en el tema de Sistemas Instrumentados de Seguridad, lo cual se traduce en un mejor criterio de cálculo, análisis y diseño de los SIS y su respectivo SIL.

Se desarrolló un documento que puede servir como tutorial teórico/práctico para el cálculo de SIL y diseño de SIS.

RECOMENDACIONES

En futuros proyectos el Nivel de Integridad de Seguridad (SIL) se debe determinar empleando métodos cuantitativos. Los métodos cualitativos se deben emplear sólo para tener aproximaciones iniciales del SIL.

Para la determinación del SIL por métodos cualitativos se debe conformar un equipo multidisciplinario conformado por personal de ingeniería con experiencia en el área de riesgos, instrumentación y procesos con la finalidad de obtener un resultado confiable.

En proyectos grandes (más de 40 lazos críticos a analizar) se debe conformar un equipo de trabajo para realizar el estudio del SIL y el diseño del Sistema Instrumentado de Seguridad (SIS) lo más eficientemente posible en términos de tiempo. El número de integrantes de dicho equipo de trabajo debe establecerse de acuerdo a la complejidad de la planta y proceso a estudiar.

El fitness compuesto del algoritmo genético desarrollado para el diseño del SIS, se debe ampliar colocando un fitness que controle el costo real del ciclo de vida de los equipos (instalación y mantenimiento) con la finalidad de tener la capacidad de diseñar un SIS con mejores características costo-efectivas.

La base de datos de equipos (elementos sensor/transmisor, logic solver y elementos finales de control) certificados por TÜV y/o *exida.com* para trabajar en sistemas instrumentados de seguridad, se debe continuar ampliando con el objetivo de tener mayor información de la diversidad de equipos que existen en el mercado al momento de diseñar un SIS.

La empresas que realicen estudios del SIL deben adquirir los software especializados para el Análisis de Árboles de Falla (ejemplo: Logan Fault and Event Tree Analysis de RM Consultants, CARA-Fault Tree de Sydvest Software, FaultTree+ de Isograph Inc.) y Cálculo de Consecuencias (FRED de Shell Global Solutions, Canary de QUEST Consultants Inc.), necesarios para el cálculo cuantitativo del SIL.

REFERENCIAS BIBLIOGRÁFICAS

[1] PDVSA IR–S–00 (1992). Definiciones. Caracas: PDVSA. p. 17.

[2] PDVSA IR–S–02 (1993). Criterios para el Análisis Cuantitativo de Riesgos. Caracas: PDVSA. p.p. 8 - 20.

[3] Storch De Gracia, J.M. *Manual de seguridad Industrial en plantas químicas y Petroleras,* (Libro). Madrid: McGraw-Hill/Interamericana de España, 1998, p. 51.

[4] Goble, William. *Evaluating Control Systems Reliability, Techniques and Applications,* (Libro). USA: The Instrumentation, Systems and Automation Society (ISA), 1992, p.p. 43 - 265.

[5] IEC 61508 (1997). Functional Safety of electrical/electronic/ programmable electronic safety-related systems. International Electrotechnical Commission (IEC).

[6] ANSI/ISA-84.00.01-2004 (2004). Functional Safety: Safety Instrumented Systems for the Process Industry Sector. USA: The Instrumentation, Systems and Automation Society (ISA).

[7] PDVSA IR-P-02 (2002). Nivel de Integridad (SIL) de un Sistema Instrumentado de Seguridad (SIS). Caracas: Petróleos de Venezuela, S.A. (PDVSA). p. 17- 18

[8] Summers, Angela. *Viewpoint on ISA TR84.0.02 – Simplified Methods and Fault Tree Analysis*. Houston: SIS-TECH Solutions, LLC, 1999, p.p. 4 – 14.

[9] E&P Forum. Hydrocarbon Leak and Ignition Database, E&P Forum, Mayo 1992.

[10] Off Shore Reliability Data (1997), Det Norske Veritas, OREDA Publications.

BIBLIOGRAFÍA

1. ANSI/ISA-84.00.01-2004 (2004). Functional Safety: Safety Instrumented Systems for the Process Industry Sector. USA: The Instrumentation, Systems and Automation Society (ISA).
2. IEC 61508 (1997). Functional Safety of electrical/electronic/ programmable electronic safety-related systems. International Electrotechnical Commission (IEC).
3. IEC 61511 (2003). Functional Safety: Safety Instrumented Systems for the Process Industry Sector. International Electrotechnical Commission (IEC).
4. Mijares, Rubén. Desarrollo de una metodología para el diseño de Sistemas de Seguridad y Protección de la estación de producción del Centro Operativo Carito. Mijares Rubén (Tesis). Caracas: Universidad Central de Venezuela, 2000.
5. PDVSA IR-P-02 (2002). Nivel de Integridad (SIL) de un Sistema Instrumentado de Seguridad (SIS). Caracas: Petróleos de Venezuela, S.A. (PDVSA).
6. PDVSA IR–S–02 (1993). Criterios para el Análisis Cuantitativo de Riesgos. Caracas: Petróleos de Venezuela, S.A. (PDVSA).
7. PDVSA 90620.1.117 (2002). Selección y verificación de la arquitectura de un Sistema Instrumentado de Seguridad (SIS). Caracas: Petróleos de Venezuela, S.A. (PDVSA).
8. PEMEX NRF-045 (2003). Determinación del Nivel de Integridad de Seguridad de los Sistemas Instrumentados de Seguridad. México: Petróleos Mexicanos (PEMEX).
9. PIP PCESS001 (1999). Safety Instrumented Systems Guidelines. USA: Process Industry Practices (PIP).
10. Dr. Stamatelatos, Michael. Fault Tree Handbook with aerospace applications, Washington: NASA, 2002.

11. Trujillo, Damián. Actualización tecnológica de sistema de control de los expansores-compresores de la Planta Extracción San Joaquín. Trujillo Damián (Tesis). Caracas: Universidad Central de Venezuela, 2002.
12. Risknowlogy. A practical approach for the selection of programmable electronic systems used for safety functions in the process industry [en línea] <http://www.risknowlogy.com>[Consulta: 2004].
13. Exida.com. Selecting Instrumentation Equipment for safety Applications [en línea] <http://www.exida.com>[Consulta: 2005].

GLOSARIO

Arquitectura. Arreglo de elementos de hardware y/o software en un sistema, por ejemplo,

- arreglo de los subsistemas de un sistema instrumentado de seguridad (SIS);
- estructura interna de un subsistema de un SIS;
- arreglo interno de programas de software.

Canal. Elemento o grupo de elementos que independientemente realizan una función.

Capas de protección. Sistemas de protección que generalmente involucran diseños especiales, equipo de proceso, sistema de control básico de proceso, procedimientos administrativos, y/o respuestas planeadas para protección contra un riesgo inminente.

Chorro de Fuego ("Jet Fire"). Incendio a manera de soplete resultante de la ignición inmediata de una fuga de un líquido y/o gas presurizado.

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

Componente. Una de las partes de un sistema, subsistema o elemento que realiza una función específica.

Complejidad. Un indicador del número de grados de libertad al cometer errores.

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

Demanda. Una condición ó evento que requiere que el SIS lleve a cabo una acción apropiada para prevenir un evento peligroso, ó para mitigar sus consecuencias.

Desenergizado para disparo. Circuitos SIS en donde las salidas y dispositivos se encuentran energizados en operación normal. Cuando se suspende el suministro de energía se produce una acción de disparo.

Disparos en falso. Activación de cualquier Función Instrumentada de Seguridad (FIS) perteneciente al SIS, sin existir una demanda real en campo.

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

Dispositivo. Unidad funcional de hardware o software, capaz de cumplir un propósito específico (por ejemplo: dispositivos de campo, sensores, elementos finales de control, logic solvers).

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

Elemento final. Parte de un SIS que implementa la acción física necesaria para alcanzar el estado seguro.

Energizado para disparo. Circuitos SIS en donde las salidas y dispositivos se encuentran desenergizados en operación normal. Cuando a dichos circuitos se les aplica energía se produce una acción de disparo.

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

Explosión. Liberación masiva de energía que causa una discontinuidad de presión u onda de sobrepresión. Las explosiones pueden ser de tipo físico o químico. A su vez las explosiones de tipo químico pueden ser detonaciones o deflagraciones.

Explosión de una Nube de Vapor ("VCE"). Evento que puede ocurrir como consecuencia del escape masivo de un gas o líquido volátil inflamable produciéndose una nube, que al encontrar un foco de ignición empieza a arder en la periferia, generando mayor inducción de aire hacia el centro de la misma y en consecuencia una aceleración de la velocidad de combustión, que finalmente termina en una explosión.

Falla. Terminación de la habilidad de una unidad funcional de realizar una función determinada.

Falla dependiente. Falla cuya probabilidad no puede ser expresada como el simple producto de las probabilidades incondicionales de los eventos individuales que la ocasionan.

Falla no revelada. Fallas que pueden ser clasificadas como ocultas, encubiertas, no detectadas, latentes, entre otras.

Falla peligrosa. Fallas que tienen el potencial de colocar el SIS en un estado peligroso (no seguro).

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

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

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

Fitness. Valor que representa la capacidad de un individuo para resolver un determinado problema. Este valor puede variar de 0 a 1, donde 0 representa el menor fitness y 1 el mayor.

Fogonazo ("Flash– Fire"). Combustión de una mezcla de vapor inflamable en aire, en la cual el frente de llama pasa a través de la porción de mezcla que no ha reaccionado, a una velocidad menor que la del sonido, de forma tal que se genera radiación térmica y cierta sobrepresión. La sobrepresión es despreciable en comparación con las consecuencias de la radiación térmica.

Función lógica. Función que realiza la transformación entre la información de entrada y la información de salida; las funciones lógicas realizan la transformación de una o más funciones de entrada en una o más funciones de salida.

Función de seguridad. Es aquella función implantada por un sistema de seguridad.

Intervalo de prueba. Intervalo de tiempo entre pruebas funcionales.

Instrumento. Aparato usado para realizar una acción específica.

Knock out drum. Tambor de estabilización.

Mitigación. Acción que reduce las consecuencias de un evento peligroso.

Modo degradado. Es aquél estado en el cuál el SIS aún está operando satisfactoriamente pero se encuentra vulnerable con respecto a fallas posteriores.

MooN. SIS o parte de él, que consta de "N" canales independientes, conectados de manera tal que "M" canales son suficientes para realizar la función instrumentada de seguridad.

Probabilidad. La probabilidad es un método cuantitativo de expresar el azar. Se trata de asignar un número entre 0 y 1, ambos inclusive. Una probabilidad de 0 significa que el evento nunca es esperado. Una probabilidad de 1 significa que el evento es siempre esperado.

Probabilidad de Falla en Demanda (PFD). Un valor que indica la probabilidad de que un SIS falle para responder a una demanda.

Procesador lógico (logic solver). Es la parte del SIS que realiza una o más funciones lógicas. Éste es un sistema o elemento electrónico diseñado para tomar las acciones necesarias sobre la base de una lógica determinada, estos sistemas incluyen módulos de entrada y salida.

Prueba funcional. Actividad periódica para verificar que el SIS esta en operación de acuerdo a la especificación de los requerimientos de seguridad.

Redundancia. Uso de elementos o sistemas múltiples, de igual o diferente tecnología, para desempeñar la misma función.

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

Relé (Contactor). Relevador. Tecnología usada en Sistemas Instrumentados de Seguridad basada en señales lógicas discretas (encendido/apagado).

Seguridad. Libertad de riesgo inaceptable.

Sensor. Dispositivo o combinación de dispositivos que miden las condiciones del proceso (transmisores, interruptores de proceso, interruptores de posición, entre otros).

Skid. Patín para sistemas de medición.

Sistema. Conjunto de elementos que interactúan de acuerdo a un diseño. Un elemento de un sistema puede ser otro sistema, llamado subsistema, el cual puede ser un sistema controlador o un sistema controlado y puede incluir hardware, software e interacción humana.

Sistema Básico de control de Proceso (BPCS). Este sistema responde a señales de entrada del proceso, su equipo asociado, otros sistemas programables y/o un operador y genera señales de salida haciendo que el proceso y sus equipos asociados operen de una manera previamente determinada. Este sistema no realiza ninguna función instrumentada de seguridad con un SIL ≥ 1.

Sistemas de seguridad. Es todo aquél sistema que implanta las funciones de seguridad necesarias para mantener un estado seguro en el equipo bajo control.

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

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

Validación. Confirmación por medio de revisión y suministro de evidencia objetiva que los requerimientos particulares para un uso particular y específico son totalmente cumplidos.

Válvula de shutdown. Válvula de bloqueo.

Verificación. Confirmación por medio de revisión y suministro de evidencia objetiva del cumplimiento total de los requerimientos.

Well casing. Chaqueta de protección del pozo.