INFORME DEL TRABAJO DE GRADO

"DESARROLLO DE UNA METODOLOGÍA PARA EL DISEÑO DE SISTEMAS DE SEGURIDAD Y PROTECCIÓN DE LA ESTACIÓN DE PRODUCCIÓN DEL CENTRO OPERATIVO CARITO"

Autor: MIJARES SEMINARIO,
RUBÉN ENRIQUE.

Trabajo presentado ante la Ilustre Universidad Central de Venezuela para optar al Titulo por Reválida de Ingeniero Electricista

Junio, 2000

INFORME DEL TRABAJO DE GRADO

'DESARROLLO DE UNA METODOLOGÍA PARA EL DISEÑO DE SISTEMAS DE SEGURIDAD Y PROTECCIÓN DE LA ESTACIÓN DE PRODUCCIÓN DEL CENTRO OPERATIVO CARITO"

Autor: MIJARES SEMINARIO, RUBÉN ENRIQUE.

Trabajo presentado ante la Ilustre Universidad Central de Venezuela para optar al Titulo por Reválida de Ingeniero Electricista

Junio, 2000

Autor: Mijares Seminario, Rubén E.

Titulo Académico a obtener: Ingeniero Electricista

Universidad, fecha: Universidad Central de Venezuela, 5 de Junio del 2000.

Profesor Guía: Ing. Pedro Pablo Pinto Rodríguez.

Titulo del Trabajo: DESARROLLO DE UNA METODOLOGÍA PARA EL DISEÑO DE SISTEMAS DE SEGURIDAD Y PROTECCIÓN DE LA ESTACIÓN DE PRODUCCIÓN DEL CENTRO OPERATIVO CARITO.

RESUMEN

La seguridad de los procesos es hoy en día un tema que ha alcanzado gran relevancia y por tal razón se ha considerado importante trabajar este aspecto dentro del contexto de los Sistemas Instrumentados de Seguridad y Protección, su aplicación en el diseño de plantas industriales debe ser parte elemental del diseño del proceso y de los equipos. En este trabajo de desarrolla una metodología para el diseño del Sistema Instrumentado de Seguridad (SIS) que permite alcanzar la disponibilidad requerida para el Nivel de Integridad de Seguridad (SIL) calculado para la estación de Producción de Carito (COC).

Se describen los diferentes tópicos teóricos y prácticos relacionados con los Sistemas Instrumentados de Seguridad, indicando las fuentes y técnicas utilizadas, así como una descripción general del Centro Operativo Carito y un estudio de cuatro lazos de control críticos para esta estación de producción:

• Bajo-Bajo Nivel de Crudo en el Separador Gas Crudo. • Alto-Alto Nivel de Crudo en los Tanques.

• Alto-Alto Diferencial de Presión a la Entrada de las Bombas de Transferencia. • Bajo-Bajo Nivel de Crudo en el Separador-Hidrostático.

El SIL del Proceso se determina mediante el método Cualitativo/Cuantitativo y para el procesamiento de la información se utilizó una Hoja de Cálculo Excel de Microsoft.

DEDICATORIA

Gracias a Dios y a mis Padres por ser la fuente de iluminación para mi desarrollo profesional.

A mi esposa Eunice por su comprensión, amor e infinita paciencia.

A mis hijos Simón, Rubén y Gabriel, que les sirva de ejemplo para su constante desarrollo y superación.

A los estudiantes de Ingeniería Eléctrica de la UCV y de otras universidades del país, así como a los profesionales interesados en el tema de la Seguridad y Protección de las instalaciones industriales.

AGRADECIMIENTOS

Agradecimiento a PDVSA, S.A. quien siempre me estimulo para hacer la reválida y me dio todo el apoyo material y moral para el logro de este objetivo.

Al Prof. de Ingeniería Eléctrica Pedro Pinto, mi Tutor Académico, por su comprensión, calidad humana y su orientación en el aspecto metodológico de este trabajo.

Al apreciado estudiante de Ingeniería Eléctrica y actual colega Wilmer Guerrero, por su gran colaboración en el logro de esta importante meta.

A mis colegas Ingenieros Nerio Zambrano, Gonzalo J. Alvarado y Carlos Hernández, con quienes en la confrontación y tormenta de ideas, me ayudaron a darle una mayor calidad y valor agregado a mi trabajo.

ÍNDICE GENERAL

	Pág.
RESUMEN	II
DEDICATORIA	IV
AGRADECIMIENTOS	V
ÍNDICE GENERAL	VI
ÍNDICE DE FIGURAS	X
ÍNDICE DE TABLAS	XII
INTRODUCCIÓN	1
CAPÍTULO 1. PLANTEAMIENTO DEL PROBLEMA	2
1.1.TRANSFORMACIÓN Y ÉXITO.	2
1.2.JUSTIFICACIÓN.	6
1.3.ALCANCE.	8
1.4.LIMITACIONES.	8
1.5.OBJETIVOS.	9
1.5.1. Objetivo General.	9
1.5.2. Objetivos Específicos.	9
CAPÍTULO 2. MARCO TEÓRICO	11
2.1.PELIGRO.	11
2.1.1. Identificación de Peligros.	11
2.1.1.1. Análisis de Riesgo Preliminar (PHA).	12
2.1.1.2. Estudio de Operabilidad y Peligro (HAZOP).	12
2.2.RIESGO.	13
2.2.1. Cuantificación del Riesgo.	14
2.2.1.1. Riesgo Individual.	15
2.2.1.2. Riesgo Social.	16

Pág.

2.3.FILOSOFÍA DE DISEÑO SEGURO. 17
2.3.1. Principios Fundamentales para un Diseño Seguro. 18
2.4.SISTEMA INSTRUMENTADO DE SEGURIDAD (SIS). 20
2.4.1. Estados del SIS. 21
2.4.2. Términos Estadísticos. 23
2.5.CARACTERÍSTICAS DE LOS SIS. 24
2.5.1. Índices de Desempeño. 25
2.5.2. Función Distribución de Falla (Distribución Exponencial). 28
2.5.3. Relación entre los Indices de Seguridad. 31
2.5.4. Índices de Integridad. 31
2.6.MÉTODOS CUALITATIVOS Y CUANTITATIVOS PARA LA DETERMINACIÓN DEL SIL REQUERIDO POR EL PROCESO. 32
2.6.1. Métodos Cualitativos. 32
2.6.1.1. Método General de Matriz de Capas de Seguridad. 35
2.6.1.2. Método General de Gráfica de Riesgo. 37
2.6.2. Método Cuantitativo. 42
2.7.CAPAS DE PROTECCIÓN INDEPENDIENTES [IPL(S)]. 45
2.7.1. Reglas para IPL(s). 46
2.7.2. Reducción de Riesgo Necesaria. 49
2.8.CONFIGURACIÓN DE UN SIS. 49
2.8.1. Modelaje de Sensores y Elementos Finales de Control. 50
2.8.2. Modelaje del Sistema Controlador Programable (PES). 50
2.8.3. Riesgo y la Integridad de Seguridad. 51
2.8.4. Técnica de Evaluación. 52
2.8.5. Cálculo de un SIL de un SIS utilizando las Ecuaciones Simplificadas. 52
2.8.6. Determinación del SIL de un SIS utilizando el Análisis de Árbol de Falla. 53
2.8.7. Determinación del SIL de un Modelo de Markov. 53
2.8.8. Diagnostico en Línea. 54
2.8.9. Aproximaciones Asumidas Para los Cálculos. 55

Pág.

2.8.10. Base de Datos de Confiabilidad del Equipo. 56
2.8.10.1. Modos de Fallas. 61
2.8.10.2. Selección de la Data de Rata de Fallas. 61
2.8.10.3. Cálculo del $PFD_{PELIGROSO}$. 62
2.9. ARQUITECTURAS DEL SIS. 64
2.9.1. Arquitectura 1001. 64
2.9.2. Arquitectura 1002. 65
2.9.3. Arquitectura 2002. 68
2.9.4. Arquitectura 1001D. 70
2.9.5. Arquitectura 2003. 71
2.9.6. Arquitectura 2002D. 74
2.9.7. Arquitectura 1002D. 77

CAPÍTULO 3. MARCO METODOLÓGICO 79
3.1. FUENTES Y TÉCNICAS RECOPILADAS. 80
3.2. TRATAMIENTO DE LA INFORMACIÓN. 81
3.3. DISEÑO DE LA INVESTIGACIÓN. 81

CAPÍTULO 4. METODOLOGÍA PARA LA DETERMINACIÓN DEL SIL DEL SIS 84
4.1. METODOLOGÍA DISEÑADA. 84
4.2. DISEÑO, VERIFICACIÓN Y VALIDACIÓN DEL SIS. 88
4.3. TABLAS DE TÉRMINOS Y RANGOS SUGERIDOS. 90

CAPÍTULO 5. DESARROLLO CENTRO OPERATIVO CARITO 99
5.1. DESCRIPCIÓN GENERAL DEL CASO EN ESTUDIO. 99
5.2. OPERACIÓN Y CONTROL DE LA ESTACIÓN. 102
5.3. IDENTIFICACIÓN PARCIAL DE EVENTOS PELIGROSOS. 106
5.4. IDENTIFICACIÓN DE LOS LAZOS CRÍTICOS DEL PROCESO C.O.C. 108
5.5. MÉTODO CUALITATIVO / CUANTITATIVO PARA LA DETERMINACIÓN DEL SIL DEL PROCESO. 109

Pág.

5.5.1. Evento 1: Arrastre de Gas por una Línea de Liquido. 109

5.5.1.1. Análisis Cualitativo. 110

5.5.1.2. Determinación de las Capas Independientes de Protección Evento 1. 111

5.5.2. Evento 2: Alto Alto Nivel de Crudo en los Tanques de Estabilización T-01A/B. 112

5.5.2.1. Análisis Cuantitativo. 115

5.5.2.2. Determinación de las Capas Independientes de Protección Evento 2. 116

5.5.3. Evento 3: Baja Presión de Succión Bombas de Crudo Sucio P-0702 A/B. 117

5.5.3.1. Análisis Cuantitativo. 119

5.5.3.2. Determinación de las Capas Independientes de Protección Evento 3. 120

5.6. CONFIGURACIÓN DEL SIS. 128

5.7. SELECCIÓN DE LAS ARQUITECTURAS DEL SIL QUE CUMPLEN EL SIL REQUERIDO. 128

CONCLUSIONES **140**

REFERENCIAS BIBLIOGRÁFICAS **142**

ANEXOS **143**

ÍNDICE DE FIGURAS

Pág.

Capítulo 2.

Figura 2.1.- Criterio PDVSA de Tolerancia del Riesgo Social. 17

Figura 2.2.- Proceso de un Diseño de Seguridad. 19

Figura 2.3.- Definición del Sistema Instrumentado de Seguridad. 21

Figura 2.4.- Modos de Fallas. 24

Figura 2.5.- Diagrama de Venn del SIS. Availability. 26

Figura 2.6.- Diagrama de Venn del SIS. Safety Availability. 27

Figura 2.7.- Metodología Cualitativa para la Determinación del Nivel de Integridad de Seguridad. 34

Figura 2.8.- Matriz de Capas de Seguridad para la Determinación del SIL. 35

Figura 2.9.- Método Cualitativo de Gráfica de Riesgo para Determinación del SIL. 41

Figura 2.10.- Reducción de Riesgo: Conceptos Generales. 46

Figura 2.11.- Capas Múltiples de Protección. 48

Figura 2.12.- Componentes de un SIS. 50

Figura 2.13.- Modelo Simple del Sistema Controlador Programable (PES). 51

Figura 2.14.- Curva de Frequencia/Consecuencia 57

Figura 2.15.- Distribución de Data. 59

Figura 2.16. - Cambio de la Frequencia sin cambiar la Consecuencia 60

Figura 2.17.- Arquitectura 1001. 64

Figura 2.18.- Arquitectura 1001, Árbol de Falla PFD. 65

Figura 2.19.- Arquitectura 1001, Árbol de Falla PFS. 65

Figura 2.20.- Arquitectura 1002. 66

Figura 2.21.- Arquitectura 1002, Árbol de Falla PFD. 67

Figura 2.22.- Arquitectura 1002, Árbol de Falla PFS. 67

Figura 2.23.- Arquitectura 2002. 68

Figura 2.24.- Arquitectura 2002, Árbol de Falla PFD. 69

Figura 2.25.- Arquitectura 2002, Árbol de Falla PFS. 69

Pág.

Figura 2.26.- Arquitectura 1001D. 70
Figura 2.27.- Arquitectura 1001D, Árbol de Falla PFD. 71
Figura 2.28.- Arquitectura 1001D, Árbol de Falla PFS. 71
Figura 2.29.- Arquitectura 2003. 72
Figura 2.30.- Arquitectura 2003, Árbol de Falla PFD. 73
Figura 2.31.- Arquitectura 2003, Árbol de Falla PFS. 74
Figura 2.32.- Arquitectura 2002D. 75
Figura 2.33.- Arquitectura 2002D, Árbol de Falla PFD. 76
Figura 2.34.- Arquitectura 2002D, Árbol de Falla PFS. 76
Figura 2.35.- Arquitectura 1002D. 77
Figura 2.36.- Arquitectura 1002D, Árbol de Falla PFD. 78
Figura 2.37.- Arquitectura 1002D, Árbol de Falla PFS. 78

Capítulo 3.

Figura 3.1.- Metodología para la Determinación del SIL de los SIS. 83

Capítulo 4.

Figura 4.1.- Metodología para la Determinación del SIL de los SIS 85
Figura 4.2.- Hoja de Cálculo de "Sensores". 94
Figura 4.3.- Hoja de Cálculo de "Logic Solver". 95
Figura 4.4.- Hoja de cálculo de "Válvulas". 96
Figura 4.5.- Hoja de Cálculo de "Resumen". 97
Figura 4.6.- Hoja de Cálculo de "Comparación". 98

Capítulo 5.

Figura 5.1.- Diagrama de Bloques "Estación de Producción". 104
Figura 5.2.- Diagrama de Bloques "Planta Compresora ". 105
Figura 5.3.- Lazo Critico: Bajo Bajo Nivel de Crudo en el Separador Gas Crudo. 123
Figura 5.4.- Lazo Critico: Bajo Bajo Nivel de Crudo en el Separador Gas Crudo. 124
Figura 5.5.- Lazo Critico: Alto Alto Nivel de Crudo en el Tanque de Estabilización. 125

Pág.

Figura 5.6.- Lazo Critico: Baja Presión de Succión Bombas de Crudo Sucio P-702A/B. 126

Figura 5.7.- Instrumentación Lazo Critico: Bajo Bajo Nivel de Crudo en el Separador Gas- Crudo V-02-03. 129

Figura 5.8.- Alto Alto Nivel de Crudo en el Tanque de Estabilización de Crudo T-0701A y Baja Presión de Succión Bombas de Crudo Sucio P-0702 A/B. 130

ÍNDICE DE TABLAS

Pág.

Capítulo 2.

Tabla 2.1.- Modelo del documento final HAZOP. 13

Tabla 2.2.- Criterio PDVSA Riego Individual. 15

Tabla 2.3.- Niveles de Integridad de Seguridad (SIL). 32

Tabla 2.4.- Probabilidad de Ocurrencia del Evento Peligroso por el Método de Matriz de Capas de Seguridad. 37

Tabla 2.5.- Severidad de Consecuencias. 37

Tabla 2.6.- Extensión de los Daños. 40

Tabla 2.7.- Frecuencia de Exposición al Peligro. 40

Tabla 2.8.- Posibilidad de Evitar el Peligro. 40

Tabla 2.9.- Probabilidad de Ocurrencia del Evento Peligroso por el Método General de Gráfica de riesgo. 41

Tabla 2.10.- Niveles de Integridad de Seguridad (SIL). 44

Tabla 2.11.- Meta de Nivel de Riesgo Tolerable – Mínimo. 44

Tabla 2.12.- Ejemplo de Distribución de Modos de Fallas. 62

Tabla 2.13.- Cálculo de los $PFD_{Peligroso}$ de los diferentes elementos utilizados para el cálculo del $PFD_{Peligroso}$ del Proceso y BPCS. 63

Capítulo 4.

Tabla 4.1.- Data típica para los Sensores. 91

Tabla 4.2.- Data típica para el Controlador CPU (Logic Solver). 92

Tabla 4.3.- Data típica para los Elementos Finales de Control (Válvulas). 93

Capítulo 5.

Tabla 5.1.- Sumario Parcial de Valorización Preliminar de Peligros para el Desarrollo de Estrategias de Seguridad. 107

Tabla 5.2.- Evaluación de Riesgo del Sistema / Documentación del SIL. 127

Tabla 5.3.- Entradas y Salidas Lazos Críticos – Configuración Básica. 131

Pág.

Tabla 5.4.- Datos de Entrada Sensores. 132
Tabla 5.5.- Resultados Sensores. 133
Tabla 5.6.- Datos de Entrada Válvulas. 133
Tabla 5.7.- Resultados Válvulas. 134
Tabla 5.8.- Datos de Entrada CPU. 134
Tabla 5.9.- Resultados CPU. 135
Tabla 5.10.- Resumen Resultados Sistema Instrumentado de Seguridad. 135
Tabla 5.11.- Arquitectura 1oo1 (Sensores), 1oo1 (CPU), y 1oo1 (Válvulas). 135
Tabla 5.12.- Datos de Entrada Sensores. 136
Tabla 5.13.- Resultados Sensores. 137
Tabla 5.14.- Datos de Entrada Válvulas. 137
Tabla 5.15.- Resultados Válvulas Configuración 1oo2. 138
Tabla 5.16.- Resumen Resultados SIS. 138
Tabla 5.17.- Resumen de Arquitecturas. 139

INTRODUCCIÓN

Este trabajo presenta el "Desarrollo de una Metodología para el Diseño de Sistemas de Seguridad y Protección de la Estación de Producción del Centro Operativo El Carito" en un compendio o resumen de las Normas Nacionales e Internacionales relacionadas con Sistemas de Seguridad Industrial.

Esta metodología ayuda a los profesionales del sector industrial encargados del diseño de sistema de seguridad y de protección a obtener resultados de una arquitectura al mejor costo-valor, en un tiempo menor al que actualmente se utiliza en el diseño de estos sistemas.

En el capítulo correspondiente al marco teórico se pueden encontrar una serie de definiciones, técnicas y procedimientos que sirven de base para el desarrollo de la metodología.

Para la implantación de la metodología y con miras de facilitar el trabajo de los profesionales o técnicos, se desarrolló un programa que muestra todas las diferentes combinaciones comerciales de arquitectura posible de Sistemas Instrumentados de Seguridad, que cumplan el Nivel de Integridad deseado.

Capítulo 1.

PLANTEAMIENTO DEL PROBLEMA

Desde su creación en 1976, Petróleos de Venezuela, S.A. (PDVSA) se ha convertido en una de las corporaciones energéticas más importantes del mundo. PDVSA es la casa matriz de la corporación, propiedad de la República de Venezuela, que se encarga del desarrollo de la industria petrolera, petroquímica y carbonífera, y de planificar, coordinar, supervisar y controlar las actividades operativas de sus divisiones, tanto en Venezuela como en el exterior.

PDVSA lleva adelante actividades en materia de exploración y producción para el desarrollo de petróleo y gas, bitumen y crudo pesado de la Faja del Orinoco, producción y manufactura de Orimulsión, así como explotación de yacimientos de carbón. Ocupa una destacada posición entre los refinadores mundiales y su red de manufactura y mercadeo abarca Venezuela, el Caribe, Estados Unidos y Europa. Además, realiza actividades en las áreas de petroquímica, investigación y desarrollo tecnológico, educación y adiestramiento en sectores vinculados con la industria energética.

1.1. TRANSFORMACIÓN Y ÉXITO.

Luego de dos décadas de actividades, PDVSA se ha constituido en una corporación de primera línea en el ámbito nacional e internacional. Ocupa una posición relevante entre las empresas del mundo, por sus niveles de producción, reservas, capacidad instalada de refinación y ventas.

PDVSA ha asumido oportunamente el reto de mantenerse competitiva y rentable frente a los nuevos tiempos. Para ello, ha puesto en marcha la transformación de su estructura corporativa, con el propósito fundamental de redefinir el papel de la casa matriz y consolidar la estructura operativa.

En este sentido, a finales de 1997, la corporación energética venezolana creó la empresa de PDVSA Petróleo y Gas, la cual está constituida por tres grandes divisiones, dedicadas a las actividades medulares del negocio: PDVSA Exploración y Producción, PDVSA Manufactura y Mercadeo, y PDVSA Servicios. Cada una de estas divisiones a su vez está integrada por diversas empresas y unidades de negocio, ubicadas tanto en Venezuela como en el exterior.

El sector petroquímico es desarrollado por Pequiven y sus empresas mixtas. Asimismo, existen otras empresas filiales de PDVSA: CIED, Intevep, Palmaven, SOFIP, las cuales tienen como función principal: adiestramiento y capacitación, investigación y desarrollo, apoyo al sector agroindustrial venezolano, y promoción de nuevas modalidades de inversión y ahorro dentro del proceso de apertura petrolera, respectivamente.

Las actividades de exploración están dirigidas hacia la búsqueda de nuevas reservas de crudo liviano y mediano para sustentar los planes de crecimiento de la capacidad de producción, así como para profundizar el conocimiento de áreas prospectivas. Las reservas probadas de crudo se ubican en 72 millardos de barriles y capacidad de crudo y condensado en 3,4 millones de barriles diarios. Las reservas de gas natural alcanzan los 143 billones de pies cúbicos, lo cual ratifica la posición de

Venezuela como líder en reservas gasíferas en Latinoamérica y como quinta en el ámbito internacional.

PDVSA posee uno de los planteles refinadores más grandes del mundo con una capacidad total instalada de 3,4 millones de barriles diarios, incluyendo las refinerías que posee en Venezuela, el Caribe, Estados Unidos y Europa. En refinación, PDVSA ha culminado importantes proyectos diseñados con el fin de garantizar la competitividad futura de la corporación en los mercados finales especialmente en lo referente a exigencias ambientales en calidad de productos.

La corporación realiza actividades de comercio y suministro nacional e internacional a través de empresas propias o asociadas en el exterior. Las actividades de comercialización en el mercado nacional son llevadas a cabo a través de la marca PDV, con el mercado de productos como gasolinas de motor y aviación, diesel automotor, combustible Jet A-1, fuel oil para plantas eléctricas e industriales, lubricantes y grasas, aditivo para motores de inyección, liga de frenos, asfalto para pavimentación, bunker para los barcos mercantes y petroleros, entre muchos otros; en una amplia red de distribuidores y puntos de venta.

En el mercado internacional a través de su filial CITGO Petroleum Corporation, PDVSA realiza el mercadeo y transporte de gasolina, "Jet turbine fuel", diesel, lubricantes, aceites; ceras refinadas, petroquímicos, asfaltos y otros productos industriales derivados del petróleo. PDVSA cuenta con su propia flota de tanqueros para el transporte marítimo nacional e internacional. Posee oficinas de mercadeo e inteligencia en varias ciudades de los Estados Unidos y Europa. Para mantenerse al día en materia tecnológica, la corporación cuenta con la filial Intevep, centro de

investigación que presta servicio a toda la corporación. La filial CIED, Centro Internacional de Educación y Desarrollo está dedicado a la formación del recurso humano del sector petrolero nacional e internacional.

El desarrollo de la industria petrolera y su acelerado avance tanto en tamaño y nuevas tecnologías como se expresó anteriormente, ha impulsado la implantación de nuevos sistemas que permiten optimizar los procesos que intervienen en sus actividades mediante la automatización de los mismos. Actualmente la Industria ha optado por la premisa de minimizar los riesgos, tomando en cuenta por orden de prioridades la protección contra la ocurrencia de eventos que pudiesen causar daños al personal, a los equipos, al ambiente y pérdida de producción.

La expansión de la industria petrolera nacional y el hecho de poseer procesos más complejos han impactado directamente en el crecimiento de las plantas y esto a su vez ha incrementado el nivel de riesgo en las mismas, lo que implica un aumento elevado de peligros potenciales que pueden conducir a un evento no deseado.

Por lo expuesto anteriormente y el hecho de que en la actualidad las regulaciones ambientales son extremadamente exigentes, la industria petrolera ha tratado de elaborar una serie de metodologías en busca de la seguridad de los procesos y así reducir los riesgos al valor mínimo permitido.

La seguridad de los procesos es hoy en día un tema que ha alcanzado una gran relevancia y por tal razón se ha considerado importante trabajar este aspecto dentro del contexto de los Sistemas Instrumentados de Seguridad y Protección, y su aplicación en el diseño de plantas industriales debe ser parte elemental del diseño del proceso y de los equipos. Las Plantas de Proceso requieren de la protección con el fin de enfrentar los

eventos indeseables que pudiesen causar daños al personal, equipos, al ambiente y pérdida de producción.

Actualmente el diseño de los Sistemas Instrumentados de Seguridad y Protección (Safety Instrumented System: SIS) no se basan en estimaciones cuantitativas sobre cuales deberían ser los Niveles de Integridad de Seguridad (Safety Integrity Level: SIL) y de confiabilidad mínimos necesarios que cumplan con los requerimientos que cubran los niveles de riesgo aceptable.

El aspecto de la seguridad debe necesariamente comenzar junto con la decisión de iniciar un proyecto y continúa a través de todo el diseño, implantación y operación. Los aspectos de seguridad inherentes a las instalaciones de la industria deben ser abordados como una parte integral del trabajo iniciado con las evaluaciones de factibilidad y conceptualización de los procesos, continuando a través de las diferentes fases del diseño, construcción y arranque, manteniéndose de igual forma durante toda la vida operativa de las instalaciones.

1.2. JUSTIFICACIÓN.

Así como los procesos industriales se han incrementado en tamaño y en complejidad, los Sistemas Instrumentados de Seguridad y Protección (SIS) también han incrementado su sofisticación y efectividad, siendo que la razón primordial de estos sistemas es prevenir los riesgos y proteger al personal y equipos. Un SIS diseñado deficientemente pudiera suministrar menos protección de la necesaria ó causar innecesarias paradas de planta causando bajas en la producción y por ende pérdidas financieras, mientras que un sistema instrumentado de seguridad bien diseñado,

suministrará siempre una supervisión continua de las operaciones y de paradas del proceso solo en caso necesario, para garantizar la seguridad al personal y al equipo permitiendo el máximo en la producción.

La falta de información y de una metodología que soporten los diseños de sistemas de protección bajo la filosofía de sistemas seguros y confiables hace necesario la realización de este trabajo, en el cual se establece una metodología que permite determinar a través de métodos cuantitativos (Análisis de Arbol de Fallas y Cálculos de Confiabilidad) cual debe ser la configuración óptima de la instrumentación de los sistemas instrumentados de seguridad requerido por el proceso, de allí la importancia de esta tesis de pretender suministrar una respuesta a tal carencia.

El Proyecto de "Desarrollo de una Metodología para el Diseño de Sistemas de Seguridad y Protección para La Estación de Producción de Carito (COC)" es de vital importancia para la industria petrolera y se justifica por lo siguiente:

La no disposición actual de una metodología para el cálculo cuantitativo del riesgo en una planta en particular.

El Sistema Instrumentado de Seguridad es más económico por la selección acertada de los Niveles de Integridad de Seguridad (SIL).

Ser más confiable, gracias a la metodología para la evaluación y diseño de un mejor Sistema Instrumentado de Seguridad que minimice las probabilidades de fallas en demanda y paradas innecesarias.

La implementación de tal sistema se traduciría directamente en beneficios a la industria obteniendo finalmente un SIS con bajos niveles de Riesgos y mayores factores de disponibilidad y confiabilidad por la reducción de fallas peligrosas y falsas paradas.

1.3. ALCANCE.

El alcance de este Trabajo de Grado, está orientado al desarrollo de una metodología, que permita de una manera metódica, cualitativa y cuantitativa, siguiendo el Ciclo de Vida de Seguridad y empleando las técnicas más avanzadas para la justificación de este tipo de sistemas en los diferentes procesos, adaptando dichas técnicas a las exigencias de nuestra industria petrolera para el diseño de los Sistemas Instrumentados de Seguridad (SIS), y de esta forma evitar el sobre y subdimencionamiento de los sistemas.

La norma utilizada en este trabajo de grado y por PDVSA para el diseño de los SIS es la Norma de PDVSA K-336 de Sistemas Instrumentados de Seguridad recientemente revisada y aprobada en diciembre de 1998 y que en la misma esta asume como su norma base la ANSI/ISA S84.01- 1996. Esta norma define la aplicación del Ciclo de Vida de Seguridad (Safety Life Cycle) el cual permitirá determinar los requerimientos mínimos de diseño que debe satisfacer el sistema de seguridad a implementar para garantizar la reducción de riesgo necesaria para un peligro especifico del proceso.

Este trabajo no contempla la implementación de los resultados obtenidos.

1.4. LIMITACIONES.

Actualmente la Industria Petrolera Nacional no cuenta con una base de datos estadístico propia de fallas de equipos, indispensable para efectuar las evaluaciones de frecuencias de accidentes. Por lo tanto se hace necesario el uso de una sola base de datos de rata de falla genérica (que incluye muchos tipos de falla) que nos dará resultados de frecuencias de falla con una misma constante de error. En este trabajo se utilizaran las

base de datos: GUIDELINES FOR PROCESS EQUIPMENT RELIABILITY DATA *of Center for Chemical Process Safety of American Institute of Chemical Engineer* y OFFSHORE REALIBILITY DATA HANDBOOK (OREDA), 2nd Edition, que son las utilizadas por PDVSA en estos cálculos.

1.5. OBJETIVOS.

1.5.1. Objetivo General.

Desarrollo de una metodología para el diseño del Sistema Instrumentado de Seguridad (SIS) que permita alcanzar la disponibilidad requerida para el nivel de integridad de seguridad (SIL) calculado para La Estación de Producción de Carito (COC), Dtto. Punta de Mata, Estado Monagas.

1.5.2. Objetivos Específicos.

- Desarrollo y revisión de los fundamentos teóricos que rigen requerimientos de seguridad: Riesgo: Concepto, Alcance, Definición. Capas de Protección Independientes (IPL) y de Mitigación.
- Metodología de Análisis de Riesgo de Proceso.
- Metodología de Análisis de Riesgo Cualitativas.
- Técnicas basadas en Árbol.
- Estudio del funcionamiento de La Estación de Producción de Carito (COC), Diagrama de Instrumentación y Control (D.T.I.), Riesgos y Modos de Fallas.
- Consideraciones de Diseño para la selección de la arquitectura del sistema instrumentado de seguridad (safety systems hardware) de acuerdo al nivel de

integridad de seguridad (SIL) requerido para La Estación de Producción de Carito (COC).

Capítulo 2.

MARCO TEÓRICO

En el presente capítulo se establecerá el marco teórico relacionado a los Sistemas Instrumentados de Seguridad.

2.1. PELIGRO[1]

Los peligros son las fuentes físicas o químicas de un sistema, planta o proceso que tienen el potencial para causar daños a las personas, a la propiedad y/o al medio ambiente. Se debe entender como la combinación de una substancia peligrosa y un ambiente operacional, tal que, la ocurrencia de ciertos eventos no deseados, puedan resultar en un accidente.

2.1.1. Identificación de Peligros.

La identificación de los peligros inherentes al proceso o planta, constituye el primer paso para un análisis cuantitativo de riesgo. En esta etapa se evalúan entre otros los materiales, inventarios y las condiciones operacionales del proceso que pudiesen ocasionar eventos indeseables. La identificación de peligros es un paso crítico en el Análisis Cuantitativo de Riesgo, por cuanto un peligro omitido, es un peligro no analizado. Los métodos que aplica la Industria Petrolera Nacional en la identificación de peligros son: Análisis Preliminar de Peligros (APP) y Estudios de Peligros y Operabilidad (HAZOP).

A continuación se presenta una breve descripción de los métodos utilizados

mayormente por la Industria Petrolera Nacional.

2.1.1.1. Análisis de Riesgo Preliminar (PHA).

Esta técnica cualitativa consiste en el análisis disciplinario de las consecuencias del evento que podrían transformar un peligro potencial en accidente. En esta técnica, los posibles eventos indeseables son identificados primeros y luego analizados separadamente. Para cada uno de los peligros o eventos indeseables, son formuladas medidas preventivas o posibles mejoras. El resultado de esta técnica proporciona una base para determinar cuales categorías de peligro deberían ser estudiadas más detenidamente y cuales métodos de análisis son los más adecuados. Con la ayuda de un diagrama o matriz frecuencia/consecuencia, los peligros identificados pueden ser clasificados de acuerdo al riesgo y permitir medidas prioritarias para prevenir accidentes.

2.1.1.2. Estudio de Operabilidad y Peligro (HAZOP).

La técnica HAZOP fue desarrollada a comienzos de 1970 por Industrias Químicas Imperial LTD. El HAZOP es un método de análisis que consiste en un examen crítico y sistemático del diseño de una instalación industrial, sistema, etc., para evaluar e identificar los peligros potenciales y problemas operacionales así como consecuencias en la instalación examinada.

En el estudio HAZOP se examina cada subsección del sistema con respecto a las condiciones de proceso (por ejemplo: presión, temperatura, flujo). A cada condición de proceso se aplica un juego de palabras guía para mostrar las posibles desviaciones de dichas variables (por ejemplo: más, menos, no).

Para cada desviación de la condición del proceso se establecen las causas o eventos iniciadores que conlleven a dicha desviación y las posibles consecuencias, indicando daños a personas, pérdidas materiales e impacto ambiental. Para cada situación peligrosa se enumeran las acciones de protección existentes que entren en funcionamiento para normalizar la situación de desviación que se presenta.

Al final del análisis de cada subsección del sistema, se hacen anotaciones y recomendaciones de acuerdo a la necesidad o no de la implantación de sistemas de protección adicionales, en función del riesgo y de los sistemas de seguridad existentes. El resultado y documento final del HAZOP se presenta en forma tabular, tal como se muestra en la tabla 2.1.

Palabra Guía	Desviación	Causas	Consecuencias	Protecciones	Acciones
Tipo de desviación que ocurre.	Condición del proceso que sufre la desviación.	Eventos iniciadores de la desviación.	Efecto de la desviación sobre propiedades, personas y ambiente.	Acciones de protección contra la desviación.	Recomendaciones en función del riesgo actual del proceso.

Tabla 2.1.- Modelo del documento final HAZOP.

2.2. RIESGO[1].

Riesgo es definido como la combinación de la frecuencia y la consecuencia de un evento peligroso especifico. El concepto de riesgo esta asociado siempre a dos elementos donde:

Frecuencia = Evento / Unidad de Tiempo.

Magnitud = Consecuencia / Evento.

La Magnitud del Evento esta relacionada a:

- Personas, fatalidades, heridos, tanto de la planta como de la comunidad, incluye la responsabilidad moral por su protección y del medio ambiente.
- Propiedad, incluyendo perdidas financieras debido al evento. Estos incluye por lo menos:
  - Costo de reemplazo de la planta.
  - Costo de defensa penal.
  - Costo de perdida en la producción.
  - Costo de los materiales de proceso perdidos.

Habiendo identificado los peligros, es necesario cuantificar el nivel de riesgo implícito a objeto de determinar el alcance de las medidas de control. La cuantificación de riesgo está basada tanto en la estimación de la frecuencia de ocurrencia de accidentes como en el cálculo de sus consecuencias.

2.2.1. Cuantificación del Riesgo.

Las medidas mas comunes de cuantificación de 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.

2.2.1.1. Riesgo Individual.

Riesgo a que está sometida una persona en la proximidad de un peligro. Esto incluye la naturaleza del daño al individuo, la probabilidad de la lesión y el periodo de tiempo en el cual la lesión puede ocurrir.

En PDVSA el riesgo individual posee una tolerancia de acuerdo a una comparación individual de riesgo anual con los riesgos asociados a ciertas actividades conocidas y de donde se puede determinar que estos riesgos pueden ser del tipo voluntario e involuntario. Los trabajadores pueden ser clasificados entes involuntarios de riesgo y las personas aledañas a las plantas o industrias también son clasificadas como entes involuntarios de riesgo.

A continuación se puede apreciar la tabla 2.2 del criterio de PDVSA para la tolerancia del riesgo individual según el Manual de Ingeniería de Riesgos PDVSA.

CRITERIO PDVSA PARA TOLERANCIA DE RIESGO INDIVIDUAL	
FRECUENCIA	**TOLERABILIDAD**
$F > 10^{-3}$/año	**Intolerable: El riesgo debe ser reducido a cualquier costo.**
10^{-6} /año $< F <= 10^{-3}$/año	**Deseable: Reducción adicional del riesgo basado en análisis costo beneficio. Representa la región de riesgo reducible.**
$F <= 10^{-6}$ /año	**Tolerable o mínimo: Reducción del riesgo si los recursos lo permiten. Aún aplica concepto de costo beneficio.**

Tabla 2.2.- Criterio PDVSA Riego Individual.

2.2.1.2. Riesgo Social.

Medida del riesgo a un grupo de personas, frecuentemente expresado en el término de la distribución de frecuencia y las fatalidades de accidentes múltiples.

El criterio de tolerancia del riesgo social formulado a continuación considera la experiencia de varios años de operación de PDVSA y sus filiales, acumulando tanto las estadísticas de accidentes con consecuencias de lesiones y fatalidades a personal propio y terceros, como las consecuencias de daños ambientales, perdidas materiales y de producción. Tales consecuencias han sido categorizadas de acuerdo a su severidad en los rangos de severas, mayores y catastróficas, como se especifica en la figura 2.1. Asimismo, un análisis de las frecuencias de tales accidentes, considerando el total de instalaciones de PDVSA y sus filiales ha permitido establecer los ordenes de magnitud o rangos de frecuencia típicas para cada una de las categorías de accidentes antes indicadas. En base a este análisis PDVSA estableció una curva de tolerancia del riesgo social como se muestra en la figura 2.1, la cual define los rangos de accidentes en diferentes categorías que pueden considerarse como Intolerables, Mínimos (Tolerables) y la Zona intermedia en la cual la reducción del riesgo es deseable.

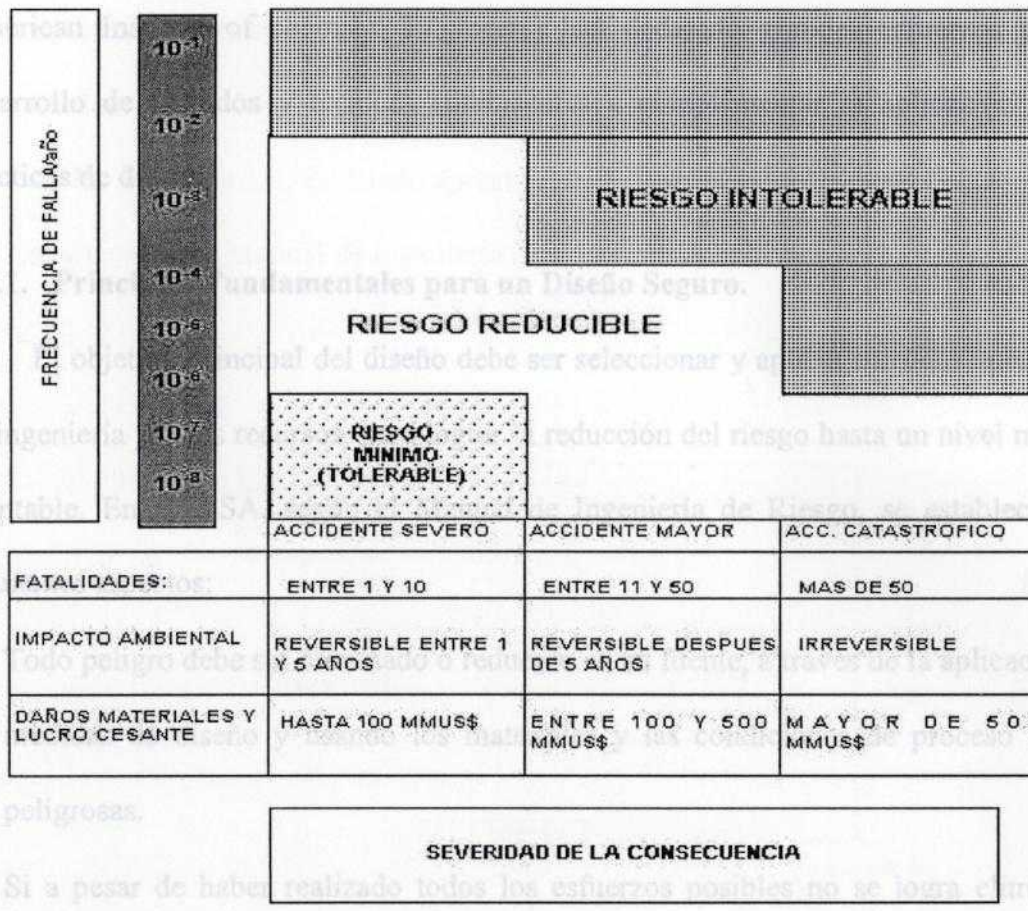


Figura 2.1.- Criterio PDVSA de Tolerancia del Riesgo Social.

2.3. FILOSOFÍA DE DISEÑO SEGURO[1].

Los códigos normalmente utilizados en el diseño de instalaciones no contemplan todos los posibles eventos y escenarios que generan accidentes, por lo tanto la sola aplicación de un código o conjunto de códigos no garantiza la integridad y seguridad de una instalación. Las experiencias a nivel nacional e internacional tales como Tacoa (Venezuela), Pasadena (USA), Chernobyl, etc., han demostrado en forma evidente la anterior afirmación; razón por la cual algunas organizaciones internacionales (ISA "Instrument Society of America", IEC "International Electrotechnical Commission" y

American Institute of chemical Engineers) han dedicado grandes esfuerzos para el desarrollo de métodos y técnicas conducentes a complementar la aplicación de las prácticas de diseño.

2.3.1. Principios Fundamentales para un Diseño Seguro.

El objetivo principal del diseño debe ser seleccionar y aplicar medidas apropiadas de ingeniería y otros recursos, para lograr la reducción del riesgo hasta un nivel mínimo aceptable. En PDVSA, según el Manual de Ingeniería de Riesgo, se establecen los siguientes aspectos:

- Todo peligro debe ser eliminado o reducido en su fuente, a través de la aplicación de medidas de diseño y usando los materiales y las condiciones de proceso menos peligrosas.
- Si a pesar de haber realizado todos los esfuerzos posibles no se logra eliminar o reducir el peligro en su fuente hasta el nivel de riesgo mínimo, será necesario utilizar sistemas de protección. Estos sistemas deben ser diseñados y construidos cumpliendo con lo establecido en la normativa de Ingeniería de Riesgos de PDVSA, aplicando en primer lugar sistemas pasivos y de ser necesario sistemas activos. Los *Sistemas Pasivos* eliminan o reducen el peligro a través del diseño de equipos y procesos que disminuyen la frecuencia o consecuencia del riesgo, sin la necesidad de que un sistema funcione activamente, ejemplo: separación entre equipos e instalaciones, diques de contención, revestimiento contra incendios, etc. Por otro lado, los *Sistemas Activos* requieren controles instrumentados, enclavamientos, Sistemas Instrumentados de Seguridad (SIS), sistemas de agua contra incendio, etc.,

para detectar y tomar acción correctiva, en caso de desviaciones peligrosas de los procesos.

En la figura 2.2, se puede apreciar un diagrama para el diseño de un proceso seguro según el Manual de Ingeniería de Riesgo **PDVSA IR-S-01**.

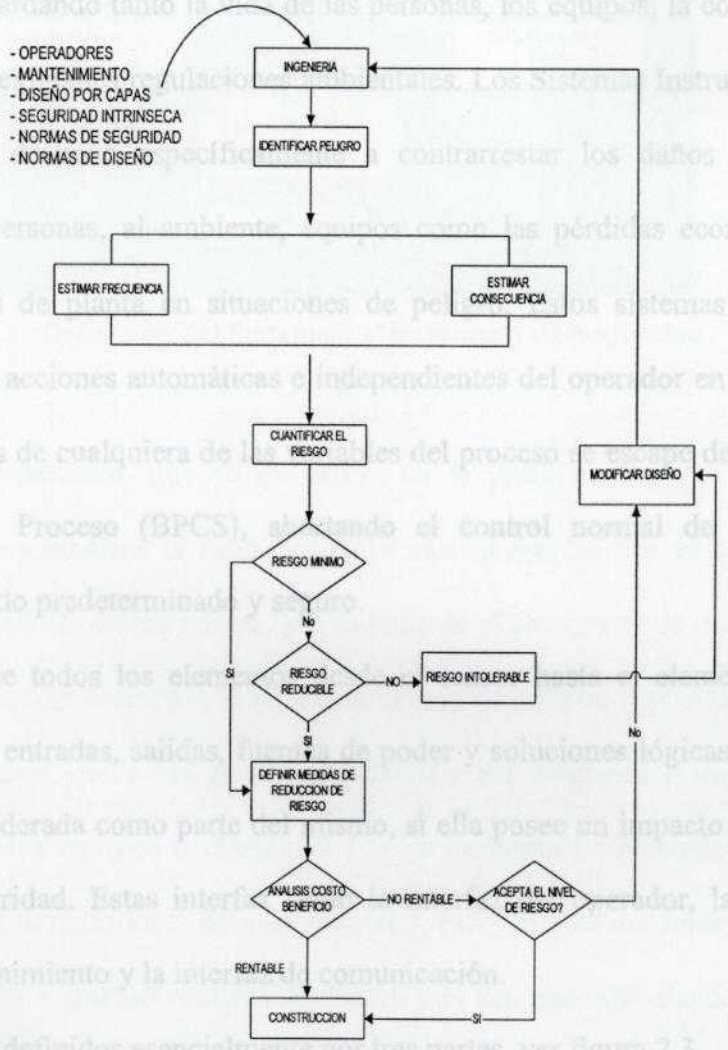


Figura 2.2.- Proceso de un Diseño de Seguridad.

2.4. SISTEMA INSTRUMENTADO DE SEGURIDAD (SIS)[2].

El Sistema Instrumentado de Seguridad (SIS, "Safety Instrumented System") proporciona los mecanismos necesarios para llevar el proceso a 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 SIS, se destinan específicamente a contrarrestar los daños que puedan ocasionarse a las personas, al ambiente, equipos como las pérdidas económicas que resulten de paradas de planta en situaciones de peligro. Estos sistemas están en la capacidad de tomar acciones automáticas e independientes del operador en los casos de que las desviaciones de cualquiera de las variables del proceso se escape del Sistema de Control Básico de 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 interfaz serán la interfaz del operador, la interfaz de ingeniería de mantenimiento y la interfaz de comunicación.

Los SIS están definidos esencialmente por tres partes, ver figura 2.3.

Las entradas al sistema, que se encuentran en la parte izquierda del diagrama y 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 censando, tales como flujo, presión y temperatura.

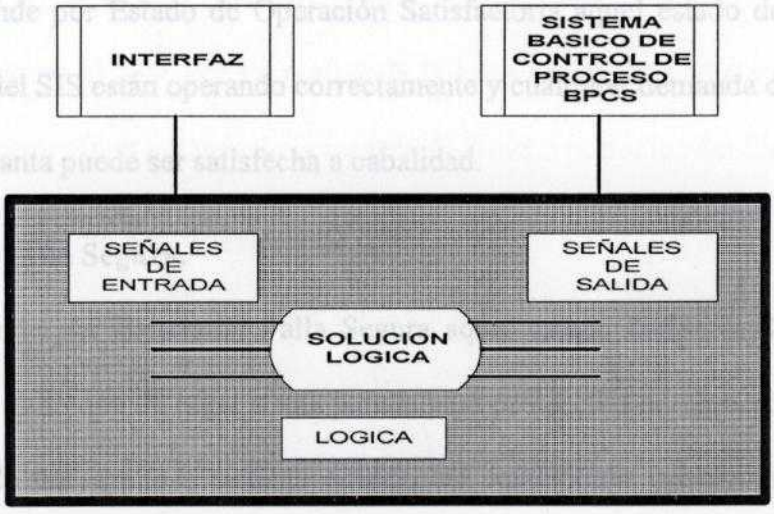


Figura 2.3.- Definición del Sistema Instrumentado de Seguridad.

La lógica de enclavamiento, que se encuentra en la parte central del diagrama y 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,

Las salidas del sistema, que están en la parte derecha del diagrama y 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.

2.4.1. Estados del SIS.

El Sistema Instrumentado de Seguridad (SIS, "Safety Instrumented System")

puede ubicarse en cada uno de los siguientes estados descritos a continuación:

- **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.**

Se entiende por Estado de Falla Segura aquel estado donde el SIS ha actuado generando 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 bien es cierto que puede tener algún impacto en seguridad dado que un alto porcentaje de accidentes están ubicados en los momentos de paradas y arranques.

- **Estado de Falla Peligrosa.**

Se entiende por Estado de Falla Peligrosa 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", "revealed" o "overt") pero en el cual el autodiagnóstico del sistema ha logrado descubrir el elemento fallado en el SIS reportándolo oportunamente al operador/mantenedor.

- **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/prueba periódica del Sistema.

- **Estado de Falla de Alto Riesgo (Hazardous).**

Se entiende por Estado de Falla de Alto Riego aquel estado donde el SIS está fallado para actuar ante una demanda de la Planta, y la demanda de la Planta se ha hecho una realidad quedando 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 este estado.

2.4.2. Términos Estadísticos.

Para evaluar apropiadamente un sistema inherentemente seguro (desenergizar para disparar) deben revisarse los modos de falla del sistema y para el presente trabajo, se asumen solo dos modos de falla: en demanda ó en falla segura, ver figura 2.4.

- **Probabilidad de Falla en Demanda (PFD).**

Es la probabilidad de que el sistema falle con sus salidas energizadas. Este término se refiere a que el SIS ha fallado y este no responderá a una demanda del proceso, condición de falla peligrosa (D: Dangerous).

- **Probabilidad de Falla Segura (PFS).**

Es la probabilidad de que el sistema falle con sus salidas desenergizadas. Este

término se refiere a que el sistema ha actuado (ha desenergizado sus salidas) sin existir una demanda del proceso, condición de falla segura (S: Safe).

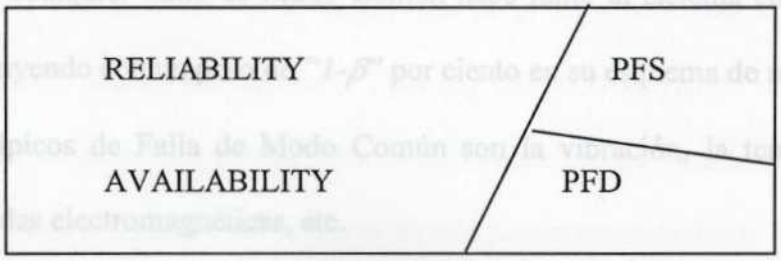


Figura 2.4.- Modos de Fallas.

2.5. CARACTERÍSTICAS DE LOS SIS[2].

Los Sistemas Instrumentados de Seguridad presentan características propias de su capacidad de autodiagnosticar las fallas y de robustez frente a los factores de falla común.

- **Factor de Diagnóstico o Cobertura "C" ("Coverage Factor"):**

Es una medida de la capacidad de diagnóstico del SIS. Está determinada por la fracción de las fallas que pueden ser detectadas por su propio sistema de diagnóstico en línea.

- **Falla de Modo Común "β" ("Common Mode Failure"):**

Falla de Modo Común es una falla simple que es capaz de producir la falla completa de un sistema redundante. La Falla de Modo Común se expresa a través de "β", la cual indica el porcentaje o fracción del total de fallas (del "failure rate") que es debido a Modo Común.

Desde el punto de vista práctico un sistema sujeto a Falla de Modo 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 Modo 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 Modo 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%.

2.5.1. Índices de Desempeño.

El desempeño o comportamiento de los Sistemas Instrumentados de Seguridad puede ser calificado de acuerdo a índices preestablecidos tales como "Reliability" y "Availability".

- **Reliability".**

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

Matemáticamente *R* tiene una definición precisa "la probabilidad que un dispositivo opere satisfactoriamente en el intervalo de tiempo de cero a *t*".

- **"Unreliability".**

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

La relación entre Reliability y Unreliability es:

$$F(t) = 1 - R(t) \qquad (2.01)$$

- **"Availability".**

En términos matemáticos "Availability" es la probabilidad que un dispositivo tenga una operación exitosa en el tiempo "*t*". No hay 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, ver figura 2.5.

"Availability" 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 Availability, *A(t)*, es igual a Reliability, *R(t)*. En sistemas reparables *A(t)* es mayor o igual que *R(t)*.

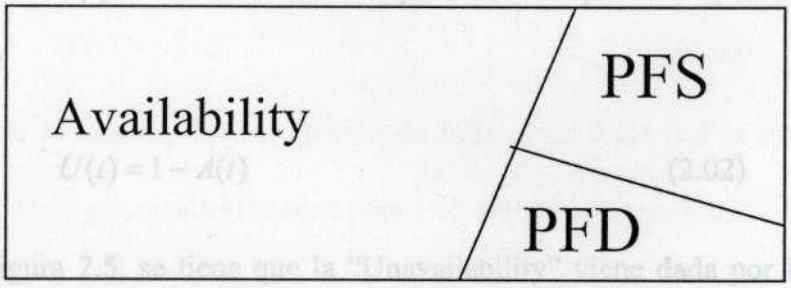


Figura 2.5.- Diagrama de Venn del SIS. Availability.

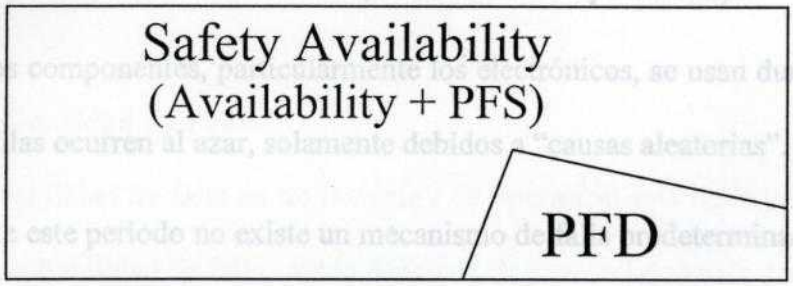


Figura 2.6.- Diagrama de Venn del SIS. Safety Availability.

De la figura 2.6, se observa que la Disponibilidad Segura o "Safety Availability", es la unión de la Probabilidad de Falla Segura más la Probabilidad de que el SIS opere libre de toda falla ("Availability").

- **"Unavailability".**

"Unavailability", *U(t)*, es una medición de falla, es usada principalmente para sistemas reparables, y es definida como la probabilidad que un dispositivo esté fallado en el tiempo *t*.

$$U(t) = 1 - A(t) \qquad (2.02)$$

De la figura 2.5, se tiene que la "Unavailability" viene dada por la suma de las áreas *PFS y PFD (PFS + PFD)*. También se tiene de la figura 2.6, que la "Unavailability Dangerous" viene dada por el área correspondiente a *PFD*.

Obsérvese que "Availability", *PFD* y *PFS* son mutuamente excluyentes dado que no tiene elementos de intersección.

2.5.2. Función Distribución de Falla (Distribución Exponencial).

Muchos componentes, particularmente los electrónicos, se usan durante el período en que las fallas ocurren al azar, solamente debidos a "causas aleatorias".

Durante este período no existe un mecanismo de falla predeterminado responsable. Las fallas consecuencia de la "mortalidad infantil" han sido eliminadas mediante acciones correctivas ligadas al diseño, los procedimientos operativos o los métodos de inspección y prueba en fábrica. Además, considerándose, no haber llegado al período de desgaste o degradación de la actuación hasta salirse de los límites de tolerancia, se observa una tasa de falla que tiende a un valor relativamente constante.

La exponencial negativa es la distribución que puede caracterizar la tasa de falla constante.

Denotaremos *por f(t)* la densidad de falla exponencial.

$$f(t) = \lambda \cdot e^{-\lambda \cdot t} \qquad (2.03)$$

Entonces la función de distribución de falla viene dado por la integral desde -∞ hasta *t*, pero dado que probabilidades para $t<0$ carecen de sentido, la integral fija sus límites entre *0* y *t*. La función de distribución de probabilidad *F(t)* falla expresa la probabilidad que el sistema falle en el intervalo *0* y *t*.

$$F(t) = \int_0^t \lambda \cdot e^{-\lambda \cdot t} \cdot dt = 1 - e^{-\lambda \cdot t} \qquad (2.04)$$

De acuerdo a la ecuación 2.02

$$F(t) = 1 - R(t) \qquad (2.05)$$

La "Reliability" de un sistema con distribución de falla exponencial es:

$$R(t) = e^{-\lambda \cdot t} \qquad (2.06)$$

- **Función Densidad de Falla.**

La probabilidad de falla en un instante t de operación está dada por la función de densidad de probabilidad de falla. Así la densidad de probabilidad está dada por:

$$f(t) = \frac{dF(t)}{dt} \qquad (2.07)$$

Donde $F(t)$ es la función de distribución de probabilidad.

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

$$\lim_{\Delta t \to 0} = P(t < T \leq t + \Delta t) \qquad (2.08)$$

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

- **Rata o Tasa de falla ("Failure Rate").**

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

$$\lambda(t) = \frac{Fallas\ por\ unidad\ de\ tiempo}{Cantidad\ Expuesta} \qquad (2.09)$$

La tasa de falla de un equipo o sistema viene dado típicamente por λ, en la cual se

empresa la razón de cualquier tipo de falla, sin embargo podríamos distinguir dos tipos de razones o ratas dependiendo si la falla es del tipo segura λ_S, o si la falla es de condición peligrosa λ_D.

- **Tiempo Medio para Fallar ("Mean Time To Failure" (*MTTF*)).**

MTTF es el índice que señala el tiempo promedio de falla de un dispositivo y no la vida mínima esperada de éste.

Se puede demostrar que:

$$MTTF = E(T) = \int_0^{+\infty} R(t)dt \qquad (2.10)$$

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

Observación:

Nótese que *MTTF* no es igual a la inversa de la rata de falla λ.

- **Tiempo Medio para Reparar ("Mean Time To Repair" (*MTTR*)).**

MTTR es el tiempo promedio de la variable aleatoria tiempo para reparar.

- **Tiempo Medio entre Fallas ("Mean Time Between Failure" (*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.

$$MTBF = MTTF + MTTR \qquad (2.11)$$

2.5.3. Relación entre los Indices de Seguridad.

A continuación se establecen las relaciones mas frecuentemente usadas entre los índices de seguridad.

- **Safety Availability.**

  Disponibilidad del Sistema frente a fallas de condición peligrosa

$$A_D = 1 - PFD \qquad (2.12)$$

- **MTTF**

Tiempo promedio entre fallas. En términos generales se usa la aproximación práctica:

$$MTTF = \frac{1}{\lambda} \qquad (2.13)$$

que es válida sólo para tasas de falla constantes, es decir, haciendo uso de la distribución exponencial. Igualmente que las ecuaciones son válidas cuando la rata de reparación es mucho mayor que la rata de falla ($1/MMTR >> \lambda$)

- **Risk Reduction Factor.**

  Indice de Reducción de Riesgo viene dado como:

$$RRF = \frac{1}{PFD} \qquad (2.14)$$

2.5.4. Índices de Integridad.

Los índices de integridad (SIL, "Safety Integrity Level") definen el nivel de comportamiento o desempeño requerido del Sistema Instrumentado de Seguridad para alcanzar el objetivo de seguridad establecido. De acuerdo a la ISA-S84.01 se tienen los

siguientes niveles de integridad de seguridad: SIL 1, SIL 2 y SIL 3, los cuales serán mencionados posteriormente. SIL´s superiores al 3 no son establecidos por la ISA-S84.01, ver tabla 2.3.

Niveles de Integridad de Seguridad (SIL)	Probabilidad de Falla en Demanda (PFD)
1	10^{-1} a 10^{-2}
2	10^{-2} a 10^{-3}
3	10^{-3} a 10^{-4}

Tabla 2.3.- Niveles de Integridad de Seguridad (SIL).

2.6. MÉTODOS CUALITATIVOS Y CUANTITATIVOS PARA LA DETERMINACIÓN DEL SIL REQUERIDO POR EL PROCESO[3].

Los métodos de análisis cualitativos y cuantitativos utilizados para definir el SIL requerido por el proceso, han sido concebidos para reforzar la aplicación de la buena práctica de Ingeniería, con el fin de obtener elementos de juicio para soportar acciones que permitan alcanzar el nivel de seguridad requerido en las instalaciones.

2.6.1. Métodos Cualitativos.

El uso de análisis cualitativos para la determinación del SIL del SIS requiere de personal con gran experiencia en operaciones/procesos, instrumentación y seguridad para la identificación de: peligros, evaluación del riesgo (evaluación de la probabilidad

de ocurrencia y severidad de la consecuencia de cada evento), determinación de medidas reductoras de riesgos (capas de protección independientes y/o SIS).

La figura 2.7, muestra en forma general la metodología cualitativa para la determinación del SIL.

Los análisis cualitativos pueden presentar cierto nivel de incertidumbre dado a su carácter cualitativo. No obstante, la ventaja principal de esta metodología es su simplicidad, lo cual conlleva a un requerimiento menor de tiempo para el establecimiento del SIL.

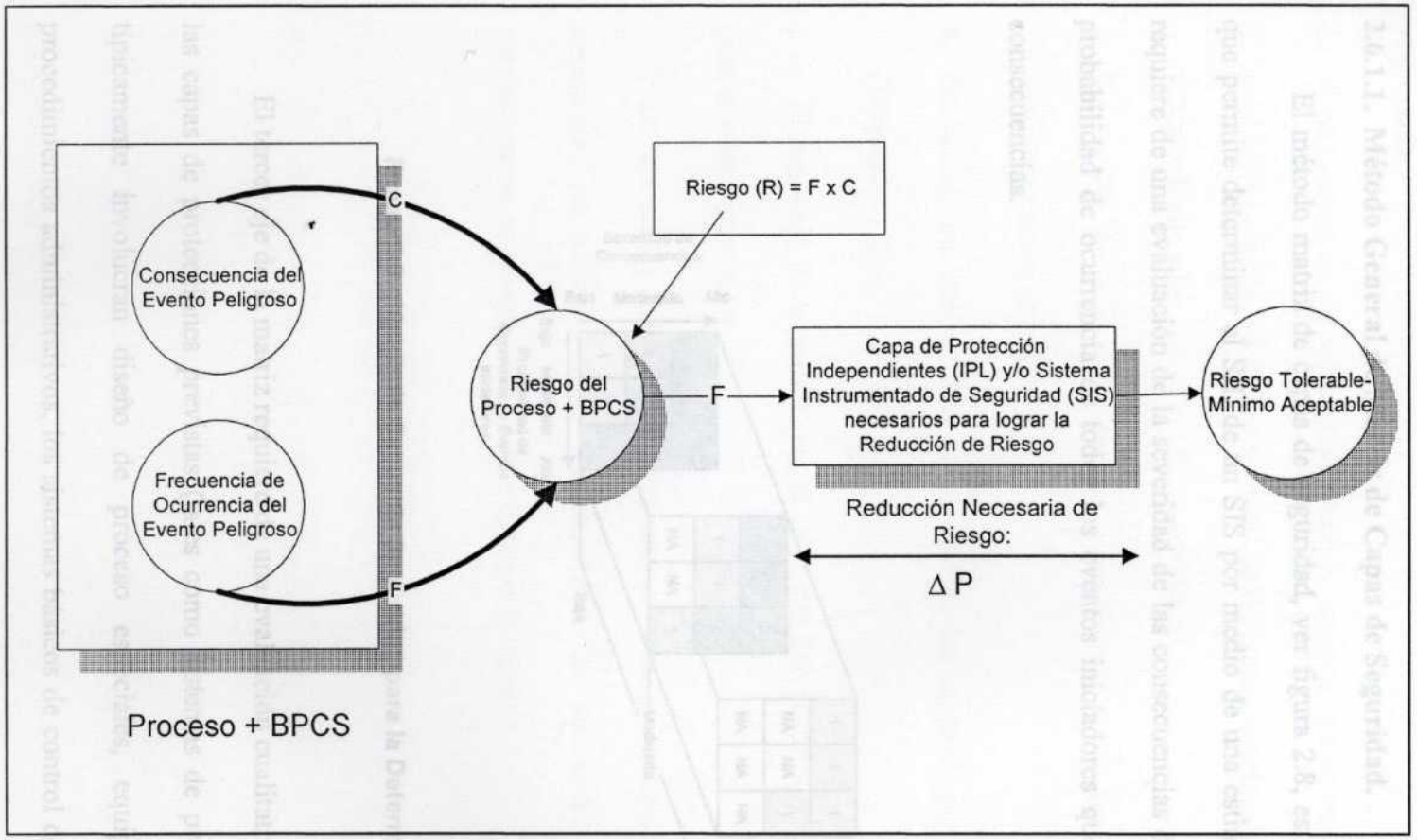


Figura 2.7.- Metodología Cualitativa para la Determinación del Nivel de Integridad de Seguridad.

A continuación, se detallan las dos metodologías:

2.6.1.1. Método General de Matriz de Capas de Seguridad.

El método matriz de capas de seguridad, ver figura 2.8, es un método cualitativo que permite determinar el SIL de un SIS por medio de una estimación del riesgo, que requiere de una evaluación de la severidad de las consecuencias de los peligros, y de la probabilidad de ocurrencia de todos los eventos iniciadores que podrían conllevar a consecuencias.

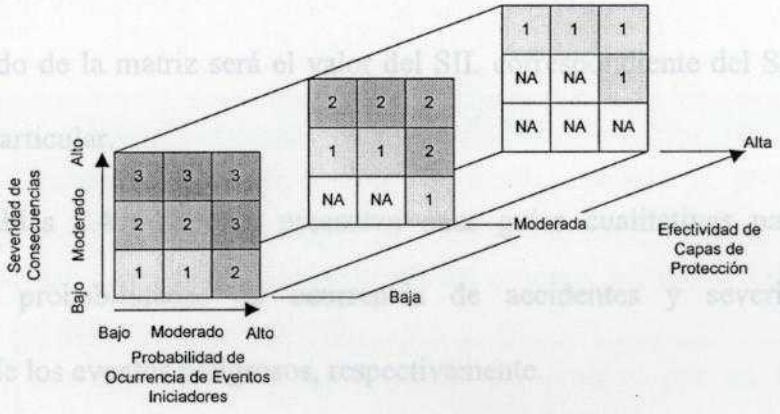


Figura 2.8.- Matriz de Capas de Seguridad para la Determinación del SIL.

El tercer eje de la matriz requiere de una evaluación cualitativa de la efectividad de las capas de protecciones previstas (tales como sistemas de protección o capas que típicamente involucran diseño de proceso especiales, equipo del proceso, los procedimientos administrativos, los sistemas básicos de control de procesos, y/o planes de emergencias).

A continuación se describen los pasos a seguir en el uso de la Matriz de capas de seguridad:

1. Identificación de los peligros del proceso / eventos iniciadores indeseables.
2. Evaluación cualitativa de la severidad de las consecuencias de los peligros de forma independiente a los cuales el SIS va a proteger.
3. Evaluación de la probabilidad de ocurrencia de todos los eventos que pudiesen ocasionar consecuencias
4. Evaluación cualitativa de la efectividad de las capas de protección independientes (Diferentes - SIS).

El resultado de la matriz será el valor del SIL correspondiente del SIS a instalar para el evento particular.

En las tablas 2.4 y 2.5, se presentan unas guías cualitativas para ayudar a determinar las probabilidades de ocurrencia de accidentes y severidad de las consecuencias de los eventos peligrosos, respectivamente.

Tipo de Evento	Probabilidad	
	Frecuencia ($año^{-1}$)	Rango Cualitativo
Eventos de muy baja probabilidad de ocurrencia, tales como fallas múltiples de instrumentos, errores humanos múltiples ó fallas espontaneas de equipos.	$F<10^{-4}$	Bajo
Eventos de baja probabilidad de ocurrencia, incluye la combinación de fallas de instrumentos con fallas humanas.	$10^{-4} < F < 10^{-2}$	Moderado
Eventos de probabilidad mediana - alta, tales como fallas de válvulas ó de instrumentación.	$F > 10^{-2}$	Alto

Tabla 2.4.- Probabilidad de Ocurrencia del Evento Peligroso por el Método de Matriz de Capas de Seguridad.

Severidad	Severidad del Evento
Baja	Daños menores al equipo, no implica parada al proceso, heridas y/o daños menores al personal y al ambiente.
Moderada	Daños al equipo, breve parada del proceso, heridas y/o daños al personal y al ambiente.
Alta	Graves daños al equipo, parada del proceso por un largo periodo de tiempo, consecuencias catastróficas al personal y/o el ambiente.

Tabla 2.5.- Severidad de Consecuencias.

2.6.1.2. Método General de Gráfica de Riesgo.

Los pasos a seguir en el método gráfico de riesgo esta simplificado basándose en la siguiente ecuación:

R (Riesgo) = F (Frecuencia) x C (Consecuencia)

- R: Riesgo sin el sistema instrumentado de seguridad (SIS)
- F: Frecuencia del evento peligroso sin el SIS
- C: Consecuencia del evento peligroso (Las consecuencias pueden estar relacionadas a daños asociados a personas, equipos y/o ambiente).

La frecuencia (F) del (los) evento(s) peligroso(s), se considera, influenciada por tres factores:

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

Por lo tanto, esto conlleva a los siguientes parámetros:

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

A continuación se describen los pasos a seguir en el uso del método de Gráfica de Riesgo:

- La combinación de los parámetros de riesgo descritos anteriormente, permite el

desarrollo de la gráfica del riesgo. En la figura 2.9, se puede apreciar que $C_1 < C_2 < C_3 < C_4$; $F_1 < F_2$; $P_1 < P_2$; $W_1 < W_2 < W_3$.

Los parámetros del método gráfica de riesgo, se describen a continuación:

- 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 son direccionadas a una de las tres escalas de probabilidad de ocurrencia del evento peligroso (W_1, W_2 y W_3). Cada punto en esta escala es una indicación del SIL requerido. En algunos casos particulares un SIS no es suficiente para la reducción del riesgo requerida.

- La selección entre W_1, W_2 y W_3 dependerá de la probabilidad de ocurrencia del evento no deseado.

- El resultado final de la Gráfica de Riesgo puede conllevar a la obtención de:

  - SIL (1, 2 ó 3). Como medida de reducción de riesgo requerida del sistema.
  - Al no requerimiento de un SIS (el cual es denotado por la letra "a").
  - Casos particulares donde un SIS no es suficiente (identificado con la letra "b").

La definición de los parámetros indicados en la figura 2.9 (C, F, P y W) son representados en las tablas 2.6, 2.7, 2.8 y 2.9.

Parámetro	Clasificación	Severidad del Evento
C1	Muy Baja	Sin daños al equipo, heridas leves al personal y daños al ambiente menores.
C2	Baja	Daños menores al equipo, no implica Parada al proceso, heridas y/o daños menores al personal y al ambiente.
C3	Moderada	Daños al equipo, breve parada del proceso, heridas y/o daños al personal y al ambiente.
C4	Alta	Graves daños al equipo, parada del proceso por un largo periodo de tiempo, consecuencias catastróficas al personal y/o el ambiente.

Tabla 2.6.- Extensión de los Daños.

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

Tabla 2.7.- Frecuencia de Exposición al Peligro.

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

Tabla 2.8.- Posibilidad de 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 (por ejemplo: 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.

Tipo de Evento	Probabilidad	
	Frecuencia/año	Rango Cualitativo
Eventos de muy baja probabilidad de ocurrencia, tales como fallas múltiples de instrumentos, errores humanos múltiples ó fallas espontaneas 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

Tabla 2.9.- Probabilidad de Ocurrencia del Evento Peligroso por el Método General de Gráfica de riesgo.

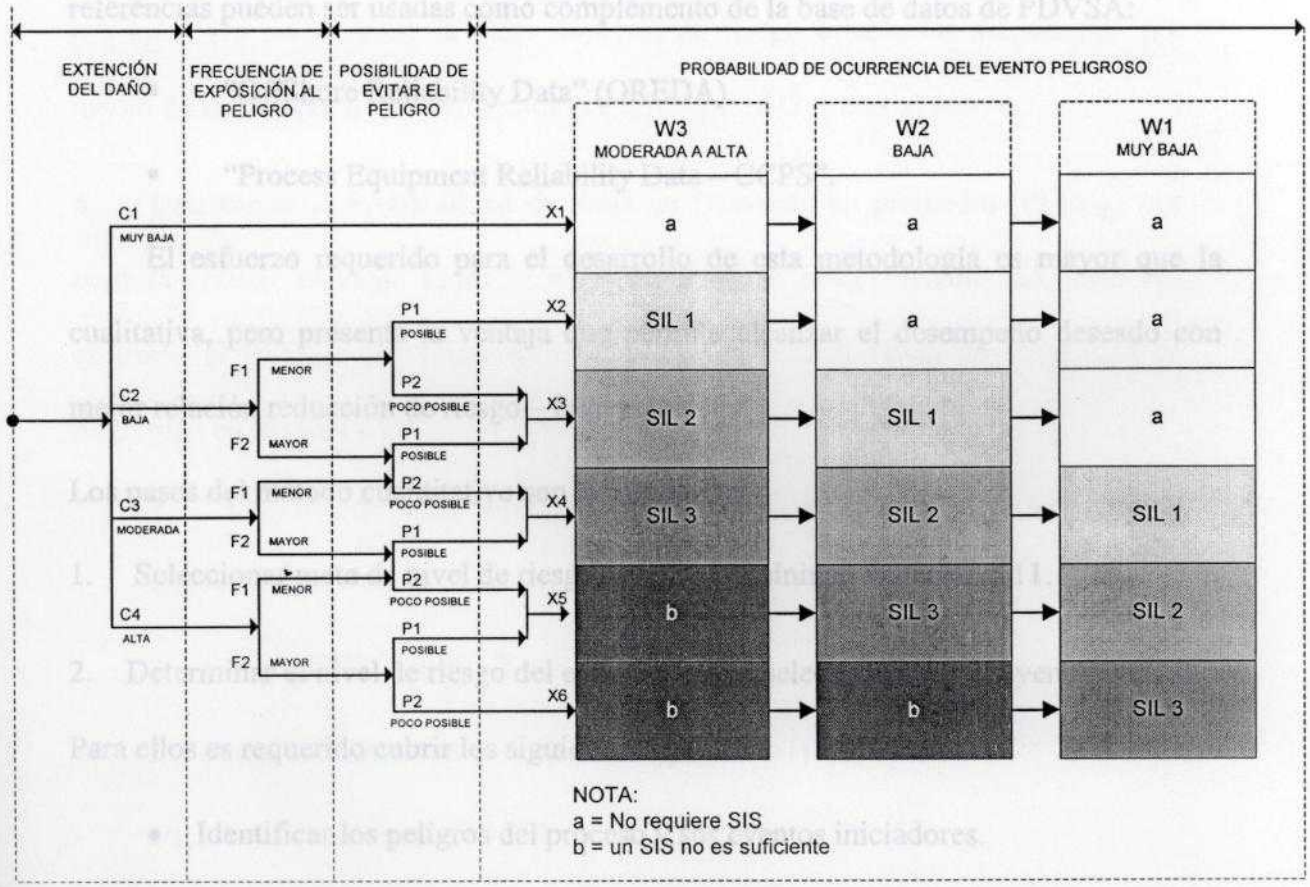


Figura 2.9.- Método Cualitativo de Gráfica de Riesgo para Determinación del SIL.

2.6.2. Método Cuantitativo.

Este método se fundamenta en la técnica de árbol de fallas. Los Análisis de Árbol de Fallas son diagramas de lógica que sistemáticamente despliegan la secuencia de fallas, que comienza con eventos iniciadores y combina las fallas equipos/instrumentos/sistemas y en errores humanos y finaliza en un evento peligroso definido, conocido como evento tope.

La guía PDVSA "IR-S-02 – Criterios para el Análisis Cuantitativo de Riesgo", presenta con mayor detalle la técnica de Árbol de Fallas, así como la base de datos de fallas de equipos y errores humanos requerida para su uso. No obstante, las siguientes referencias pueden ser usadas como complemento de la base de datos de PDVSA:

- "OffShore Reliability Data" (OREDA).
- "Process Equipment Reliability Data – CCPS".

El esfuerzo requerido para el desarrollo de esta metodología es mayor que la cualitativa, pero presenta la ventaja que permite alcanzar el desempeño deseado con mejor relación reducción de riesgo – inversión.

Los pasos del método cuantitativo son los siguientes:

1. Seleccionar meta de nivel de riesgo tolerable – mínimo, ver tabla 2.11.

2. Determinar el nivel de riesgo del equipo/sistema seleccionado (incluyendo BPCS).

Para ellos es requerido cubrir los siguientes aspectos:

- Identificar los peligros del proceso y sus eventos iniciadores.
- Identificar las diferentes capas de protección (Diferentes del SIS).

- Determinar la frecuencia de ocurrencia del evento tomando en consideración el BPCS, pero excluyendo la adición de cualquier capa de protección:

- Para determinar la frecuencia de ocurrencia del evento, se recomienda utilizar la metodología de árbol de fallas.

- Identificar si cada uno de los peligros cumplen con el nivel de riesgo tolerable - mínimo de acuerdo a la meta establecida según el tipo de instalación. De no alcanzar la meta de nivel de riesgo establecida, únicamente por medio del BPCS, pasar al paso 3.

3. Determinar la frecuencia considerando la(s) capa(s) de protección (IPL) del proyecto. De no alcanzar la meta de nivel de riesgo establecida únicamente por medio de las IPL(s), o una vez decidido a utilizar un SIS, pasar al paso 4.

4. Determinar la Probabilidad de Falla en Demanda en promedio (PFD_{avg}) que permita reducir el riego hasta la meta de nivel de riesgo establecido. Una vez asignado el PFD_{avg} correspondiente, se puede obtener el Nivel de Integridad de Seguridad en la tabla 2.10.

- Para determinar el nivel del SIL (PFD_{avg}) de un SIS puede utilizarse la siguiente relación:

  - $\mathbf{PFD_{avg} \leq F_t / F_{np} = \Delta R}$

- $\mathbf{F_t}$: Riego tolerable – mínimo (frecuencia en $año^{-1}$).

- $\mathbf{F_{np}}$: Tasa de demanda del SIS.

- **ΔR**: Reducción de riesgo necesario para alcanzar meta.

- **PFD_{avg}**: Probabilidad de falla en demanda promedio.

Niveles de Integridad de Seguridad (SIL)	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}

Tabla 2.10.- Niveles de Integridad de Seguridad (SIL).

Es importante destacar, que en esta etapa es recomendable realizar un Análisis Costo - Beneficio, donde se comparen las ventajas entre, colocación (únicamente) de IPL, SIS (únicamente) y/o la combinación de ambas (IPL y SIS), bajo la óptica, que los sistemas inherentemente seguros son aquellos sistemas sencillos y simple.

La meta de nivel de riesgo para la determinación del SIL del SIS fijados para la IPPN, son las descritas en la tabla 2.11 "Meta de Nivel de Riesgo Tolerable-Mínimo":

Clasificación de Instalación	Meta de Nivel de Riesgo ($año^{-1}$)
Normalmente atendida y no atendida con potencial de afectar a terceros.	10^{-6}
Normalmente atendida sin potencial de afectar a terceros.	10^{-5}
No atendida sin potencial de afectar a terceros.	10^{-4}

Tabla 2.11.- Meta de Nivel de Riesgo Tolerable – Mínimo.

2.7. CAPAS DE PROTECCIÓN INDEPENDIENTES [IPL(S)] [3].

Para la configuración del proceso, donde sea posible, es conveniente aplicar decisiones para una mayor reducción de riesgo hasta niveles tolerables – mínimos, vía cambio del diseño o de adición de IPL(s) y/o SIS. En la figura 2.10, se puede apreciar como el riesgo inherente al proceso (incluyendo el Sistema de Control Básico de Proceso - BPCS) debe ser reducido hasta una meta de riesgo tolerable – mínimo. En la misma se aprecia, que el primer paso a seguir es la evaluación de reducción del riesgo, es por medio del uso de Capa(s) de Protección Independiente(s) [IPL(s)]. En caso de que la reducción obtenida por la(s) IPL(s) sea insuficiente, se deberá proceder a la estimación del SIL para un SIS que cumpla la meta establecida.

Es importante destacar, que las medidas de reducción de riesgo deberán ser sustentadas por Análisis Costo-Beneficios, de acuerdo a lo establecido en la Guía PDVSA IR-S-02.

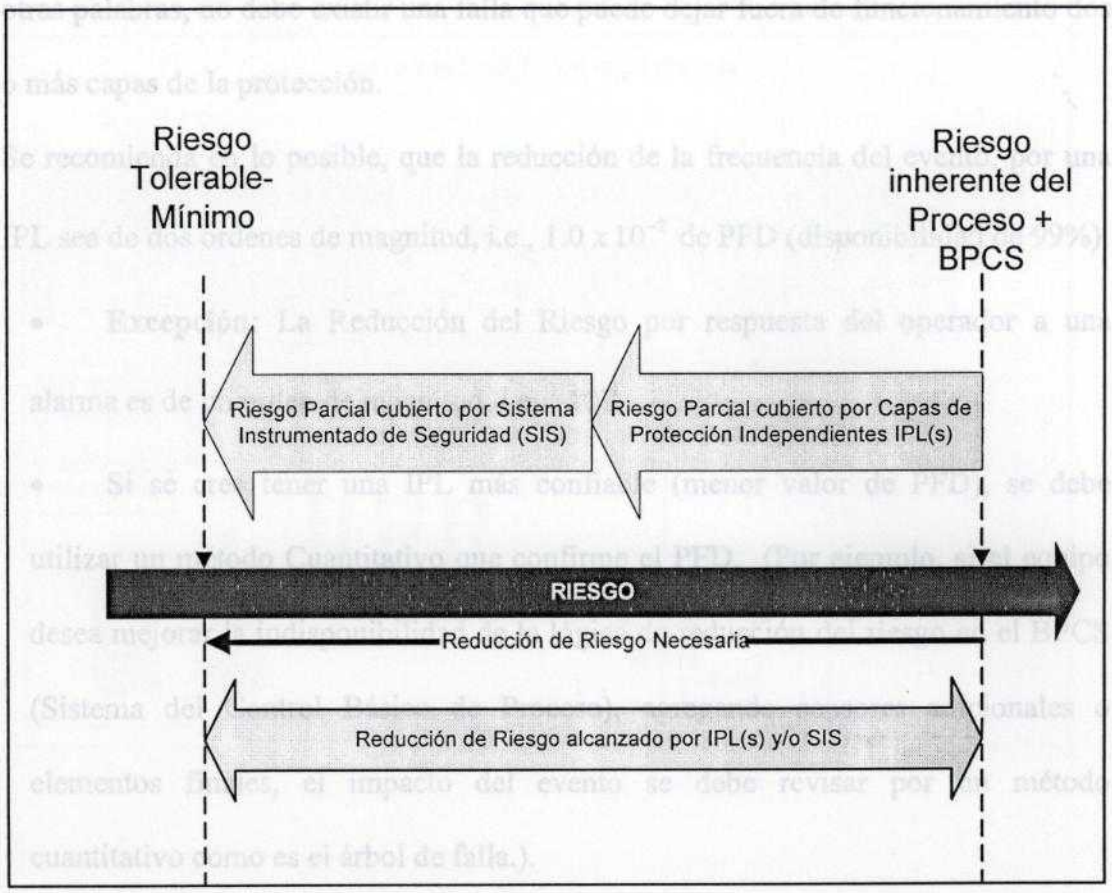


Figura 2.10.- Reducción de Riesgo: Conceptos Generales.

En al figura 2.11 de Capas Múltiples de Protección, se muestran en forma general algunas capas de protección independientes que podrían prevenir la(s) causa(s) Inicial(es) del evento peligroso. Las IPL(s) deben ser diferentes para diferentes causas iniciadoras.

Las siguientes *reglas para IPL(s),* determinan si las capas de protección evaluadas son independientes.

2.7.1. Reglas para IPL(s).

1. Cada capa de protección debe ser realmente independiente de las otras capas. En

otras palabras, no debe existir una falla que puede dejar fuera de funcionamiento dos o más capas de la protección.

2. Se recomienda en lo posible, que la reducción de la frecuencia del evento, por una IPL sea de dos ordenes de magnitud, i.e., 1.0×10^{-2} de PFD (disponibilidad de 99%).
   - **Excepción:** La Reducción del Riesgo por respuesta del operador a una alarma es de un orden de magnitud, i.e., 10^{-1}.
   - Si se cree tener una IPL más confiable (menor valor de PFD), se debe utilizar un método Cuantitativo que confirme el PFD. (Por ejemplo, si el equipo desea mejorar la indisponibilidad de la lógica de reducción del riesgo en el BPCS (Sistema del Control Básico de Proceso), agregando sensores adicionales o elementos finales, el impacto del evento se debe revisar por un método cuantitativo como es el árbol de falla.).
3. Una IPL es específicamente diseñada para prevenir o mitigar las consecuencias de un evento peligroso.
4. La IPL se diseña de tal manera que la misma pueda ser auditada.
5. En caso de que la causa inicial del evento peligroso indeseado sea causada por una falla en el Sistema del Control Básico de Proceso (BPCS), el BPCS no puede ser considerado como una IPL.
6. Las alarmas que son anunciadas y que son dependientes del BPCS, no se pueden considerar como IPL adicional.

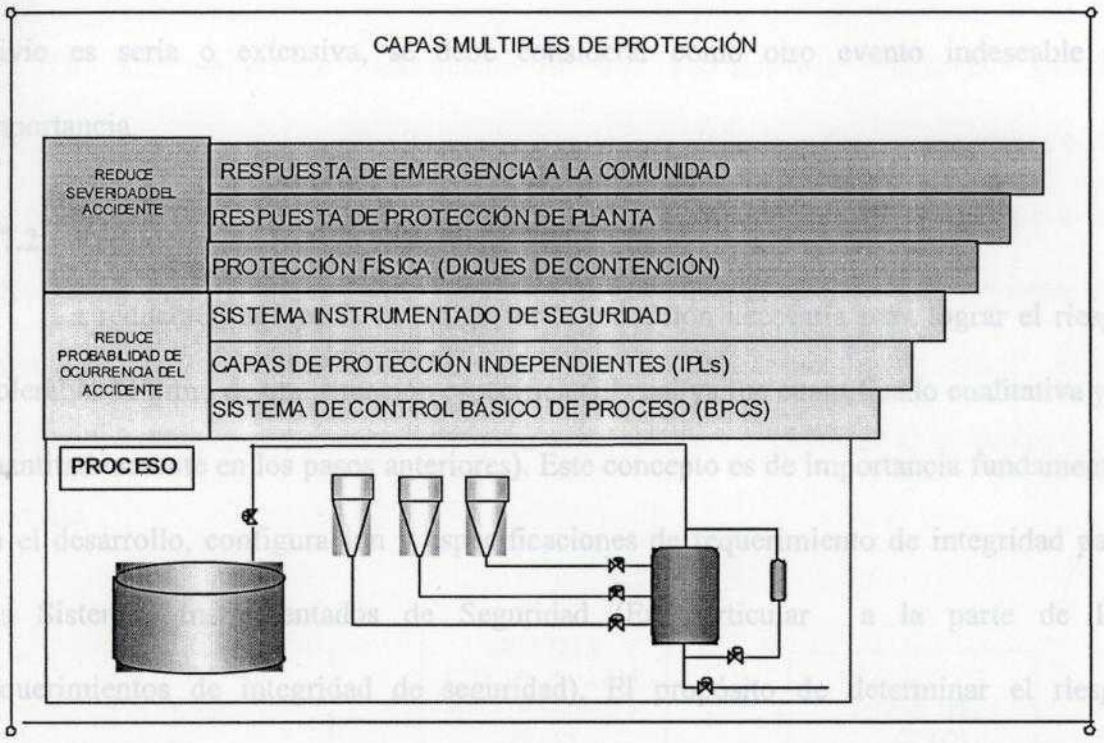


Figura 2.11.- Capas Múltiples de Protección.

En la figura. 2.11 de *Capas Múltiples de Protección*, se aprecia como las IPL(s) reducen la severidad así como la probabilidad del evento. En algunos casos, las IPL(s) que reducen la severidad, no previene todo los aspectos negativos del evento. Ejemplos de capas de mitigación son: válvulas del alivio, discos de ruptura, sensores para detección de descarga de productos al ambiente y procedimiento de evacuación, sensores y sistema de diluvio automático. De nuevo, cada capa debe ser independiente.

Se debe estar seguro de entender la severidad de la consecuencia del evento mitigado. Un evento no mitigado puede ser la rotura de un recipiente con la liberación de tóxicos o de material inflamable al medio ambiente. Se pudiera mitigar el tóxico

suelto a través de una válvula de alivio. Si la severidad de descarga de la válvula de alivio es seria o extensiva, se debe considerar como otro evento indeseable de importancia.

2.7.2. Reducción de Riesgo Necesaria.

La reducción necesaria de riesgo, es la reducción necesaria para lograr el riesgo Tolerable-Mínimo de una situación específica (El cual ya fue cuantificado cualitativa y/o cuantitativamente en los pasos anteriores). Este concepto es de importancia fundamental en el desarrollo, configuración y especificaciones de requerimiento de integridad para los Sistemas Instrumentados de Seguridad (En particular a la parte de los requerimientos de integridad de seguridad). El propósito de determinar el riesgo tolerable para un evento especifico peligroso, es el de establecer que es lo razonable permitido con respecto a los dos parámetros que determina el riesgo: la frecuencia (o probabilidad) del evento peligroso y sus consecuencias especificas. Los sistemas relacionados con la seguridad son diseñados para reducir la frecuencia (o probabilidad) del evento peligroso.

2.8. CONFIGURACIÓN DE UN SIS[4].

En los actuales momentos para la configuración de un SIS, existen diferentes maneras para distribuir (configurar) todos los componentes de un sistema de control. Algunos arreglos son diseñados para maximizar la probabilidad de éxito de la operación (Confiabilidad o Disponibilidad), otros arreglos son diseñados para minimizar la probabilidad de falla con las salidas energizadas (ó dependiendo de la aplicación:

minimizar la probabilidad de falla con las salidas desenergizadas).

Un SIS comprende básicamente de tres Sub-sistemas: Sensores, Sistema Controlador Programable (PES) (Logic Solvers) y los elementos finales (Válvulas, etc.), ver figura 2.12, por lo que los conceptos de diferentes arquitecturas se extiende a todos estos sub-sistemas. Todos los arreglos posibles de configuración de los componentes del sistema de control es lo que se entiende como la "Arquitectura del Sistema". En el presente trabajo se presentan las arquitecturas de sistemas disponibles al momento en el mercado.

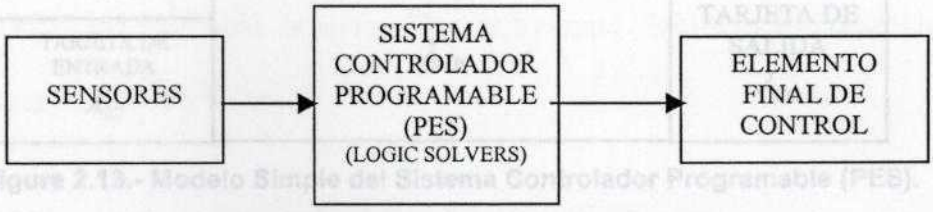


Figura 2.12.- Componentes de un SIS.

2.8.1. Modelaje de Sensores y Elementos Finales de Control.

Para el modelaje independiente de los sensores y elementos finales de control debe tenerse presente que las fallas de uno de estos dispositivos sea independiente y que no afecte a los otros subsistemas, esto es que la falla de un sensor no afecte y haga fallar al controlador.

2.8.2. Modelaje del Sistema Controlador Programable (PES).

Las diferentes arquitecturas y sus características pueden ser explicadas utilizando un modelo simple de un controlador electrónico programable. En la figura 2.13 se muestra un modelo simple de un controlador con: Tarjetas de Entrada, Tarjetas de

Salida y la Unidad Central de Procesamiento (CPU). Este nivel de detalle es suficiente para la comparación de las diferentes arquitecturas. Este controlador es una unidad reparable, por lo tanto, podemos asumir que cualquier falla de un componente, causará la falla del controlador. La rata de falla del controlador es la suma de la rata de falla de cada componente.

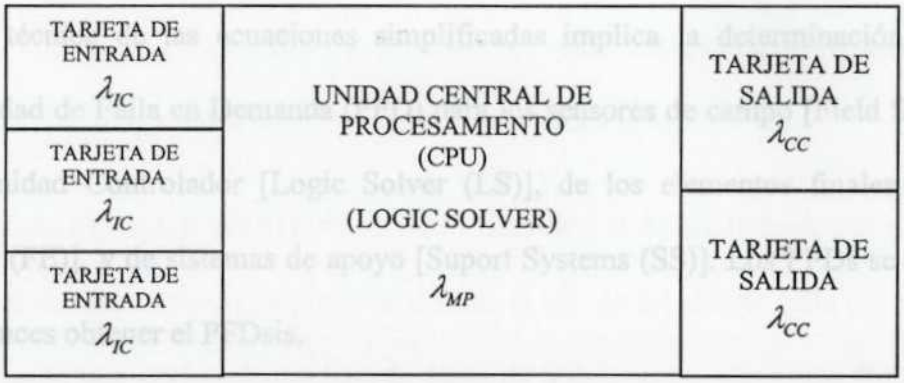


Figura 2.13.- Modelo Simple del Sistema Controlador Programable (PES).

2.8.3. Riesgo y la Integridad de Seguridad.

Es importante la distinción entre riesgo y la Integridad de Seguridad del SIS. El Riesgo es una medición de la probabilidad y consecuencia de la ocurrencia de un evento peligroso específico del proceso. La Integridad de Seguridad es aplicado solamente a los Sistemas Integrados de Seguridad SIS y es la medición de la probabilidad de estos sistemas de satisfactoriamente lograr la estimada reducción de riesgo necesaria. El Nivel de Integridad de Seguridad definido en la Norma ANSI/ISA S84.01-1996 como uno de los tres posibles niveles discretos de seguridad (SIL 1, SIL 2, SIL 3) de los Sistemas Instrumentados de Seguridad (SIS). El SIL es relacionado a la probabilidad del SIS a fallar a una demanda del proceso.

2.8.4. Técnica de Evaluación.

Se dispone de tres posibles técnicas para la evaluación de las capacidades de un diseño o arquitectura de un SIS para un SIL designado. Los tres métodos son: Ecuaciones Simplificadas, Análisis de Arbol de falla y modelo de Markov.

2.8.5. Cálculo de un SIL de un SIS utilizando las 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 Sensors (FS)], Unidad Controlador [Logic Solver (LS)], de los elementos finales [Final Elements (FE)], y de sistemas de apoyo [Suport Systems (SS)]. Los PFDs se suman para entonces obtener el PFDsis.

$$\text{PFD}_{SIS} = \sum PDF_{FS} + \sum PDF_{LS} + \sum PFD_{FE} + \sum PFD_{SS}$$

Las ecuaciones simplificadas usadas para calcular los PFDs son derivadas de los modelos de Markov, sin embargo, las simplificaciones de los modelos introducirán algunas limitaciones tales como:

- A diferencia del modelo de Markov, este método no maneja los tiempos variables de reparación, fallas dependientes del tiempo, o fallas dependientes de las secuencias.
- Otro factor limitante en el uso de este método es que las ecuaciones no permiten el modelado de tecnologías diversas. Los sensores o los elementos

finales usados en cada estrategia de la votación deben tener la misma proporción de falla.

- Este método no permite el modelado de un interruptor y un transmisor o de una válvula de control y una válvula del bloque a la vez.

Este método sólo considerará las fallas del sensor como problemas separados, por consiguiente, este es utilizado para sólo modelar SIS(s) simples.

Sin embargo, la matemática utilizada en esta metodología es sencilla. Por consiguiente, este método es excelente para una primera aproximación.

2.8.6. Determinación del SIL de un SIS utilizando el Análisis de Árbol de Falla.

En el presente trabajo de grado se discute el uso de árboles de falla para el cálculo del SIS. La técnica gráfica de análisis de árbol 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 diferentes ratas de reparación, fallas dependientes del tiempo, o de eventos secuenciales.

El análisis de árbol de falla utilizado en este trabajo es una de las técnicas más utilizadas para el modelado de sistemas instrumentados de seguridad con índices de integridad SIL2 y SIL3. Para su uso se requiere un mayor entrenamiento y experiencia que el método anterior de las ecuaciones simplificadas, pero los resultados serán más precisos.

2.8.7. Determinación del SIL de un Modelo de Markov.

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 (PES).

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". Los efectos de cada falla son determinadas al efectuar un "Análisis de Modos de Fallas y Efectos [Failure Mode and Effects Analysis (FMEA)].

El Modelo de Markov permite el modelaje de múltiples sistemas en el cual el nivel de redundancia varia con el tiempo debido a fallas de los componentes y a la reparación de los mismos.

2.8.8. Diagnostico en Línea.

La confiabilidad y seguridad del sistema puede ser sustancialmente incrementada cuando se programa rutinas de diagnostico en el sistema para detectar fallas en: componentes, módulos o unidades. El beneficio inmediato es que se reduce el tiempo de reparación. El diagnóstico identifica y anuncia la(s) falla(s). La(s) reparación(es) pueden ser realizadas rápidamente sin necesidad de esperar por las inspecciones periódicas.

Los efectos de diagnóstico en línea deben ser modelados, se incluyen cuatro categorías de fallas:

- Peligrosa - Detectada (Dangerous - Detected): DD
- Peligrosa - No Detectada (Dangerous - Undetected): DU

- Segura – Detectada (Safe – Detected) SD
- Segura – No Detectada (Safe – Undetected) SU

Los factores de diagnóstico son los siguientes:

$$\lambda^{DD} = C^D \lambda^D$$
$$\lambda^{DU} = (1 - C^D) \lambda^D$$
$$\lambda^{SD} = C^S \lambda^S$$
$$\lambda^{SU} = (1 - C^S) \lambda^S$$

Donde C^S es el Factor de Cobertura de Seguridad y C^D es el Factor de Cobertura Peligrosa.

2.8.9. Aproximaciones Asumidas Para los Cálculos.

- La rata de falla de los componentes es constante durante la vida del sistema.
- Componentes redundantes tienen iguales ratas de falla.
- 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).
- Todos los modelos tienen capacidades de auto - diagnóstico en línea y causa común.
- El mantenimiento de los equipos permite rápidas reparaciones y la detección

de fallas peligrosas sin necesidad de parada del sistema.

- Se asume inspecciones y reparaciones perfectas, esto es, todas las piezas y circuitos del equipo son inspeccionadas y reparadas (si existieran fallas ocultas).
- La aproximación (MTTF=1/λ) es válida sólo para 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/MMTR>>λ).

2.8.10. Base de Datos de Confiabilidad del Equipo[5].

La cuantificación del riesgo está basada tanto en la estimación de la frecuencia de ocurrencia del evento no deseado como en el cálculo de sus consecuencias. La frecuencia de falla de un componente particular puede ser deducida a partir de información histórica y si es posible, soportada en juicios de expertos que tomen en cuenta diferencias entre características de la planta analizada y las que pudiesen haber estado envueltas en los registros históricos de fallas (diferentes modos de fallas).

Cada bloque del diagrama del árbol de falla debe tener los valores estimados de frecuencia o probabilidad de falla para poder resolver el árbol de falla, cuyo resultado es la frecuencia de ocurrencia del evento principal. Esta frecuencia de evento principal se combina entonces en la curva de frequencia/consecuencia, ver figuras 2.1 y 2.14. La diagonal en esta curva de frecuencia/consecuencia es el criterio de aceptación de riesgo mínimo presentado para las decisiones de seguridad o de riesgo.

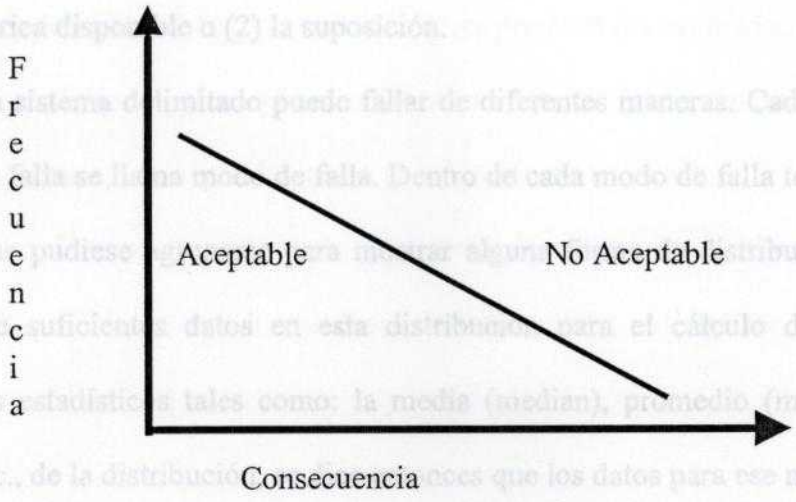


Figura 2.14.- Curva de Frequencia/Consecuencia

La exactitud de la data para el análisis del árbol de falla determina la calidad de los resultados cuantitativos de frecuencia de falla del proceso mas el BPCS para cada evento en particular considerado, y poder aplicar la mejor decisión en la reducción del riesgo hasta la meta de nivel de riesgo mínimo establecido.

Se define la data de rata de fallas como expresiones del número de fallas de un sistema a los cuales se le delimitan bien los límites por unidad de tiempo. Para tomar la mejor decisión de calidad deben escogerse la data de ratas de falla usados en un sistema delimitado. La fuente mas deseable de base de datos estadísticos de fallas de instrumentos y equipos es la propia de la planta, utilizando esta base de datos permitirá una mejor selección de instrumentos, equipos y sistemas basado en el desempeño de los equipos utilizados en el propio ambiente de operación de la planta. Actualmente PDVSA no cuenta con una base de datos estadístico de fallas de equipos propia. La data disponible es anecdótico o el resultado de data que se recoge al azar y no de un esfuerzo

continuo. Cuando éste es el caso, el analista tiene dos opciones: (1) Usar una base de datos genérica disponible o (2) la suposición.

Cada sistema delimitado puede fallar de diferentes maneras. Cada manera en que un sistema falla se llama modo de falla. Dentro de cada modo de falla tenemos un grupo de data que pudiese agruparse para mostrar alguna forma de distribución. Cuando se dispone de suficientes datos en esta distribución para el cálculo de los siguientes parámetros estadísticos tales como: la media (median), promedio (mean), desviación normal, etc., de la distribución, se dice entonces que los datos para ese modo de falla son estadísticamente relevantes. Una prueba de relevancia es cuando el valor de la media de ese modo de falla no varía significativamente con la suma de más puntos de data.

Cada sistema delimitado puede sufrir diferentes modos de fallas. A veces el árbol de falla indicará un modo de falla a ser considerado específicamente. Sin embargo, la mayoría de las veces el modo de falla no es especificado. Cuando esto ocurre la presunción es que cualquier modo de falla puede iniciar el evento no deseado. Debe considerarse entonces que los datos para todos los modos de falla del sistema delimitado deben provenir de una fuente de data representativa. Por supuesto esto cambia la calidad de la estimación de frecuencia utilizada en la curva de aceptabilidad. La distribución de todos los modos de falla específicos debe ser considerada. Generalmente se suma toda la data y producir una sola base de datos para todos los modos de falla.

La data de falla es la combinación de grandes distribuciones de datos. La desviación normal se ensancha con los datos de falla de muchos modos de falla, ver figura 2.15.

Se asume que la fuente de data es la más representativa de todos los modos de falla. Así que los árboles de falla utilizados para producir los estimados de frecuencia de los eventos no deseados que usan estos datos anecdóticos tiene ninguna descripción de la variabilidad o genealogía que describen la población de los datos.

Esto produce una incertidumbre que debe aceptarse o neutralizarse, si los datos genéricos disponible de una fuente fuera de la compañía que usa los datos será usado para tomar una decisión.

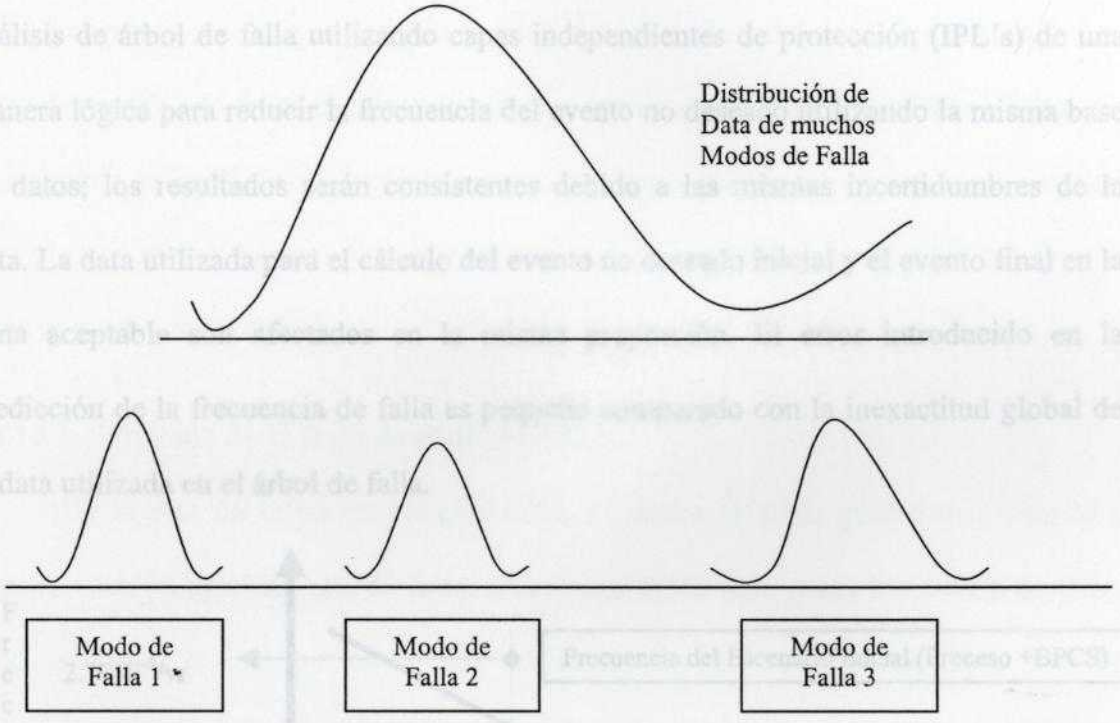


Figura 2.15.- Distribución de Data.

Una forma de reducir los errores al utilizar data genérica es evitar utilizar valores absolutos. Debido a que la data genérica no se genera dentro de la compañía, pueden esperarse errores. La data puede ser obsoleta, de baja calidad, no estrictamente aplicable

al uso presente, o diferencias debido al tipo de industria ó ambiente (servicio). La data también puede ser de relevancia estadística cuestionable debido a la insuficiente población dentro de la distribución.

Si en el análisis de riesgo de un evento no deseable, tal como se muestra en la figura 2.16, el resultado está en una posición inaceptable (arriba de la recta de frecuencia/consecuencia aceptable), esto indica que debe hacerse algo para cambiar las coordenadas de este evento en particular hacia la región aceptable (debajo de la recta de aceptación). Si las modificaciones del sistema son examinadas incluyéndolos en el análisis de árbol de falla utilizando capas independientes de protección (IPL´s) de una manera lógica para reducir la frecuencia del evento no deseado utilizando la misma base de datos; los resultados serán consistentes debido a las mismas incertidumbres de la data. La data utilizada para el cálculo del evento no deseado inicial y el evento final en la zona aceptable son afectados en la misma proporción. El error introducido en la predicción de la frecuencia de falla es pequeño comparado con la inexactitud global de la data utilizada en el árbol de falla.

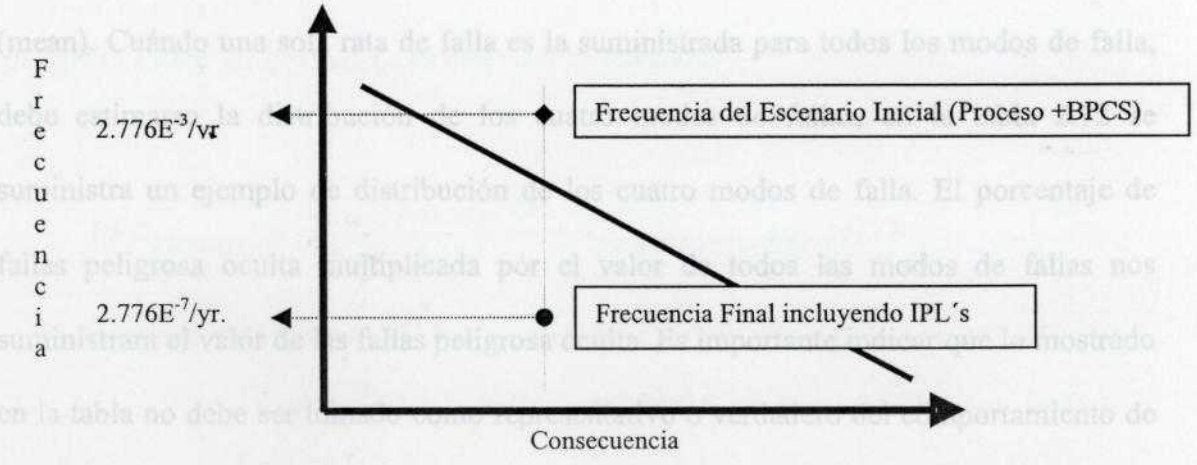


Figura 2.16. - Cambio de la Frequencia sin cambiar la Consecuencia

2.8.10.1. Modos de Fallas.

Para suministrar una valorización significativa de la operación de los sistemas, la base de datos de ratas de fallas debe suministrar información de los modos de falla. Los modos de fallas son divididos en cuatro tipos de fallas: Fallas Peligrosas Detectadas (Revealed Dangerous), Fallas Peligrosas Ocultas (Hidden Dangerous), Fallas Seguras Detectadas (Revealed Safe) y Fallas Seguras Ocultas (Hidden Safe).

Los modos de fallas peligrosas resultan en pérdida de protección, pero las fallas Peligrosas Detectadas pueden ser rápidamente detectadas y reparadas, por lo tanto, las fallas peligrosas ocultas son las más importantes para el modelaje de los sistemas. Los otros dos modos de fallas seguras: detectada y oculta resultan en una parada y luego en un arranque de la planta que pudiera ser en condiciones menos seguras que en operación normal. Los falsos disparos tienen implicaciones de seguridad y/o económicos que no serán cubiertas por este trabajo.

2.8.10.2. Selección de la Data de Rata de Fallas.

De la rata de fallas de los elementos se utiliza el valor geométrico promedio (mean). Cuándo una sola rata de falla es la suministrada para todos los modos de falla, debe estimarse la distribución de los cuatro modos de fallas, en la tabla 2.12 se suministra un ejemplo de distribución de los cuatro modos de falla. El porcentaje de fallas peligrosa oculta multiplicada por el valor de todos las modos de fallas nos suministrara el valor de las fallas peligrosa oculta. Es importante indicar que lo mostrado en la tabla no debe ser tomado como representativo o verdadero del comportamiento de los componentes en campo, siempre se debe soportar esta en un sano juicio para la

efectiva descomposición en los cuatro modos de falla. En el presente trabajo se utilizó en lo posible ratas de fallas críticas ó la mas representativa del modo de falla representada en el árbol de fallas al cual se le pretendía aplicar el valor, ejemplo: para el separador de gas petróleo en el lazo de control crítico de Bajo Bajo Nivel de Crudo se utilizo como rata de falla peligrosa $\lambda_{oculta\ peligrosa}$ la indicada por la falla de leakage externo.

Elemento	% Fallas Peligrosas Ocultas	% Fallas Seguras Ocultas	% Fallas Reveladas Peligrosas	% Fallas Reveladas Seguras
Sensor	30	20	30	20
Elemento Final	30	20	30	20
Procesador Principal	10	5	40	45
Módulo Analógico de Entrada	37,5	25	12,5	25
Módulo Analógico de Salida	37,5	25	12,5	25
Módulo Digital de Entrada	37,5	25	12,5	25
Módulo Digital de Salida	37,5	25	12,5	25
Procesador de I/O	12,5	7,5	37,5	42,5
Circuito de I/O	37,5	25	12,5	25
Relés de Control	25	0	0	75

Tabla 2.12.- Ejemplo de Distribución de Modos de Fallas.

2.8.10.3. Cálculo del $PFD_{PELIGROSO}$.

El Proceso y el BPCS fallaran en demanda peligrosamente si una falla peligrosa existe. El $PFD_{Peligroso}$ es dado por la ecuación:

$$PFD_{PELIGROSO} = \frac{\lambda_{OCULTO\ PELIGROSO}\ TI}{2} + \lambda_{DETECTADO\ PELIGROSA}\ MTTR$$

En el presente caso, el $PFD_{Peligroso}$ es suficiente calcularlo con el primer termino debido a que los elementos del proceso y del BPCS no son reparables en línea y

también debido a que el segundo termino es mucho mas pequeño que el primer termino.

A continuación se muestra en la tabla 2.13 la recopilación de los cálculos del $PFD_{Peligroso}$ para los diferentes elementos utilizados en los cálculos cualitativos de los arboles de falla. La base de datos para las Ratas de Fallas de los elementos fue la suministrada por "Process Equipment Reliability Data" del CCPS y "Offshore Reliability Data Handbook (Oreda)", 2nd edición, el intervalo de pruebas (TI) considerado es de un (1) año (8760 Horas).

ELEMENTO	Frecuencia de Todos los Tipos de Falla λ (/Hrs)	Frecuencia de Falla Peligrosa λ_P (/Hrs)	$PFD_{Peligroso}$ $P = \frac{\lambda_P * T_I}{2}$
Interruptor de Nivel	9,6 E-06	1,50E-06	6,57E-03
Transmisor de Nivel	11 E-06	6,50E-07	2,85E-03
Interruptor de Temperatura	24 E-06	6,60E-06	2,89E-02
Transmisor de Temperatura	12 E-06	8,50E-07	3,72E-03
Interruptor de Presión	13 E-06	6,80E-06	2,98E-02
Transmisor de Presión	42 E-06	8,00E-07	3,50E-03
Interruptor de Flujo	7,5 E-06	3,00E-06	1,31E-02
Transmisor de Flujo	17 E-06	1,70E-05	7,45E-02
Válvula de ESS	70,49 E-06	3,30E-05	1,45E-01
Válvula Solenoide	1,32 E-06	9,00E-07	3,94E-03
Válvula de Control Neumática	30,88 E-06	3,64E-06	1,59E-02
Válvula Motorizada	33,70 E-06	1,24E-05	5,43E-02
Convertidor I/P	62,8 E-06	6,28E-06	2,75E-02
PLC (Procesador Principal) (IEEE Guide)	50 E-06	5,00E-06	2,19E-02
Anunciadores de Alarmas	0,77 E-06	7,70E-07	3,37E-03
Operador Average		2,28E-05	1,00E-01
Separador Gas Petróleo	85,45 E-06	1,89E-05	8,28E-02
Tanques de Estabilización	24,16 E-06	9,02E-06	3,95E-02
Bomba de Crudo Vertical de Cuatro Etapas	230,77 E-06	2,31E-05	5,05E-02

Tabla 2.13.- Cálculo de los $PFD_{Peligroso}$ de los diferentes elementos utilizados para el cálculo del $PFD_{Peligroso}$ del Proceso y BPCS.

2.9. ARQUITECTURAS DEL SIS[6].

A continuación se muestran todas las posibles arquitecturas del SIS disponibles comercialmente para el presente y que son evaluados.

2.9.1. Arquitectura 1001.

Esta arquitectura, ver figura 2.17, es representada por un solo controlador con una sola unidad central de procesamiento (CPU) y una sola tarjeta de I/O. Esta arquitectura de sistema no es tolerante a fallas ni posee modo de protección de falla. Los circuitos electrónicos pueden fallar de forma segura (salidas desenergizadas, circuito abierto) ó peligrosa (salidas congeladas o energizadas, corto-circuitos).

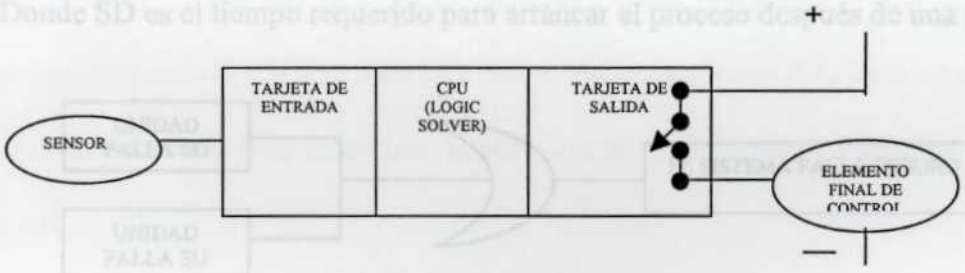


Figura 2.17.- Arquitectura 1001.

- **Cálculo de PFD por Árbol de Falla para La Arquitectura 1001.**

La figura 2.18 muestra el árbol de falla para fallas peligrosas. El sistema falla peligrosamente si la unidad falla DD o DU, la probabilidad de falla en demanda (PFD) será:

$$PFD_{Avg.1oo1} = \lambda^{DD} \; x \; RT + \frac{\left(\lambda^{DU} \; x \; TI\right)}{2}$$

Donde RT es el Tiempo de Reparación y TI es el intervalo de tiempo para inspección periódica.

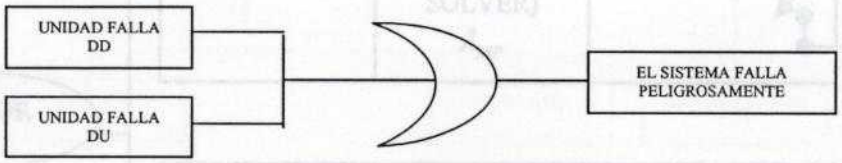


Figura 2.18.- Arquitectura 1001, Árbol de Falla PFD.

- **Cálculo de PFS por Árbol de Falla para la Arquitectura 1001.**

La figura 2.19 muestra el árbol de falla para fallas seguras. El sistema falla seguro si la unidad falla SD o SU, la probabilidad de falla Segura (PFS) será:

$$PFS_{1\infty1} = \lambda^{SD} \, x \, SD + \lambda^{SU} \, x \, SD$$

Donde SD es el tiempo requerido para arrancar el proceso después de una parada.

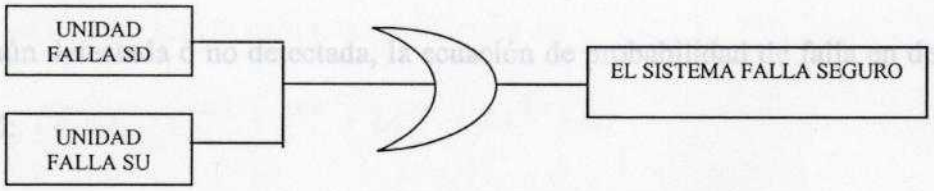


Figura 2.19.- Arquitectura 1001, Árbol de Falla PFS.

2.9.2. Arquitectura 1002.

- Dos controladores (PES), ver figura 2.20, pueden ser conectados para minimizar los efectos de las fallas peligrosas. El sistema ofrece una baja probabilidad de falla en demanda, pero se incrementa la probabilidad de falla segura.

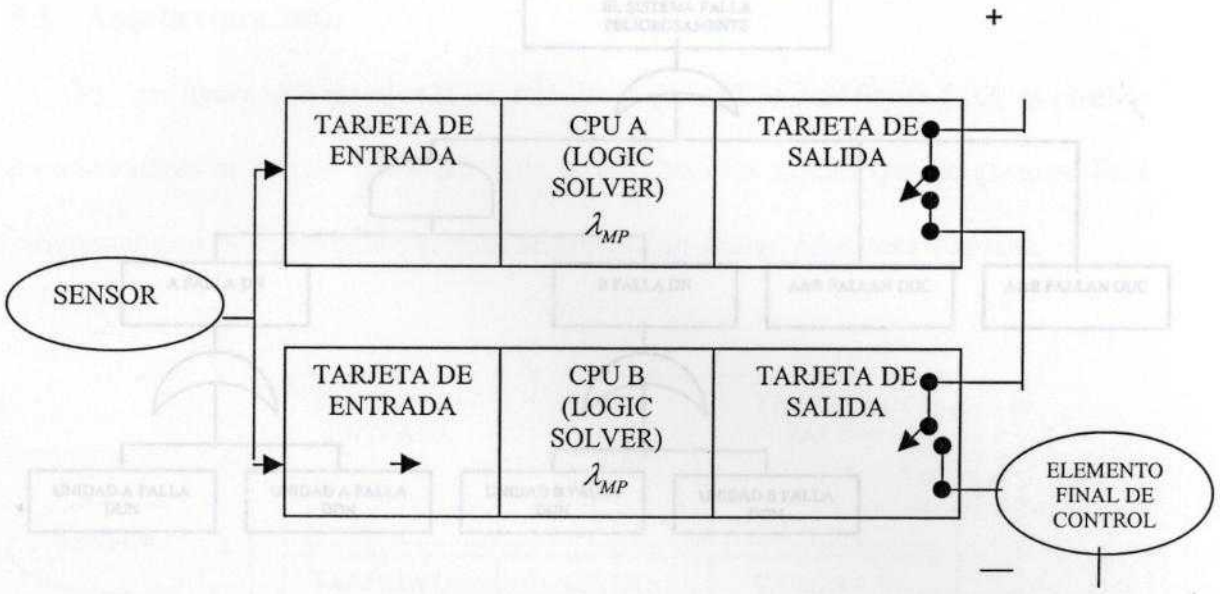


Figura 2.20.- Arquitectura 1002.

- **Cálculo de PFD por Árbol de Falla para La Arquitectura 1002.**

La figura 2.21 muestra el árbol de falla para fallas peligrosas (PFD). El sistema falla peligrosamente si las dos unidades fallan peligrosamente debido a una falla de causa común detectada o no detectada, la ecuación de probabilidad de falla en demanda (PFD) será:

$$PFD_{Avg.1oo2} = \frac{\left(\lambda^{DUC}\ x\ TI\right)}{2} + \lambda^{DDC}\ x\ RT + \left(\lambda^{DDN}\ x\ RT\right)^2 + \lambda^{DDN}\ x\ RT\ x\ \lambda^{DUN}\ x\ TI + \frac{\left(\lambda^{DUN}\ x\ TI\right)^2}{2}$$

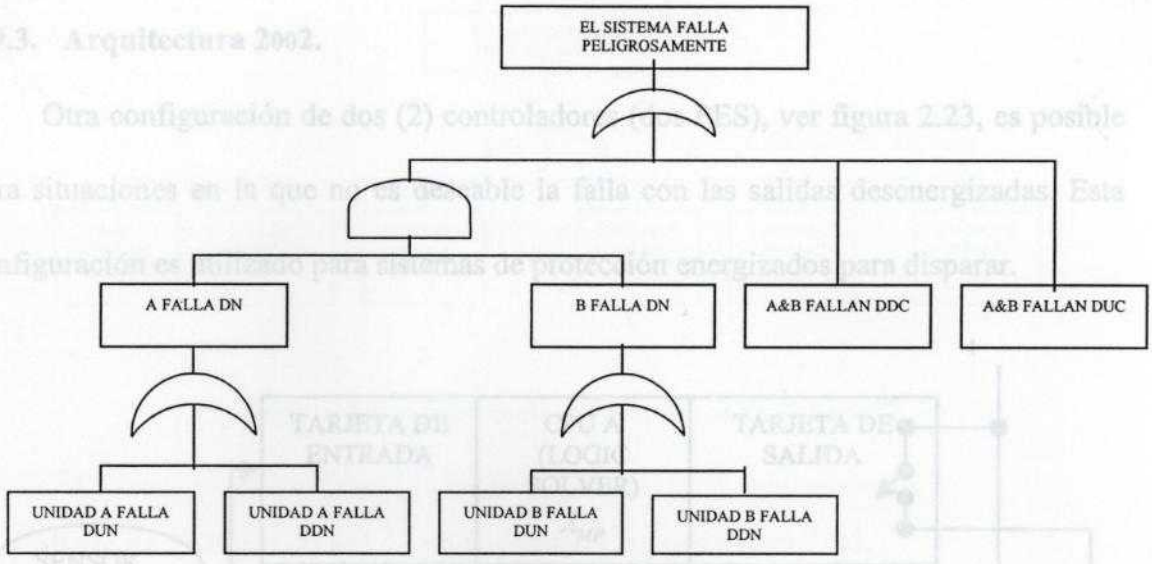


Figura 2.21.- Arquitectura 1002, Árbol de Falla PFD.

- **Cálculo de PFS por Árbol de Falla para La Arquitectura 1002.**

La figura 2.22 muestra el árbol de falla para fallas seguras (PFS). El árbol de falla muestra que una falla de cualquier unidad causará un disparo falso. La ecuación de probabilidad de falla segura para esta arquitectura es:

$$PFS_{1oo2} = (\lambda^{SDC} + \lambda^{SUC} + 2\lambda^{SDN} + 2\lambda^{SUN})\, SD$$

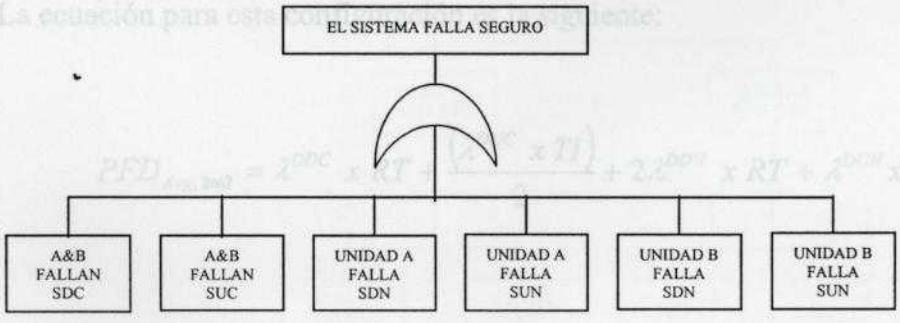


Figura 2.22.- Arquitectura 1002, Árbol de Falla PFS.

2.9.3. Arquitectura 2002.

Otra configuración de dos (2) controladores (dos PES), ver figura 2.23, es posible para situaciones en la que no es deseable la falla con las salidas desenergizadas. Esta configuración es utilizado para sistemas de protección energizados para disparar.

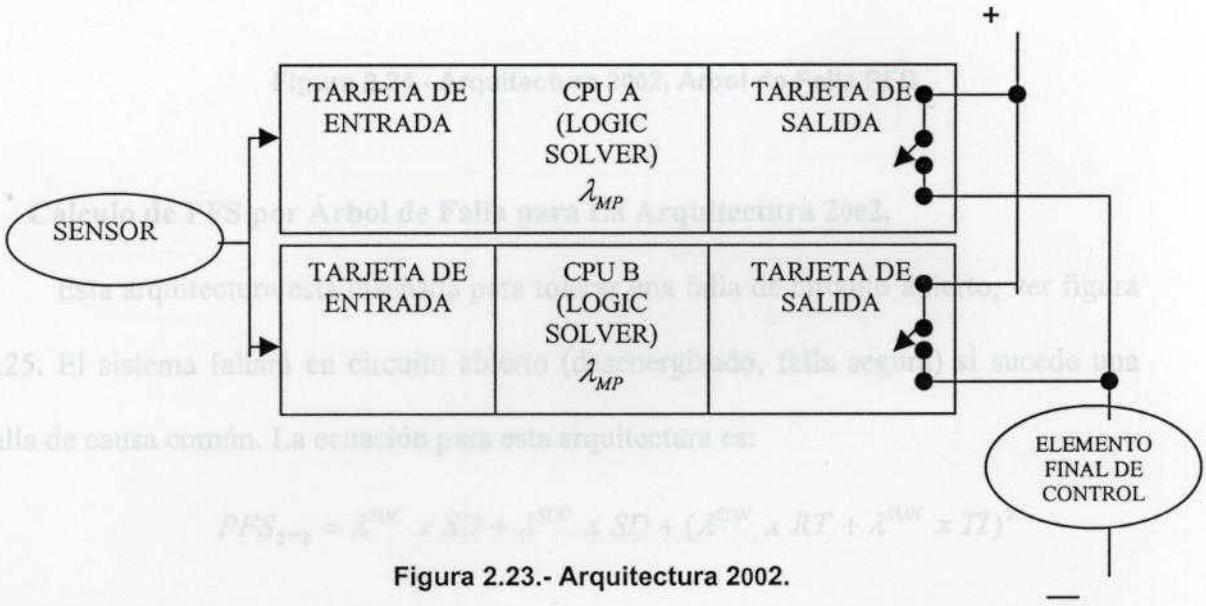


Figura 2.23.- Arquitectura 2002.

- **Cálculo de PFD Por Árbol de Falla para La Arquitectura 2002.**

Debido a que los controladores están conectados en paralelo, ver figura 2.24, cualquier falla de corto circuito de alguno de los componentes resultará en una falla peligrosa. La ecuación para esta configuración es la siguiente:

$$PFD_{Avg.2002} = \lambda^{DDC}\ x\ RT + \frac{\left(\lambda^{DUC}\ x\ TI\right)}{2} + 2\lambda^{DDN}\ x\ RT + \lambda^{DUN} x\ TI$$



Figura 2.24.- Arquitectura 2002, Árbol de Falla PFD.

- **Cálculo de PFS por Árbol de Falla para La Arquitectura 2002.**

Esta arquitectura esta diseñada para tolerar una falla de circuito abierto, ver figura 2.25. El sistema fallará en circuito abierto (desenergizado, falla segura) si sucede una falla de causa común. La ecuación para esta arquitectura es:

$$PFS_{2oo_2} = \lambda^{SDC} \, x \, SD + \lambda^{SUC} \, x \, SD + (\lambda^{SDN} \, x \, RT + \lambda^{SUN} \, x \, TI)^2$$

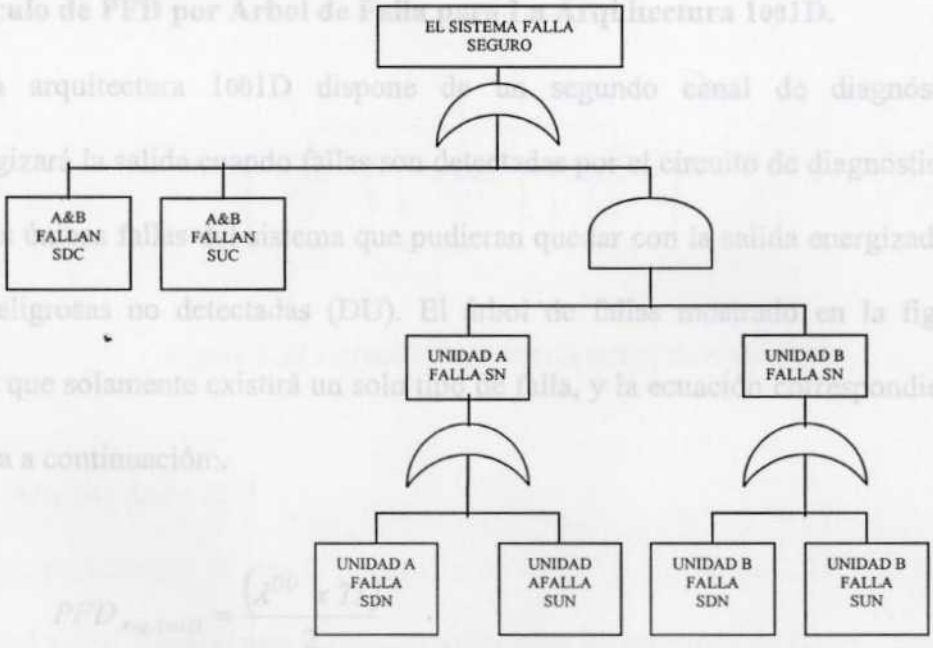


Figura 2.25.- Arquitectura 2002, Árbol de Falla PFS.

2.9.4. Arquitectura 1oo1D.

La arquitectura mostrada en la figura 2.26 utiliza un (1) solo controlador con capacidad de diagnóstico y un segundo canal de diagnóstico cableado en serie para utilizarla y desenergizar la salida.

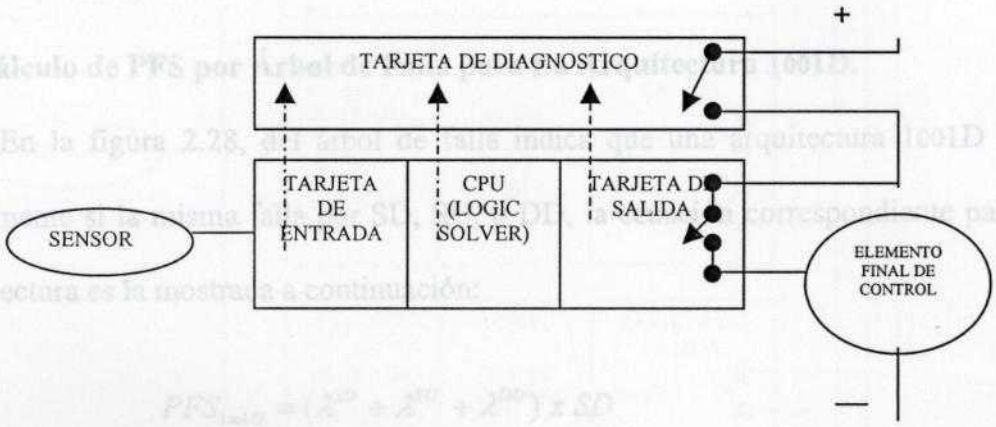


Figura 2.26.- Arquitectura 1oo1D.

- **Cálculo de PFD por Árbol de Falla para La Arquitectura 1oo1D.**

La arquitectura 1oo1D dispone de un segundo canal de diagnóstico que desenergizará la salida cuando fallas son detectadas por el circuito de diagnostico, por lo tanto, las únicas fallas del sistema que pudieran quedar con la salida energizada son las fallas peligrosas no detectadas (DU). El árbol de fallas mostrado en la figura 2.27 indicará que solamente existirá un solo tipo de falla, y la ecuación correspondiente es la mostrada a continuación:.

$$PFD_{Avg.1oo1D} = \frac{\left(\lambda^{DU} \; x \; TI\right)}{2}$$



Figura 2.27.- Arquitectura 1001D, Árbol de Falla PFD.

- **Cálculo de PFS por Árbol de Falla para La Arquitectura 1001D.**

En la figura 2.28, del árbol de falla indica que una arquitectura 1001D fallará únicamente si la misma falla por SD, SU, o DD, la ecuación correspondiente para esta arquitectura es la mostrada a continuación:

$$PFS_{1\infty 1D} = (\lambda^{SD} + \lambda^{SU} + \lambda^{DD})\, x\, SD$$



Figura 2.28.- Arquitectura 1001D, Árbol de Falla PFS.

2.9.5. Arquitectura 2003.

Esta arquitectura de dos (2) unidades de tres (3), ver figura 2.29, son requeridas para que el sistema opere, esta diseñada para tolerar las dos tipos de fallas: "peligrosa" y "segura", suministrando seguridad y una alta disponibilidad con las tres (3) unidades de

controladores.

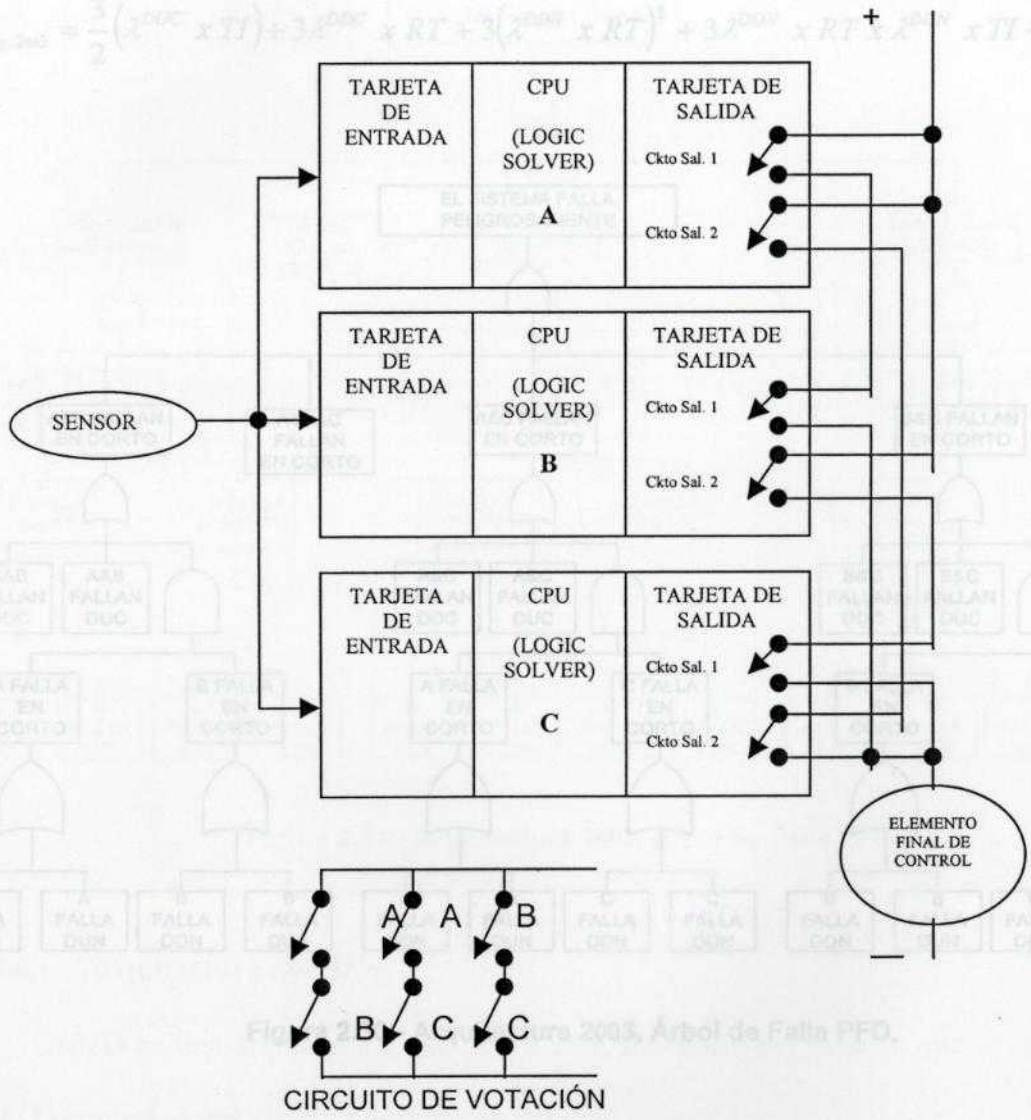


Figura 2.29.- Arquitectura 2003.

- **Cálculo de PFD por Árbol de Falla para La Arquitectura 2003.**

La arquitectura 2003 fallará peligrosamente si y solo si dos (2) ó las tres (3) unidades fallan en demanda. Existen cuatro (4) maneras de que esto suceda: Los circuitos A y B fallen, los circuitos A y C fallen, los circuitos B y C fallen, ó las cuatro circuitos fallen en corto. La ecuación aproximada para la PFD es derivada del árbol de

falla mostrado en la figura 2.30.

$$PFD_{Avg.2003} = \frac{3}{2}\left(\lambda^{DUC}\ x\ TI\right) + 3\lambda^{DDC}\ x\ RT + 3\left(\lambda^{DDN}\ x\ RT\right)^2 + 3\lambda^{DDN}\ x\ RT\ x\ \lambda^{DUN}\ x\ TI + \left(\lambda^{DUN}\ x\ TI\right)^2$$

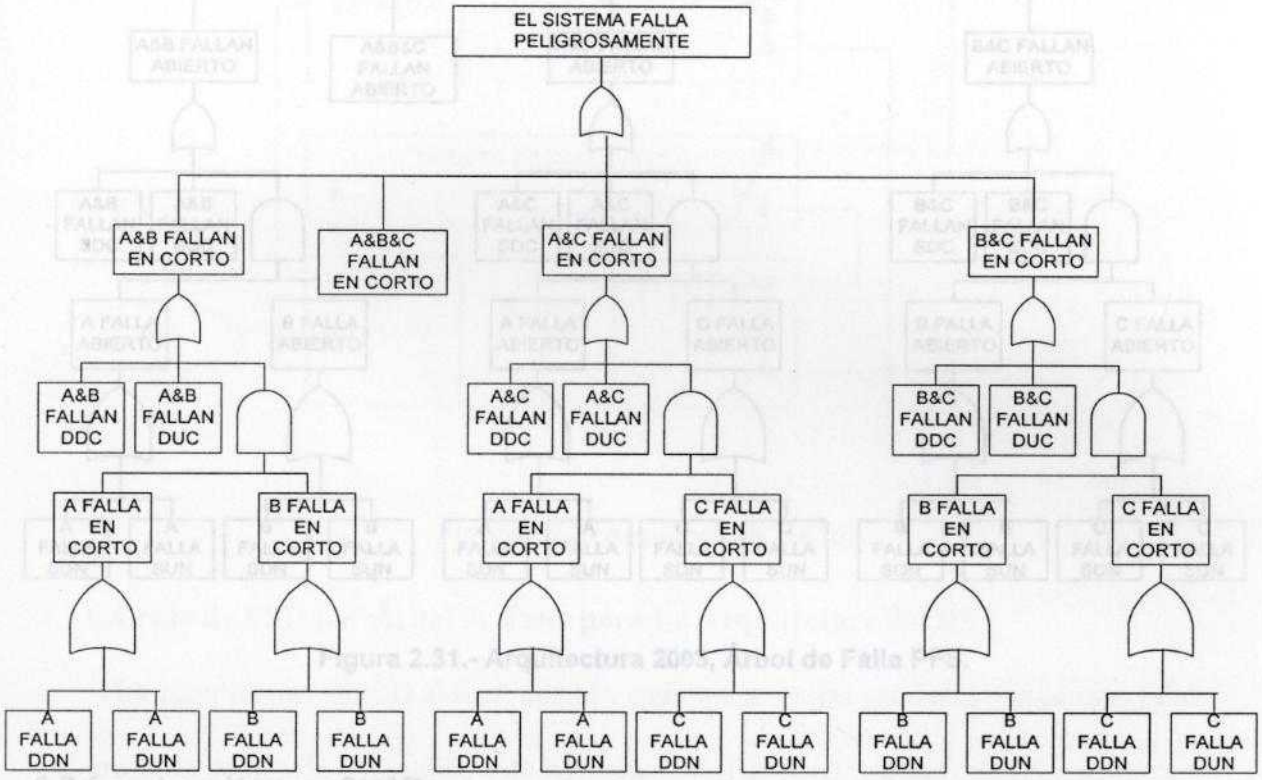


Figura 2.30.- Arquitectura 2003, Árbol de Falla PFD.

- **Cálculo de PFS por Árbol de Falla para La Arquitectura 2003.**

2003 es una arquitectura simétrica que tolera corto-circuitos como circuitos abiertos. Fallará seguro si y solo si dos (2) ó las tres (3) unidades fallan. Existen cuatro maneras de que esto suceda: Los circuitos A y B fallen, los circuitos A y C fallen, los circuitos B y C fallen, ó las cuatro circuitos fallen en circuito abierto. La ecuación aproximada para la PFS es derivada del árbol de falla mostrado en la figura 2.31.

$$PFS_{2\infty3} = 3\lambda^{SUC}\ x\ SD + 3\lambda^{SDC}\ x\ SD + 3(\lambda^{SDN}\ x\ RT + \lambda^{SUN}\ x\ TI)^2$$

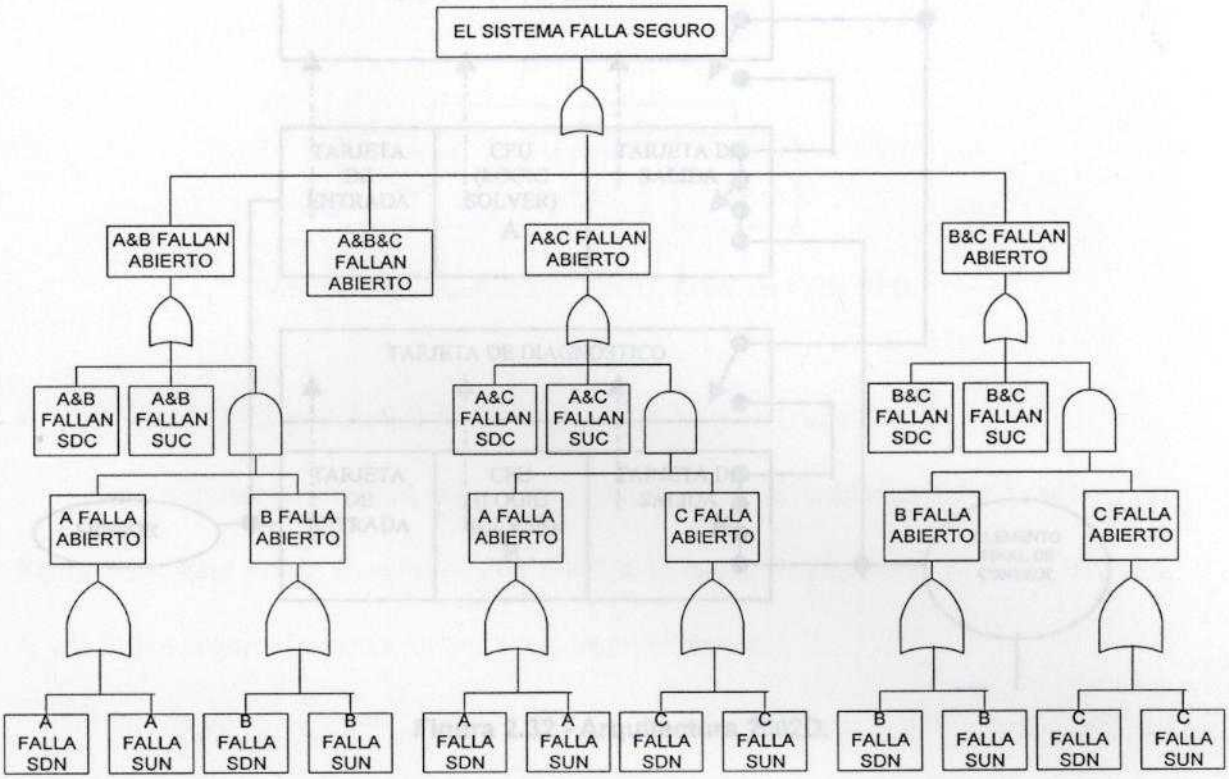


Figura 2.31.- Arquitectura 2003, Árbol de Falla PFS.

2.9.6. Arquitectura 2002D.

2002D es una arquitectura, ver figura 2.32, de cuatro (4) canales que consiste de dos (2) controladores 1001D cableados en paralelo.

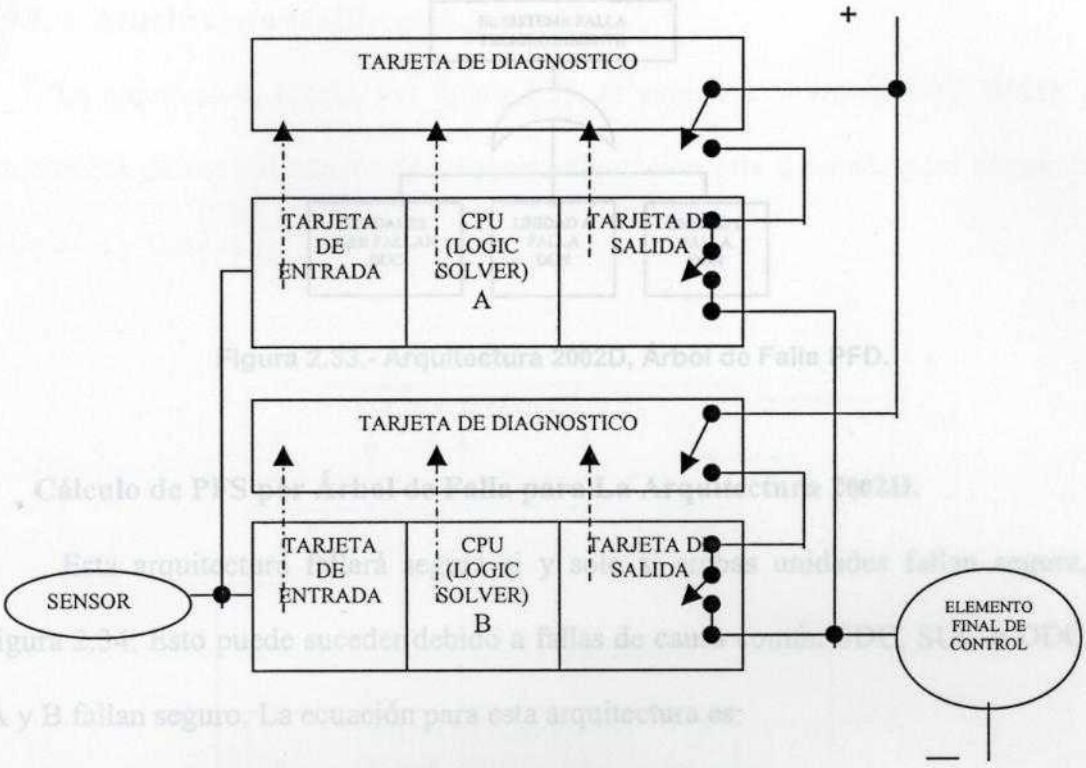


Figura 2.32.- Arquitectura 2002D.

- **Cálculo de PFD por Árbol de Falla para La Arquitectura 2002D.**

La arquitectura 2002D fallará cuando cualquiera de las unidades tenga una falla peligrosa no detectada y su salida esté energizada ó si el sistema tiene una falla peligrosa de causa común no detectada. La ecuación aproximada según el árbol de falla mostrada en la figura 2.33 es la siguiente:

$$PFD_{Avg.2oo2D} = \frac{\left(\lambda^{DUC} \; x \; TI\right)}{2} + \lambda^{DUN} \; x \; TI$$



Figura 2.33.- Arquitectura 2002D, Árbol de Falla PFD.

- **Cálculo de PFS por Árbol de Falla para La Arquitectura 2002D.**

Esta arquitectura fallará segura si y solo sí ambas unidades fallan segura, ver figura 2.34. Esto puede suceder debido a fallas de causa común SDC, SUC o DDC ó si A y B fallan seguro. La ecuación para esta arquitectura es:

$$PFS_{2oo2D} = (\lambda^{SDC} + \lambda^{SUC} + \lambda^{DDC})\ x\ SD + (\lambda^{SDN}\ x\ RT + \lambda^{DDN}\ x\ RT + \lambda^{SUN}\ x\ TI)^2$$

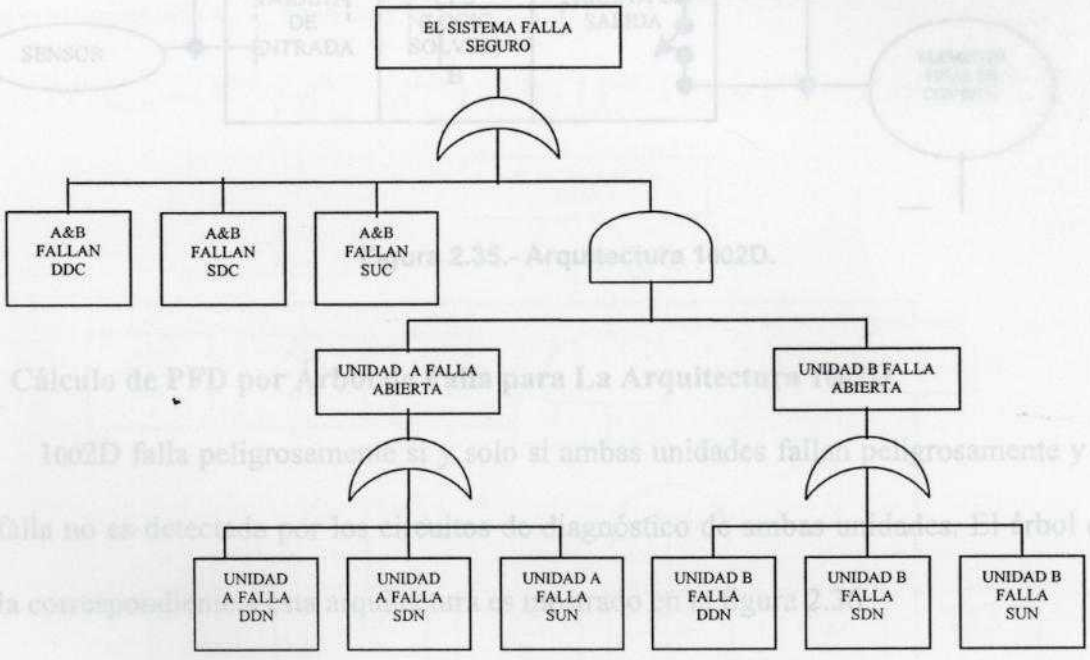


Figura 2.34.- Arquitectura 2002D, Árbol de Falla PFS.

2.9.7. Arquitectura 1002D.

La arquitectura 1002D, ver figura 2.35, es similar a la arquitectura 2002D, pero tiene líneas de control adicionales. Esta configuración esta diseñada para tolerar fallas peligrosas y seguras.

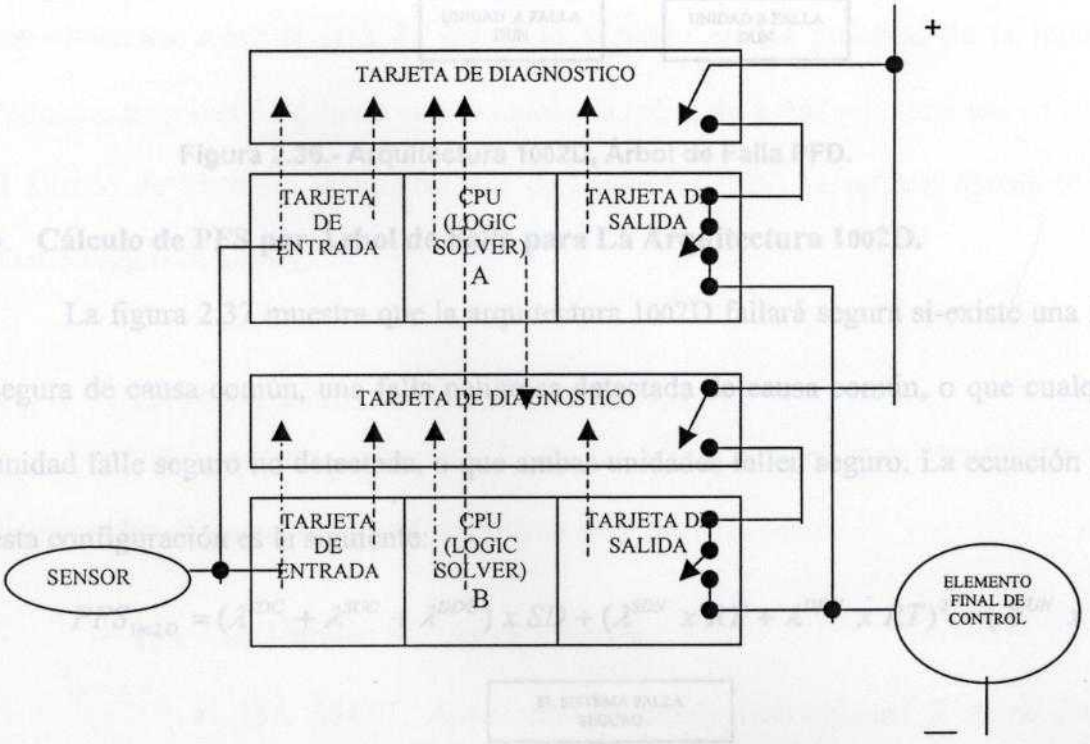


Figura 2.35.- Arquitectura 1002D.

- **Cálculo de PFD por Árbol de Falla para La Arquitectura 1002D.**

1002D falla peligrosamente si y solo si ambas unidades fallan peligrosamente y si la falla no es detectada por los circuitos de diagnóstico de ambas unidades. El árbol de falla correspondiente a esta arquitectura es mostrado en la figura 2.36.

$$PFD_{Avg.1002D} = \frac{\left(\lambda^{DUC}\ x\ TI\right)}{2} + \frac{(\lambda^{DUN}\ x\ TI)^2}{3}$$

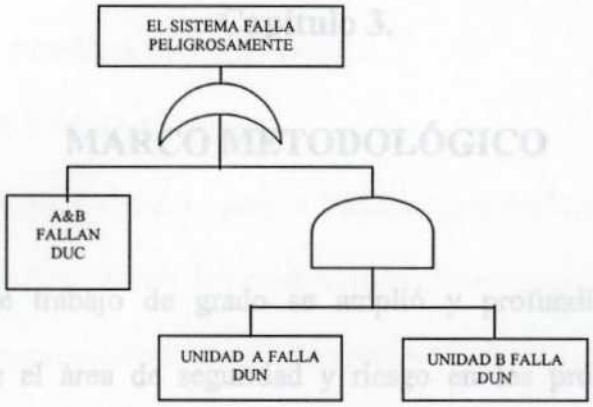


Figura 2.36.- Arquitectura 1002D, Árbol de Falla PFD.

- **Cálculo de PFS por Árbol de Falla para La Arquitectura 1002D.**

La figura 2.37 muestra que la arquitectura 1002D fallará segura si existe una falla segura de causa común, una falla peligrosa detectada de causa común, o que cualquier unidad falle seguro no detectada, o que ambas unidades fallen seguro. La ecuación para esta configuración es la siguiente:

$$PFS_{1\infty 2D} = (\lambda^{SDC} + \lambda^{SUC} + \lambda^{DDC})\ x\ SD + (\lambda^{SDN}\ x\ RT + \lambda^{DDN}\ x\ RT)^2 + (\lambda^{SUN}\ x\ TI)^2$$

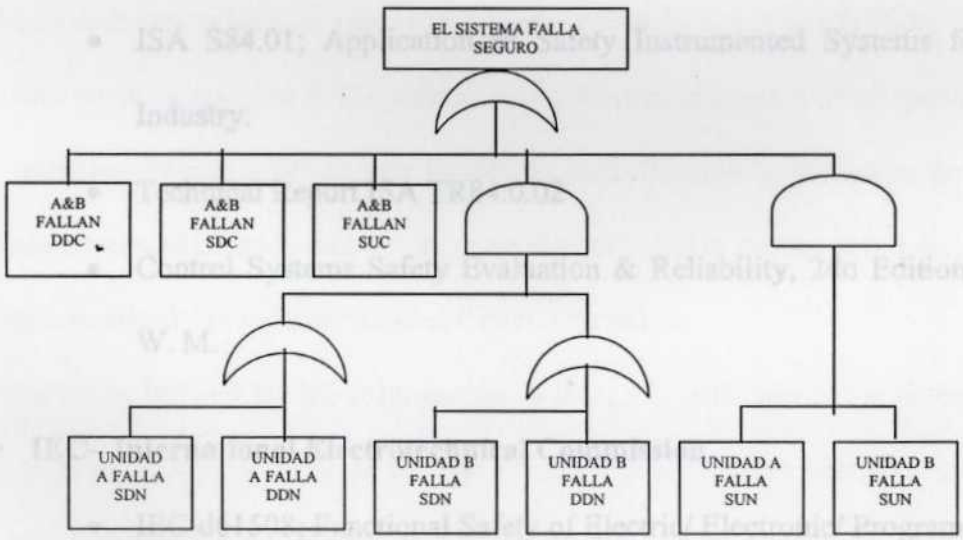


Figura 2.37.- Arquitectura 1002D, Árbol de Falla PFS.

Capítulo 3.

MARCO METODOLÓGICO

En el presente trabajo de grado se amplió y profundizó cada uno de los conocimientos sobre el área de seguridad y riesgo en los procesos de la Industria Petrolera, permitiendo generar una metodología aplicable a cualquier proceso en cuanto al Diseño de Sistemas Instrumentados de Seguridad (SIS) se refiere, obteniendo un diseño seguro de los SIS.

3.1. FUENTES Y TÉCNICAS RECOPILADAS.

El estudio, análisis e interpretación de las diferentes normas de seguridad para el diseño de los Sistemas de Seguridad Instrumentados, tales como:

- **ISA – Instrument Society of America**
  - ISA S84.01; Application of Safety Instrumented Systems for the Process Industry.
  - Technical Report ISA TR84.0.02
  - Control Systems Safety Evaluation & Reliability, 2do Edition, 1998. Globe, W. M.
- **IEC– International Electrotechnical Commission**
  - IEC-d61508; Functional Safety of Electric/ Electronic/ Programmable Electronic Systems.

- **PDVSA - Petróleos de Venezuela.**
  - IR-S-00 Definiciones
  - IR-S-02 Criterios para el Análisis Cuantitativo de Riesgos
  - IR-P-01 Safety Interlock Systems,Emergency Isolation, Emergency Despressurization and Emergency Venting Systems.
- **CCPS – Center for Chemical Process Safety.**
  - Guidelines for Safe Automation of Chemical Processes.

Generó la comparación de los distintos métodos cualitativos y cuantitativos que determinan el Índice de Integridad especifico del proceso, para el diseño de un Sistema Instrumentado de Seguridad óptimo y seguro. En este aspecto el aporte y desarrollado de estas instituciones de investigación en el campo del control de procesos, ha logrado una importante representación de los SIS en los procesos industriales. Permitiendo la adaptación de dichas normas a las especificaciones y requerimientos de PDVSA.

Por otra parte, la revisión de las normas y documentos existentes en la empresa permitió establecer bases teóricas que facilitó la identificación y ubicación de la problemática presentada, dando una observación directa sobre la misma con respecto al sitio donde se construirá y desarrollará el Centro Operativo.

El empleo de Internet facilitó información reciente y actualizada de los sistemas de seguridad y las graves consecuencias que han causado los accidentes ocurridos en otras latitudes por la no-existencia o mal diseño de los SIS, lo cual llevó a contactar a compañías extranjeras fabricantes de equipos y diseñadores de Sistemas Instrumentados

de Seguridad, con el fin de obtener la información más consistente para este trabajo. Las paginas de mayor interés se mencionan a continuación:

- http://www.isa.org
- http://www.aiche.org
- http://www.factorymutual.com

Se desarrollaron entrevistas al personal del área de Seguridad y Riesgo de la Planta, específicamente al Grupo Técnico de Trabajo (GTT), para conocer la evolución de los conceptos de protección y criterios de seguridad tomados en cuenta en el diseño del Manual de Ingeniería y Diseño de PDVSA, Volumen 9 de Instrumentación.

3.2. TRATAMIENTO DE LA INFORMACIÓN.

Con las técnicas de recolección anteriormente descritas se recopilaron los datos necesarios para diseñar el Sistema Instrumentado de Seguridad del Centro Operativo, realizando los análisis que encierra la problemática del diseño de los Sistemas de Seguridad en la Industria Petrolera Nacional; por el hecho de que los mismos siempre se han diseñado de una forma cualitativa a la hora de estimar el nivel de riesgo de las plantas.

3.3. DISEÑO DE LA INVESTIGACIÓN.

Esta metodología se realizó de forma genérica para que pueda ser aplicable a cualquier proceso, y cada uno de los puntos tratados e investigados en los diferentes capítulos contribuyó al desarrollo y diseño final del Diagrama para la Determinación del SIL de los SIS. Cabe señalar que la determinación del SIL de los SIS, implica el

cálculo de las diferentes arquitecturas o diseños de los Sistemas Instrumentados de Seguridad, realizando para ello un programa que permite obtener todas las combinaciones o diseños que cumplan con el SIL requerido por el proceso y que ha sido reflejado dentro del diseño del sistema. A continuación se presenta el diseño obtenido, el cual será descrito en detalle más adelante:

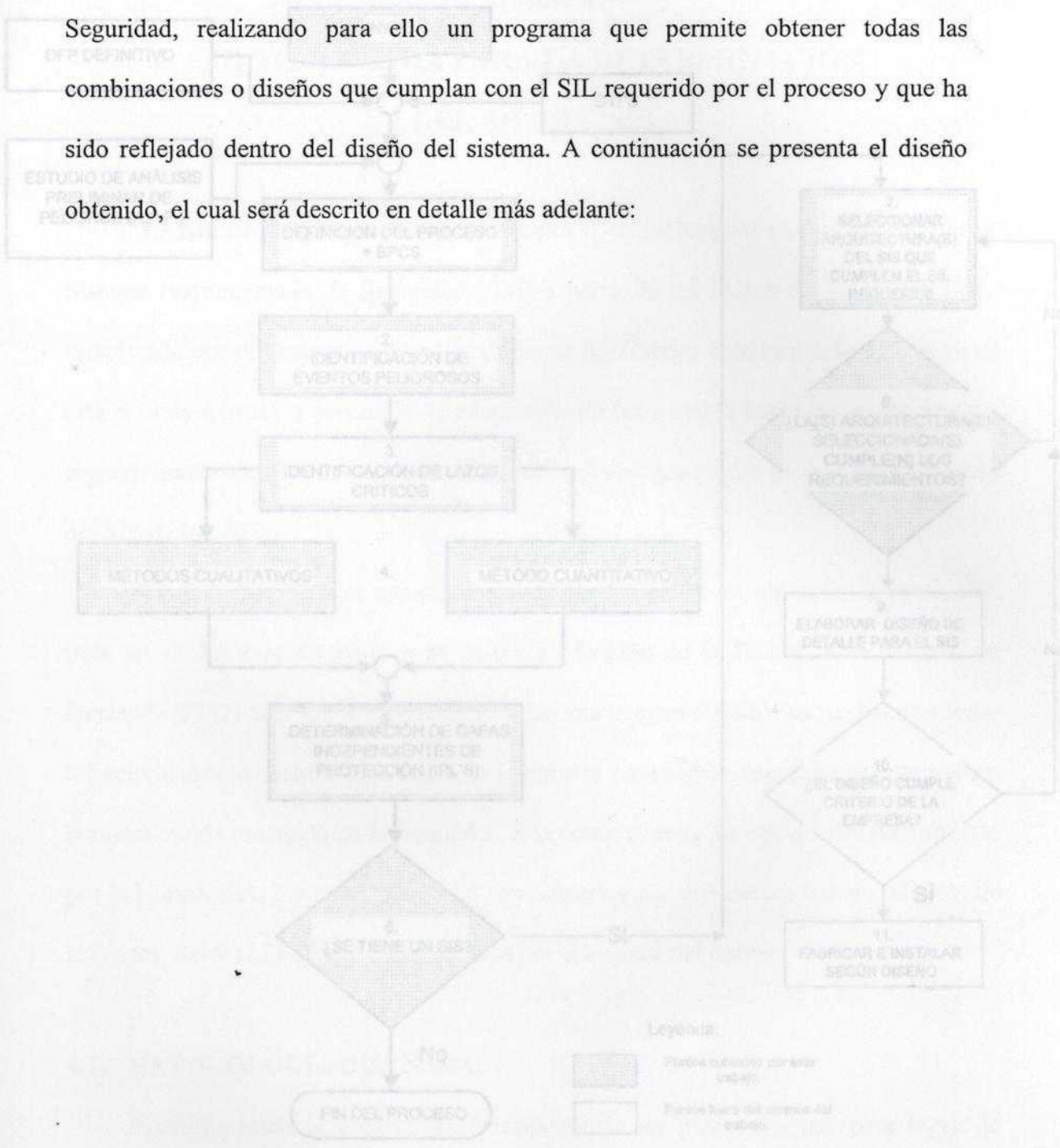


Figura 3.1.- Metodología para la Determinación del SIL de los SIS.

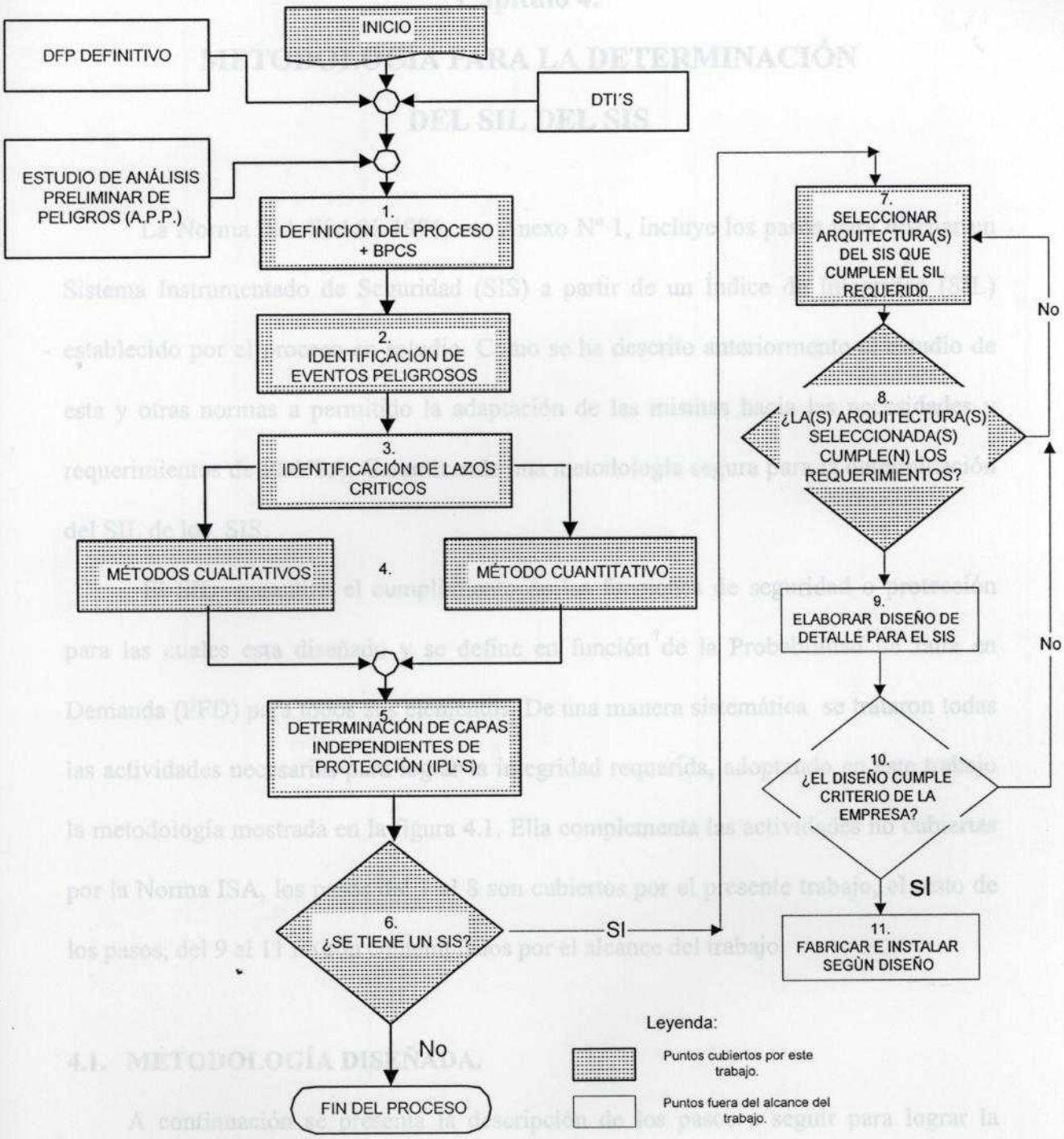


Figura 3.1.- Metodología para la Determinación del SIL de los SIS.

Capítulo 4.

METODOLOGÍA PARA LA DETERMINACIÓN DEL SIL DEL SIS

La Norma ISA-S84.01-1996, ver Anexo Nº 1, incluye los pasos para diseñar un Sistema Instrumentado de Seguridad (SIS) a partir de un Índice de Integridad (SIL) establecido por el proceso en estudio. Como se ha descrito anteriormente el estudio de esta y otras normas a permitido la adaptación de las mismas hacia las necesidades y requerimientos de PDVSA. Garantizando una metodología segura para la determinación del SIL de los SIS.

El SIL garantiza el cumplimiento de las funciones de seguridad o protección para las cuales esta diseñado y se define en función de la Probabilidad de falla en Demanda (PFD) para todos sus elementos. De una manera sistemática se trataron todas las actividades necesarias para lograr la integridad requerida, adoptando en este trabajo la metodología mostrada en la figura 4.1. Ella complementa las actividades no cubiertas por la Norma ISA, los pasos del 1 al 8 son cubiertos por el presente trabajo, el resto de los pasos, del 9 al 11 no son contemplados por el alcance del trabajo.

4.1. METODOLOGÍA DISEÑADA.

A continuación se presenta la descripción de los pasos a seguir para lograr la consecución de los objetivos, ver figura 4.1.

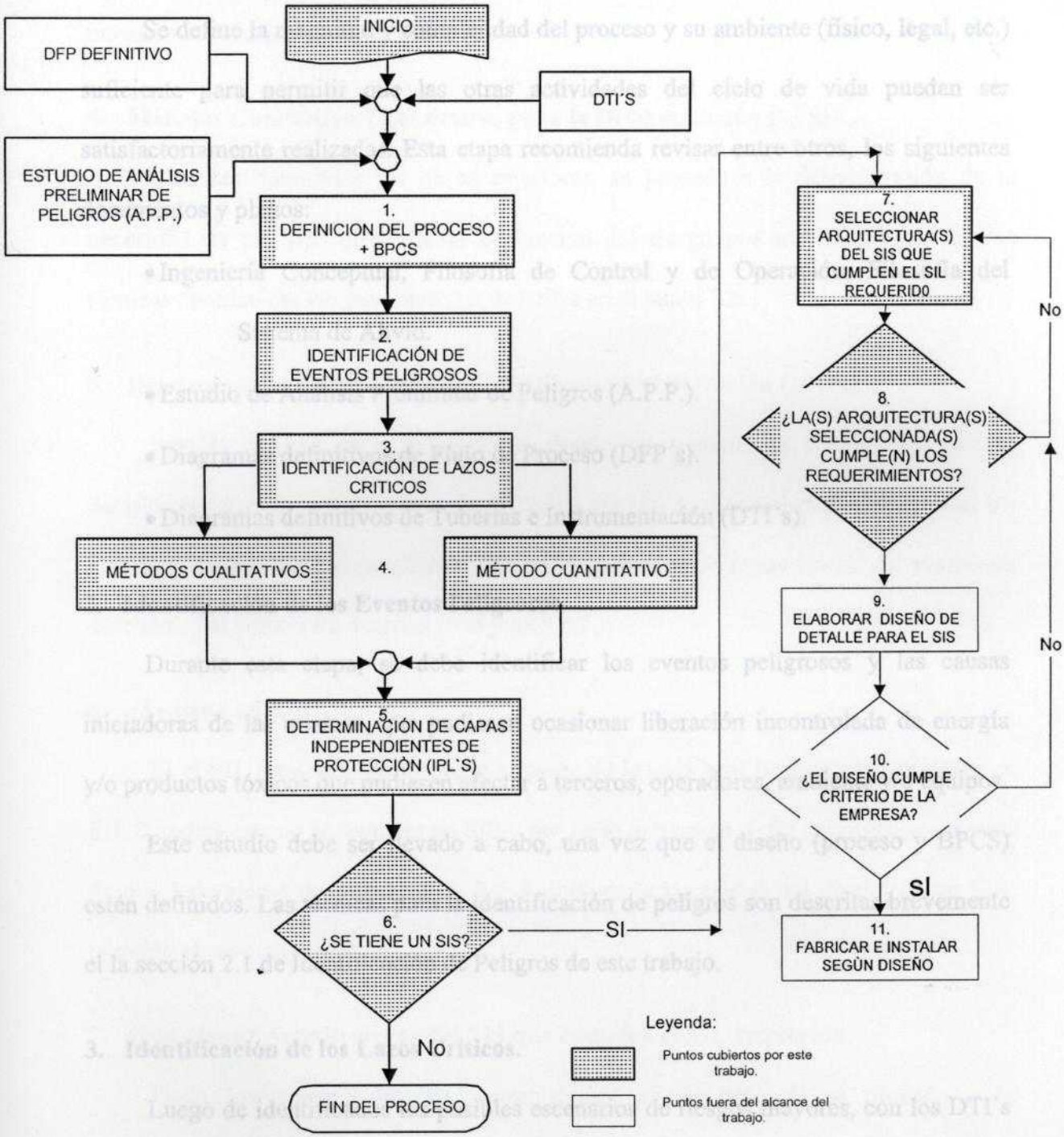


Figura 4.1.- Metodología para la Determinación del SIL de los SIS

1. Definición del Proceso.

Se define la magnitud y complejidad del proceso y su ambiente (físico, legal, etc.) suficiente para permitir que las otras actividades del ciclo de vida puedan ser satisfactoriamente realizadas. Esta etapa recomienda revisar entre otros, los siguientes documentos y planos:

- Ingeniería Conceptual, Filosofía de Control y de Operación, Filosofía del Sistema de Alivio.
- Estudio de Análisis Preliminar de Peligros (A.P.P.).
- Diagramas definitivos de Flujo de Proceso (DFP´s).
- Diagramas definitivos de Tuberías e Instrumentación (DTI´s).

2. Identificación de los Eventos Peligrosos.

Durante esta etapa, se debe identificar los eventos peligrosos y las causas iniciadoras de las mismas, que pudiesen ocasionar liberación incontrolada de energía y/o productos tóxicos que pudiesen afectar a terceros, operadores, ambiente y/o equipos.

Este estudio debe ser llevado a cabo, una vez que el diseño (proceso y BPCS) estén definidos. Las técnicas para la identificación de peligros son descritas brevemente el la sección 2.1 de Identificación de Peligros de este trabajo.

3. Identificación de los Lazos Críticos.

Luego de identificados los posibles escenarios de riesgos mayores, con los DTI`s y DFP`s de la planta, se hace un estudio minucioso de todos los lazos de control con la finalidad de determinar los lazos críticos en los cuales las desviaciones de las variables de control (temperatura, nivel presión, etc.) pueden generar posibles eventos no

deseables y acarrear potenciales accidentes que de uno u otra forma repercuten en el normal funcionamiento de la planta.

4. Métodos Cualitativo/Cuantitativo para la Determinación del SIL.

Una vez cumplidos los pasos anteriores, se procede a la determinación de la necesidad de un SIS, mediante la evaluación del riesgo por medio del uso de las técnicas cualitativas y/o cuantitativas, descritas en el punto 2.6.

5. Determinación de las Capas Independientes de Protección (IPL`s).

Para la configuración del proceso, donde sea posible, es conveniente aplicar decisiones para una mayor reducción de riesgo vía IPL`s adicionales. Se listan todas las Capas de Protección Independientes que podrían prevenir la causa inicial del evento no deseado. Tal como esta descrito en el punto 2.7.

6. ¿Se tiene un SIS?.

Si el SIL requerido del proceso a través de los cálculos hechos anteriormente es SIL 0, indica que no se requiere un SIS y por tanto determina el fin del proceso, en caso de que los valores del SIL sean 1, 2 ó 3, indican la necesidad del diseño de un SIS, pasando al paso siguiente.

7. Seleccionar Arquitecturas del SIS que cumplen el SIL requerido.

Dado los valores del SIL suministrado por el paso 4, se procede a la determinación y selección de las arquitecturas del SIS que cumplan con estos valores requeridos del proceso, utilizando la herramienta desarrollada para ello (software), para todos los lazos críticos identificados en el paso 3.

8. ¿La(s) Arquitecturas Seleccionada(s) Cumple(n) los Requerimientos?.

En base a los requerimientos y normas de la empresa, debe verificarse que las arquitecturas seleccionadas cumplan los mismos, en caso de que no cumplan, se debe regresar al paso anterior.

9, 10 y 11.

Estos pasos quedan fuera del alcance de este trabajo, y representan el desarrollo e implantación final del SIS.

4.2. DISEÑO, VERIFICACIÓN Y VALIDACIÓN DEL SIS.

El SIS debe ser diseñado y configurado para lograr el SIL requerido por el proceso en estudio. Como tal, el PFD del SIS debe estar aproximado en el rango especificado por el SIL requerido. El diseño del SIS se logra utilizando el programa "DISEÑO-SIS.XLS", el cual esta basado en las ecuaciones utilizadas para el cálculo de las correspondientes arquitecturas del SIS. Corre bajo Plataformas Win 9x, Win NT4.0 y versiones superiores a estos. Esta constituido por cinco (5) hojas de cálculo de Microsoft Excel (Versión Office 97) las cuales son de fácil manejo para el diseñador:

- **Sensores.**

En esta hoja, ver figura 4.2, se calcula la PFD y la PFS de los diferentes arreglos de sensores posibles (1001, 1002, 2002, 2003, 1001D, 1002D y 2002D) en base a la data de entrada requerida y que es solicitada en la misma hoja. Los cálculos son realizados en base a las ecuaciones de cada arreglo y los resultados de los mismos son mostrados.

- **Controladores CPU (Logic Solvers).**

En esta hoja, ver figura 4.3, se calcula la PFD y la PFS de los diferentes arreglos de controladores posibles (1001, 1002, 2002, 2003, 1001D, 1002D y 2002D) en base a la data de entrada requerida y que es solicitada en la misma hoja. Los cálculos son realizados en base a las ecuaciones de cada arreglo y los resultados de los mismos son mostrados.

- **Elementos Finales de Control (Válvulas).**

Las opciones consideradas en esta hoja, ver figura 4.4, son: una simple válvula de cierre (configuración 1001) y dos válvulas de seguridad (shutoff) en serie (configuración 1002), la data requerida es introducida en la misma hoja de cálculo. Los cálculos son realizados en base a las ecuaciones de cada arreglo y los resultados de los mismos son mostrados.

- **Tabla Resumen.**

La figura 4.5, muestra una hoja con el resumen de los resultados (PFD, RRF, PFS y el SIL) de todas las posibles combinaciones de las diferentes configuraciones posibles de los arreglos de Sensores-Controladores-Válvulas (en ella aparecen 40 posibles combinaciones). Se incluye un botón selector del SIL requerido, el cual permite iluminar la combinación que cumpla el desempeño.

- **Comparación.**

En esta hoja de cálculo, ver figura 4.6, se muestra una gráfica de comparación de todas las posibles combinaciones de las diferentes configuraciones posibles.

4.3. TABLAS DE TÉRMINOS Y RANGOS SUGERIDOS.

A continuación se muestran todos los términos, unidades y rangos sugeridos, necesarios para el diseño del SIS a través del software mencionado. Para los Sensores, ver tabla 4.1, Controladores (Logic Solvers), ver tabla 4.2 y para los Elementos Finales de Control (Válvulas), ver tabla 4.3.

Término	Unidades	Rangos del Parámetro Sugeridos
Cantidad	C/u	Cantidad de elementos sensores.
MTTF	Tiempo Promedio entre Fallas (Años)	MTTF= $1/\lambda \; x \; 8760$ (Aproximación)
% Fail Safe (Falla Segura)	Porcentaje de Probabilidad de Falla Segura	Se asume como primera aproximación: 50% de falla segura y 50% de falla peligrosa.
DC	Factor de Diagnóstico Automático (%)	0%, 60%, 90% y 99%
TI	Tiempo Promedio de Pruebas Manuales, validado por mantenimiento y operaciones (Horas)	1 Mes (730 horas) Para procesos de alta demanda o modos de uso continuo. 3 Meses (2.190 horas) Para procesos de alta demanda o modos de uso continuo. 6 Meses (4.380 horas) **1 Año (8.760 horas).** 2 Años (17.520 horas) Para procesos de baja demanda 10 Años (87.600 horas) Para procesos de baja demanda
MTTR	Tiempo Promedio para Reparación (horas)	**8 horas**
β	Factor de Causa Común	1%, **5%**, 10% Se asume $\beta = 2 \times \beta_D$
SD	Tiempo promedio para el arranque del proceso despues de una parada (horas)	**24 horas**

Tabla 4.1.- Data típica para los Sensores.

Término	Entradas Digitales	Salidas Digitales	Entradas Analógicas	CPU	Rangos del Parámetro
Cantidad	c/u	c/u	c/u	No Aplica	Se indica la cantidad de I/O(s)
MTTF (Mean Time to Failure)	Años	Años	Años	Años	MTTF= $1/\lambda \times 8760$ (Aproximación)
% Fail Safe (% Falla Segura)	% Fail Safe$_{DI}$	% Fail Safe$_{DO}$	% Fail Safe$_{AI}$	% Fail Safe$_{CPU}$	Se asume como primera aproximación: 50% de falla segura y 50% de falla peligrosa.
DC (Diagnostic Coverage)	DC$_{DI}$	DC$_{DO}$	DC$_{AI}$	DC$_{CPU}$	Factor de Diagnostico
Common Cause Beta Factor (β)	β_{DI}	β_{DO}	β_{AI}	β_{CPU}	Factor Beta de Falla de Causa Común.
MTTR (Mean Time to Repair)	No Aplica	No Aplica	No Aplica	MTTR$_{CPU}$	Tiempo Promedio para Reparación (horas) Se asume: **8 Horas**
T_1	No Aplica	No Aplica	No Aplica	$T_{1\ CPU}$	Tiempo Promedio de Pruebas Manuales, validado por mantenimiento y operaciones (Horas) Se asume: **8760 Horas** (un año).
SD	No Aplica	No Aplica	No Aplica	SD	Tiempo promedio para el arranque del proceso despues de una parada (horas) Se asume: **24 Horas.**

Tabla 4.2.- Data típica para el Controlador CPU (Logic Solver).

Término	Unidades	Rangos del Parámetro Sugeridos
Cantidad	C/u	Cantidad de Válvulas o elementos de salida.
MTTF	Tiempo Promedio entre Fallas (Años)	MTTF= $1/\lambda \; x \; 8760$ (Aproximación)
% Fail Safe (Falla Segura)	Porcentaje de Probabilidad de Falla Segura	Se asume como primera aproximación: 50% de falla segura y 50% de falla peligrosa.
DC	Factor de Diagnóstico Automático (%)	0%, 60%, 90% y 99%. Se asume **DC = 0%**
T_1	Tiempo Promedio de Pruebas Manuales, validado por mantenimiento y operaciones (Horas)	1 Mes (730 horas) Para procesos de alta demanda o modos de uso continuo. 3 Meses (2.190 horas) Para procesos de alta demanda o modos de uso continuo. 6 Meses (4.380 horas) **1 Año (8.760 horas).** 2 Años (17.520 horas) Para procesos de baja demanda 10 Años (87.600 horas) Para procesos de baja demanda
MTTR	Tiempo Promedio para Reparación (horas)	**8 horas**
β	Factor de Causa Común	1%, **5%**, 10% Se asume β = **2 x** β_D
SD	Tiempo promedio para el arranque del proceso despues de una parada (horas)	**24 horas**

Tabla 4.3.- Data típica para los Elementos Finales de Control (Válvulas).

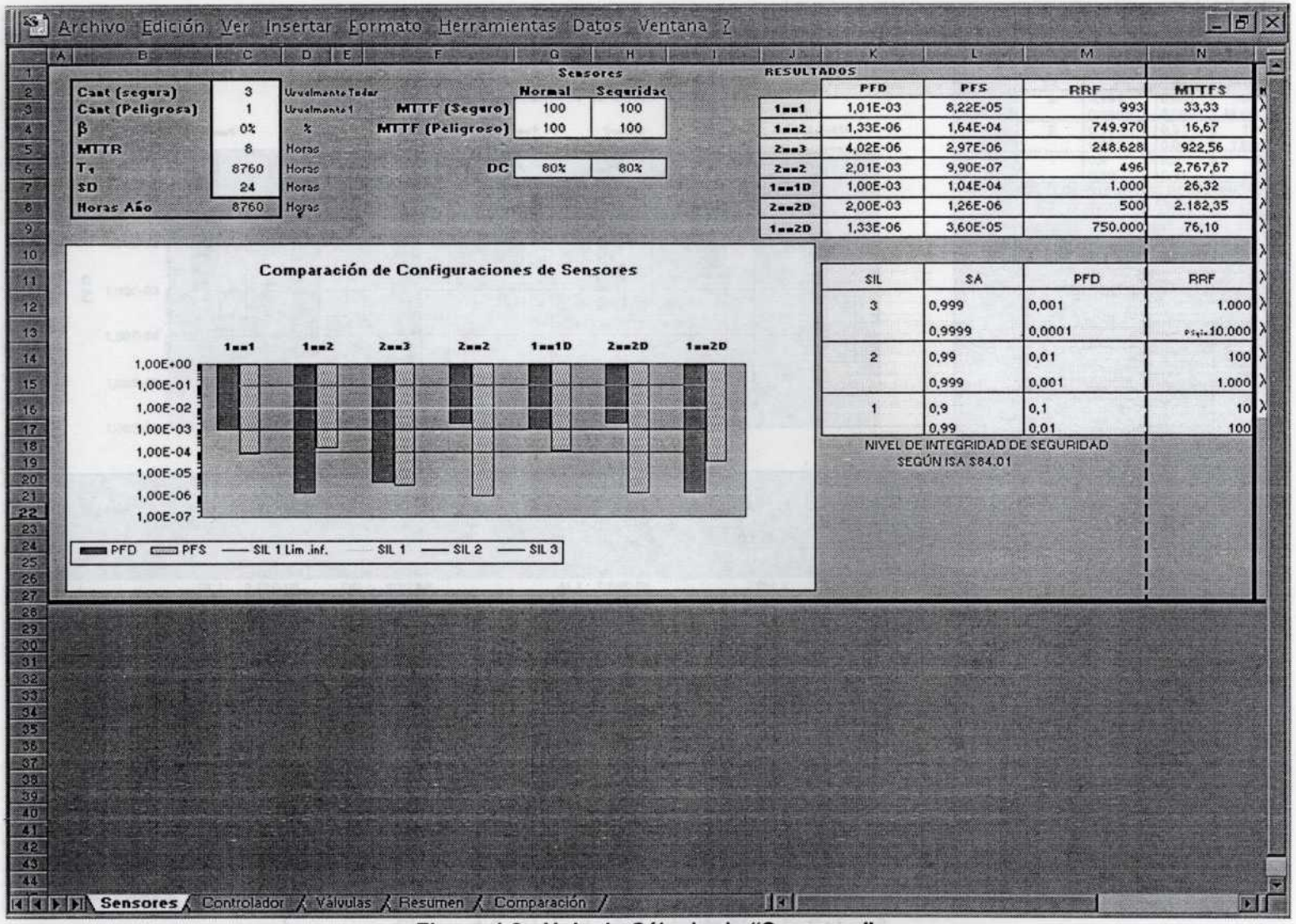


Figura 4.2.- Hoja de Cálculo de "Sensores".

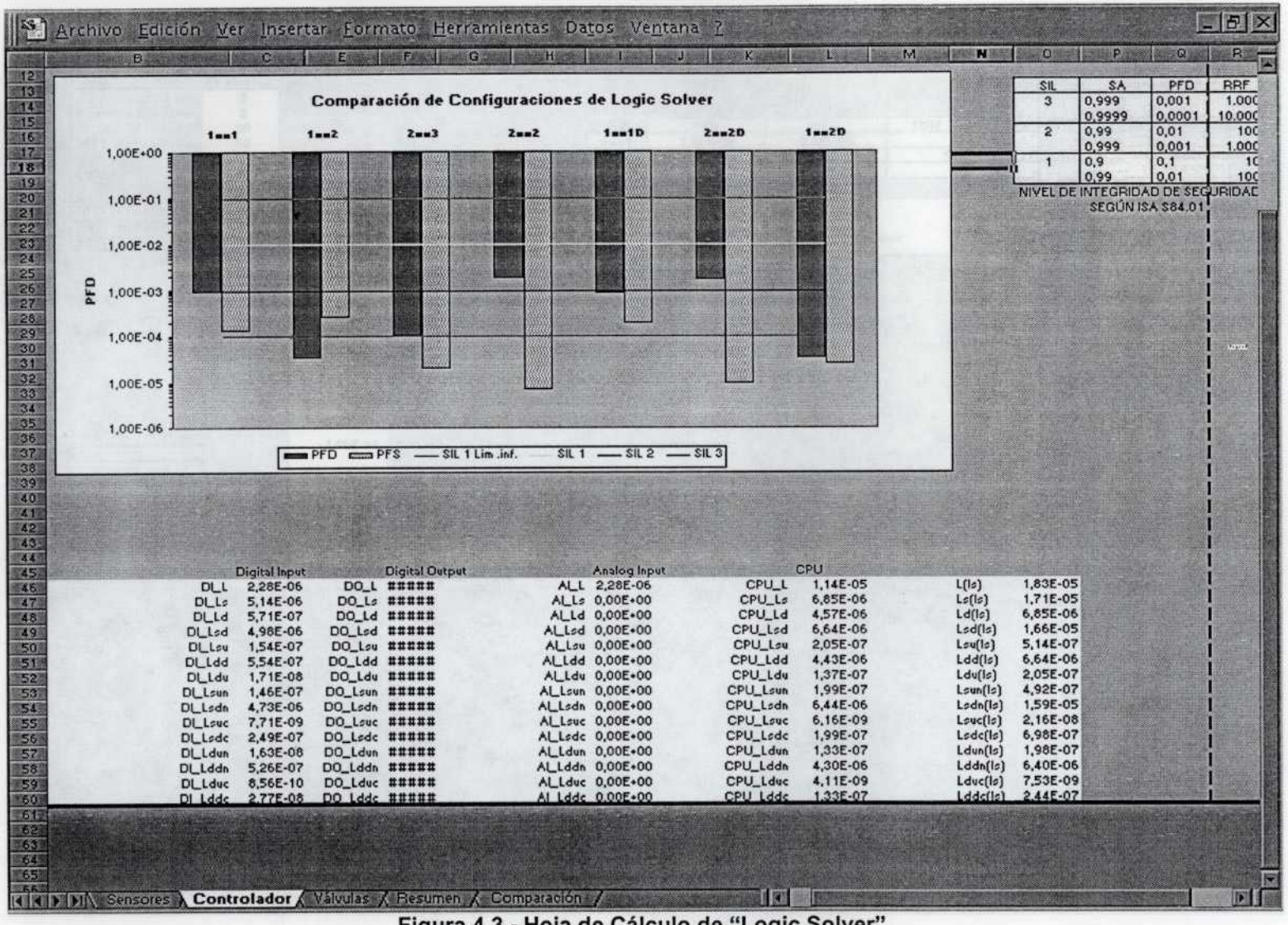


Figura 4.3.- Hoja de Cálculo de "Logic Solver".

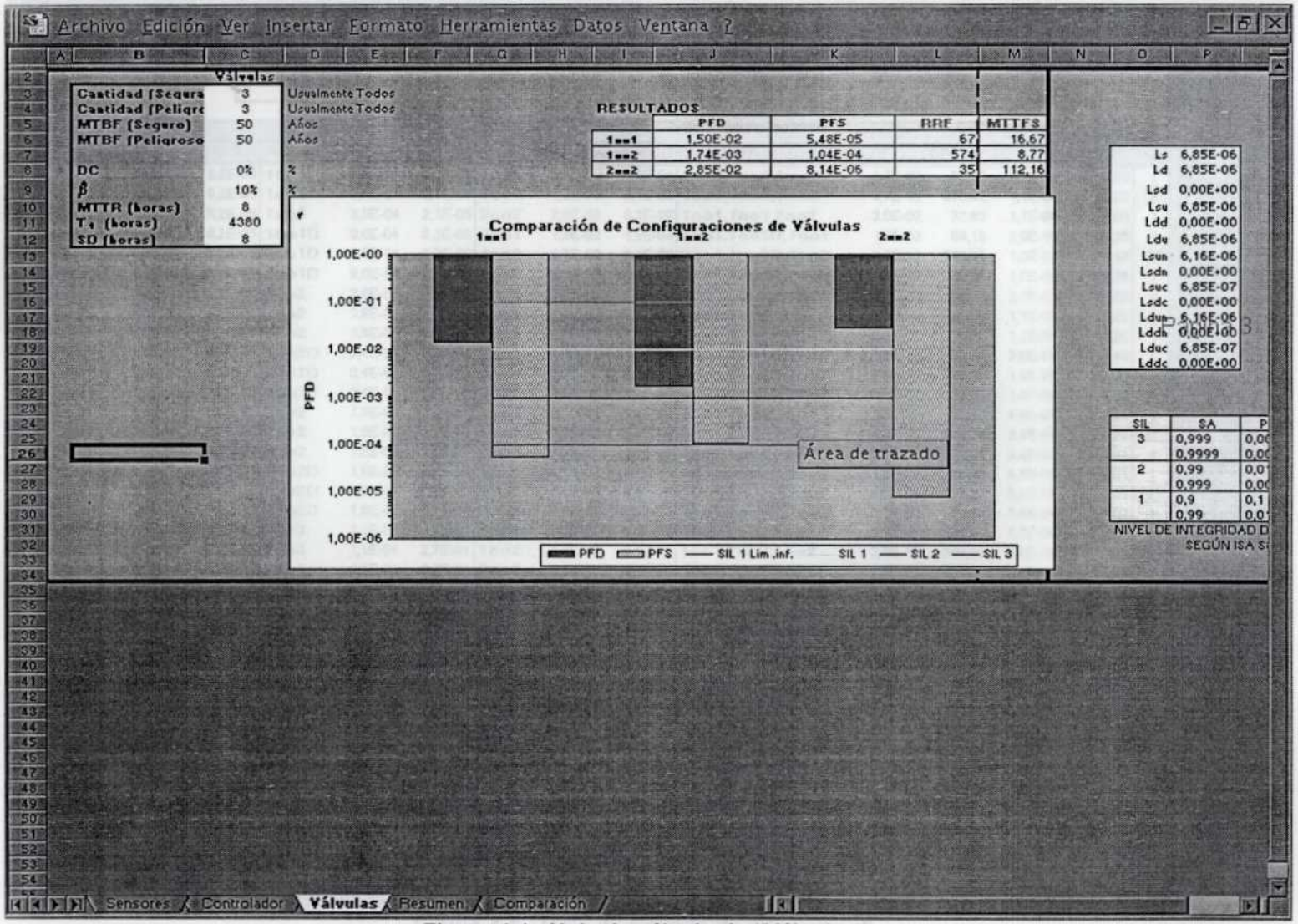
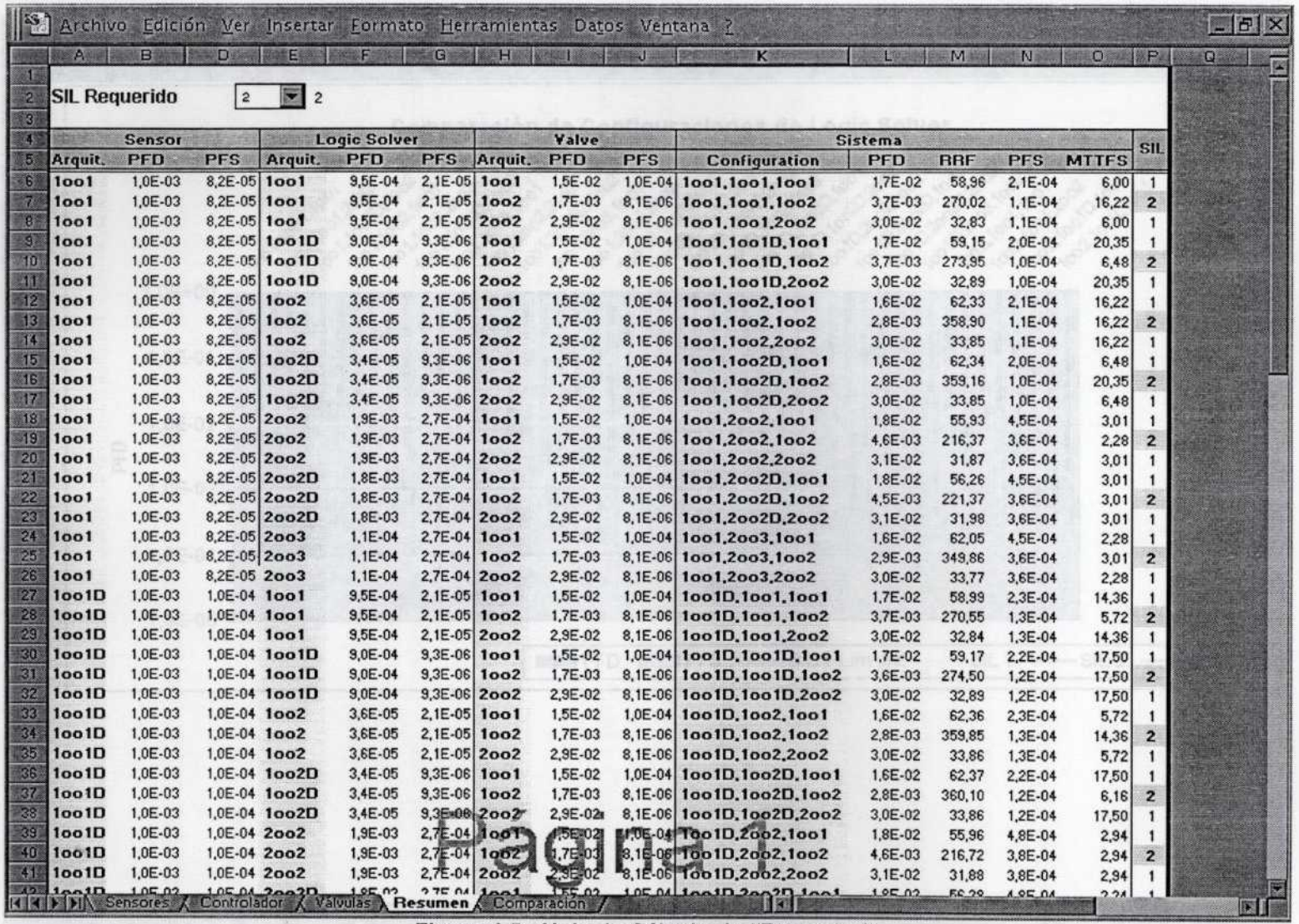


Figura 4.4.- Hoja de cálculo de "Válvulas".



Archivo Edición Ver Insertar Formato Herramientas Datos Ventana ?

SIL Requerido 2 2

	Sensor			Logic Solver			Valve			Sistema					SIL
	Arquit.	PFD	PFS	Arquit.	PFD	PFS	Arquit.	PFD	PFS	Configuration	PFD	RRF	PFS	MTTFS	
6	1oo1	1,0E-03	8,2E-05	1oo1	9,5E-04	2,1E-05	1oo1	1,5E-02	1,0E-04	1oo1,1oo1,1oo1	1,7E-02	58,96	2,1E-04	6,00	1
7	1oo1	1,0E-03	8,2E-05	1oo1	9,5E-04	2,1E-05	1oo2	1,7E-03	8,1E-06	1oo1,1oo1,1oo2	3,7E-03	270,02	1,1E-04	16,22	2
8	1oo1	1,0E-03	8,2E-05	1oo1	9,5E-04	2,1E-05	2oo2	2,9E-02	8,1E-06	1oo1,1oo1,2oo2	3,0E-02	32,83	1,1E-04	6,00	1
9	1oo1	1,0E-03	8,2E-05	1oo1D	9,0E-04	9,3E-06	1oo1	1,5E-02	1,0E-04	1oo1,1oo1D,1oo1	1,7E-02	59,15	2,0E-04	20,35	1
10	1oo1	1,0E-03	8,2E-05	1oo1D	9,0E-04	9,3E-06	1oo2	1,7E-03	8,1E-06	1oo1,1oo1D,1oo2	3,7E-03	273,95	1,0E-04	6,48	2
11	1oo1	1,0E-03	8,2E-05	1oo1D	9,0E-04	9,3E-06	2oo2	2,9E-02	8,1E-06	1oo1,1oo1D,2oo2	3,0E-02	32,89	1,0E-04	20,35	1
12	1oo1	1,0E-03	8,2E-05	1oo2	3,6E-05	2,1E-05	1oo1	1,5E-02	1,0E-04	1oo1,1oo2,1oo1	1,6E-02	62,33	2,1E-04	16,22	1
13	1oo1	1,0E-03	8,2E-05	1oo2	3,6E-05	2,1E-05	1oo2	1,7E-03	8,1E-06	1oo1,1oo2,1oo2	2,8E-03	358,90	1,1E-04	16,22	2
14	1oo1	1,0E-03	8,2E-05	1oo2	3,6E-05	2,1E-05	2oo2	2,9E-02	8,1E-06	1oo1,1oo2,2oo2	3,0E-02	33,85	1,1E-04	16,22	1
15	1oo1	1,0E-03	8,2E-05	1oo2D	3,4E-05	9,3E-06	1oo1	1,5E-02	1,0E-04	1oo1,1oo2D,1oo1	1,6E-02	62,34	2,0E-04	6,48	1
16	1oo1	1,0E-03	8,2E-05	1oo2D	3,4E-05	9,3E-06	1oo2	1,7E-03	8,1E-06	1oo1,1oo2D,1oo2	2,8E-03	359,16	1,0E-04	20,35	2
17	1oo1	1,0E-03	8,2E-05	1oo2D	3,4E-05	9,3E-06	2oo2	2,9E-02	8,1E-06	1oo1,1oo2D,2oo2	3,0E-02	33,85	1,0E-04	6,48	1
18	1oo1	1,0E-03	8,2E-05	2oo2	1,9E-03	2,7E-04	1oo1	1,5E-02	1,0E-04	1oo1,2oo2,1oo1	1,8E-02	55,93	4,5E-04	3,01	1
19	1oo1	1,0E-03	8,2E-05	2oo2	1,9E-03	2,7E-04	1oo2	1,7E-03	8,1E-06	1oo1,2oo2,1oo2	4,6E-03	216,37	3,6E-04	2,28	2
20	1oo1	1,0E-03	8,2E-05	2oo2	1,9E-03	2,7E-04	2oo2	2,9E-02	8,1E-06	1oo1,2oo2,2oo2	3,1E-02	31,87	3,6E-04	3,01	1
21	1oo1	1,0E-03	8,2E-05	2oo2D	1,8E-03	2,7E-04	1oo1	1,5E-02	1,0E-04	1oo1,2oo2D,1oo1	1,8E-02	56,26	4,5E-04	3,01	1
22	1oo1	1,0E-03	8,2E-05	2oo2D	1,8E-03	2,7E-04	1oo2	1,7E-03	8,1E-06	1oo1,2oo2D,1oo2	4,5E-03	221,37	3,6E-04	3,01	2
23	1oo1	1,0E-03	8,2E-05	2oo2D	1,8E-03	2,7E-04	2oo2	2,9E-02	8,1E-06	1oo1,2oo2D,2oo2	3,1E-02	31,98	3,6E-04	3,01	1
24	1oo1	1,0E-03	8,2E-05	2oo3	1,1E-04	2,7E-04	1oo1	1,5E-02	1,0E-04	1oo1,2oo3,1oo1	1,6E-02	62,05	4,5E-04	2,28	1
25	1oo1	1,0E-03	8,2E-05	2oo3	1,1E-04	2,7E-04	1oo2	1,7E-03	8,1E-06	1oo1,2oo3,1oo2	2,9E-03	349,86	3,6E-04	3,01	2
26	1oo1	1,0E-03	8,2E-05	2oo3	1,1E-04	2,7E-04	2oo2	2,9E-02	8,1E-06	1oo1,2oo3,2oo2	3,0E-02	33,77	3,6E-04	2,28	1
27	1oo1D	1,0E-03	1,0E-04	1oo1	9,5E-04	2,1E-05	1oo1	1,5E-02	1,0E-04	1oo1D,1oo1,1oo1	1,7E-02	58,99	2,3E-04	14,36	1
28	1oo1D	1,0E-03	1,0E-04	1oo1	9,5E-04	2,1E-05	1oo2	1,7E-03	8,1E-06	1oo1D,1oo1,1oo2	3,7E-03	270,55	1,3E-04	5,72	2
29	1oo1D	1,0E-03	1,0E-04	1oo1	9,5E-04	2,1E-05	2oo2	2,9E-02	8,1E-06	1oo1D,1oo1,2oo2	3,0E-02	32,84	1,3E-04	14,36	1
30	1oo1D	1,0E-03	1,0E-04	1oo1D	9,0E-04	9,3E-06	1oo1	1,5E-02	1,0E-04	1oo1D,1oo1D,1oo1	1,7E-02	59,17	2,2E-04	17,50	1
31	1oo1D	1,0E-03	1,0E-04	1oo1D	9,0E-04	9,3E-06	1oo2	1,7E-03	8,1E-06	1oo1D,1oo1D,1oo2	3,6E-03	274,50	1,2E-04	17,50	2
32	1oo1D	1,0E-03	1,0E-04	1oo1D	9,0E-04	9,3E-06	2oo2	2,9E-02	8,1E-06	1oo1D,1oo1D,2oo2	3,0E-02	32,89	1,2E-04	17,50	1
33	1oo1D	1,0E-03	1,0E-04	1oo2	3,6E-05	2,1E-05	1oo1	1,5E-02	1,0E-04	1oo1D,1oo2,1oo1	1,6E-02	62,36	2,3E-04	5,72	1
34	1oo1D	1,0E-03	1,0E-04	1oo2	3,6E-05	2,1E-05	1oo2	1,7E-03	8,1E-06	1oo1D,1oo2,1oo2	2,8E-03	359,85	1,3E-04	14,36	2
35	1oo1D	1,0E-03	1,0E-04	1oo2	3,6E-05	2,1E-05	2oo2	2,9E-02	8,1E-06	1oo1D,1oo2,2oo2	3,0E-02	33,86	1,3E-04	5,72	1
36	1oo1D	1,0E-03	1,0E-04	1oo2D	3,4E-05	9,3E-06	1oo1	1,5E-02	1,0E-04	1oo1D,1oo2D,1oo1	1,6E-02	62,37	2,2E-04	17,50	1
37	1oo1D	1,0E-03	1,0E-04	1oo2D	3,4E-05	9,3E-06	1oo2	1,7E-03	8,1E-06	1oo1D,1oo2D,1oo2	2,8E-03	360,10	1,2E-04	6,16	2
38	1oo1D	1,0E-03	1,0E-04	1oo2D	3,4E-05	9,3E-06	2oo2	2,9E-02	8,1E-06	1oo1D,1oo2D,2oo2	3,0E-02	33,86	1,2E-04	17,50	1
39	1oo1D	1,0E-03	1,0E-04	2oo2	1,9E-03	2,7E-04	1oo1	1,5E-02	1,0E-04	1oo1D,2oo2,1oo1	1,8E-02	55,96	4,8E-04	2,94	1
40	1oo1D	1,0E-03	1,0E-04	2oo2	1,9E-03	2,7E-04	1oo2	1,7E-03	8,1E-06	1oo1D,2oo2,1oo2	4,6E-03	216,72	3,8E-04	2,94	2
41	1oo1D	1,0E-03	1,0E-04	2oo2	1,9E-03	2,7E-04	2oo2	2,9E-02	8,1E-06	1oo1D,2oo2,2oo2	3,1E-02	31,88	3,8E-04	2,94	1

Sensores | Controlador | Válvulas | Resumen | Comparación

Learn

Figura 4.5.- Hoja de Cálculo de "Resumen".

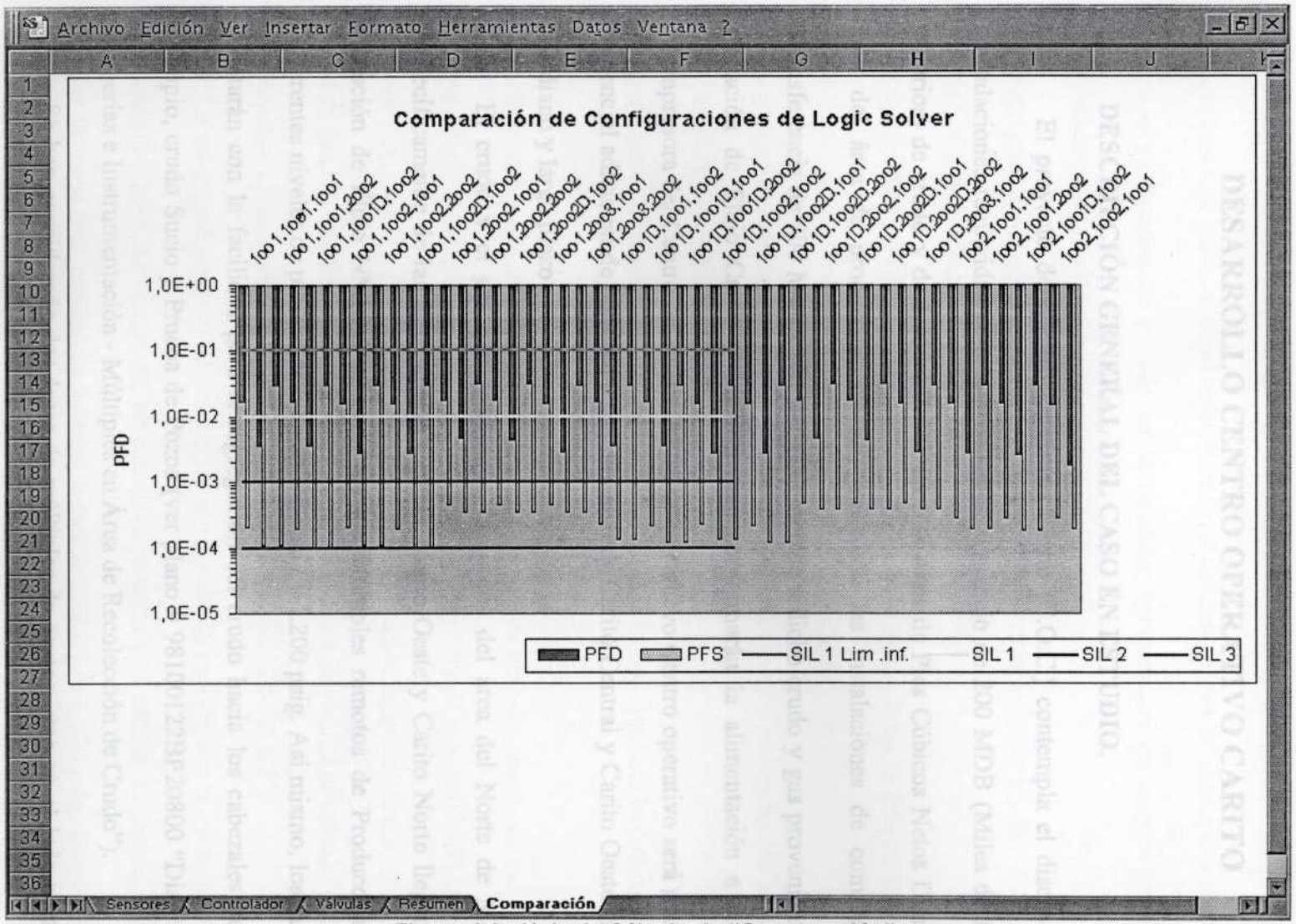


Figura 4.6.- Hoja de Cálculo de "Comparación".

Capítulo 5.

DESARROLLO CENTRO OPERATIVO CARITO

5.1. DESCRIPCIÓN GENERAL DEL CASO EN ESTUDIO.

El proyecto del Centro Operativo Carito (C.O.C.) contempla el diseño de las instalaciones requeridas para la producción y manejo de 200 MDB (Miles de Barriles Diarios) de crudo y de 1.350 MMPCND (Millones de Pies Cúbicos Netos Diarios) de gas del área de producción NMEF, así como las instalaciones de compresión y transferencia de 900 MMPCND del gas asociado a dicho crudo y gas proveniente de la Estación de Flujo Carito (NMEF-2), que conformarán la alimentación a la planta Compresora del Centro operativo. El fin de este nuevo Centro operativo será manejar el potencial adicional de petróleo y gas del área de Carito Central y Carito Oeste en corto, mediano y largo plazo.

El crudo y el gas que producirán los pozos del área del Norte de Monagas, específicamente de las áreas Carito Central, Carito Oeste y Carito Norte llegarán a la Estación de Flujo NMEF-7 a través de los Múltiples remotos de Producción a los diferentes niveles de presión de 60 psig, 450 psig y 1.200 psig. Así mismo, los múltiples contarán con la facilidad para la segregación del crudo hacia los cabezales de crudo Limpio, crudo Sucio y Prueba de Pozos (ver plano # 98100122BP20800 "Diagrama de Tuberías e Instrumentación - Múltiples en Área de Recolección de Crudo").

Se han considerado dos áreas de múltiples de campo, una en el lado norte de la carretera y otra en el lado sur, en las cuales se contará con cabezales destinados para

cada uno de los niveles de producción. De cada área salen líneas de crudo que llevarán éste hasta el Centro Operativo El Carito, en cuya entrada se unen las líneas procedentes de cada área una a una, dependiendo de su nivel de presión y de sí es limpio o sucio.

Las facilidades de entrada en la estación, comprenden los juegos de válvulas motorizadas que permitirán:

- Segregar la producción desde el cabezal de Crudo Limpio hacia los dos (2) trenes de separación Crudo Limpio-Gas.
- Segregar la producción desde el cabezal de Crudo Sucio hacia el tren de Separación Crudo Sucio-Gas.
- Segregar la producción desde el cabezal de Crudo Sucio a los trenes de separación de Crudo Limpio-Gas.
- Segregar la producción desde el cabezal de Crudo Limpio hacia el tren de separación Crudo Sucio-Gas.

El crudo sucio a niveles de 1200# y 450# es liberado de arena en los paquetes desarenadores A-0201A/B, A-0211A/B (para nivel de 1200#) y A-0202A/B (para nivel de 450#). A la salida de este sistema (Desarenador / Acumulador de Arena) el crudo sin arena es pasado a la Estación de Producción (ver plano # 98100122BP20802 "Diagrama de Tuberías e Instrumentación – Sistemas Desarenadores 1200 PSIG").

La producción entrará al sistema de separación (trenes), a tres niveles de presión: alta, media y baja. Se tendrá así niveles de separación en cascada en donde, según los niveles de los pozos, pasarán en primera instancia al nivel de 1.200 psig, luego al de 450

psig y posteriormente al de 60 psig (ver planos #´s 98100122BP20805/6/7 "Diagrama de Tuberías e Instrumentación – Sistema de Separación 1200/450/60, Tren A/B y C").

El gas obtenido en el proceso de separación de alta presión se envía, a través del Cabezal de Recolección de Gas de 1200# de la Estación, al Filtro Antiasfalténico de alta (FIL-0501) (ver plano # 98100122BP20815 "Diagrama de Tuberías e Instrumentación – Depuración 1200 PSIG – Hoja 1"). El crudo obtenido del filtro se reinyecta al Cabezal de Recibo de Crudo Sucio de 450 psig. El gas filtrado pasa a los enfriadores (E-0501), luego al Depurador de gas (V-0501) en donde le son removidos los líquidos condensados, y de allí al gasoducto COC Muscar (ver plano # 98100122BP20816 "Diagrama de Tuberías e Instrumentación – Depuración 1200 PSIG – Hoja 2").

El gas procedente del proceso de separación de media presión se envía hacia los sistemas de Filtrado, Enfriamiento y Depuración de media y de allí al cabezal de succión de 450 psig de la Planta Compresora. El crudo obtenido del filtro se envía al Cabezal de Recibo de Crudo Sucio de 60 psig.

El gas procedente del proceso de separación de baja presión se envía hacia los sistemas de Filtrado, Enfriamiento y Depuración de baja y de allí al cabezal de succión de 60 psig de la Planta Compresora. El crudo obtenido del filtro se envía al Cabezal de Recolección de Crudo Sucio de la Estación a tanques de estabilización.

El crudo separado en los Depuradores se enviará al sistema de estabilización de Condensados, Separador Trifásico V-2901 para luego ser almacenado en los tanques (T-0702, T-0703 y T-0704) (ver plano # 98100124BP20800 "Diagrama de Tuberías e Instrumentación – Almacenamiento y Bombeo Crudo Limpio").

El crudo proveniente de los separadores de baja (V-02-03 A/B/C y V-01-03), se enviará a los tanques de Estabilización (T-0701A/B); dos bombas (P-0702 A/B) serán las encargadas de enviar el crudo estabilizado al Sistema de Deshidratación (SE-0901) (ver plano # 98100122BP20820 "Diagrama de Tuberías e Instrumentación – Tanques de Estabilización y Bombeo"). El crudo será almacenado en los tanques T-0702, T-0703 y T-0704, para posteriormente ser Despachado al Oleoducto de 30" Musipan-PTT, a través de las Bombas boosters P-0802 A/B/C/D y las bombas principales P-0801 A/B/C/D (ver plano # 98100124BP20800 "Diagrama de Tuberías e Instrumentación – Almacenamiento y Bombeo Crudo Limpio")

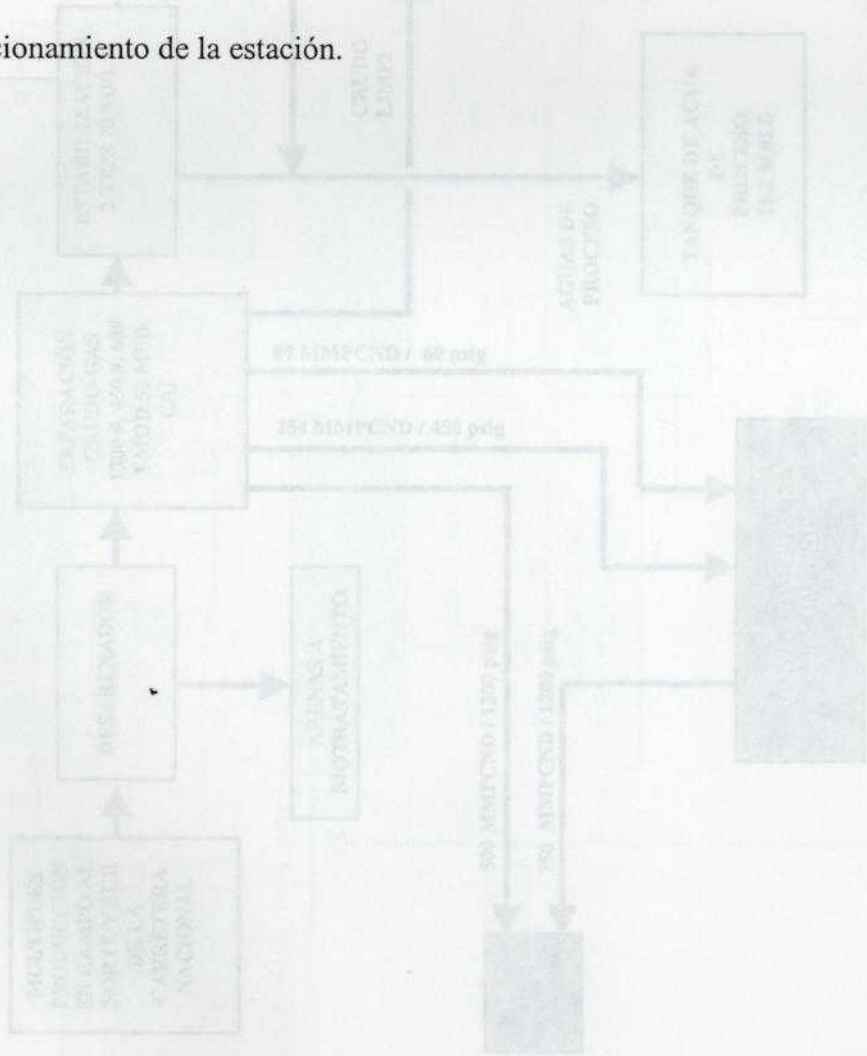
Los vapores generados en los tanques de Estabilización, Recibo y Bombeo y en el Sistema de Estabilización de Condensados, se recogerán a través del sistema de tuberías y transportados hacia el sistema de Recuperación de Vapor (URV), en donde serán comprimidos. Los líquidos aquí generados se enviarán al Cabezal de recolección de crudo limpio de la Estación, y el gas al cabezal de succión de 60 psig de la Planta Compresora (ver plano # 98100122BP20816 "Diagrama de Tuberías e Instrumentación – Depuración 1200 PSIG Hoja 2")

5.2. OPERACIÓN Y CONTROL DE LA ESTACIÓN.

La forma de operación de la estación será desatendida y automática, toda la estrategia de supervisión y control de la estación se llevará a cabo a través del Sistema Básico de Control (BPCS) basado en PLC (Controlador Lógico Programable), que funcionará con una interfaz hombre-máquina, luego todas estas señales serán

concentradas en el E.M.C.O. Carito donde también se supervisará la operación de las estaciones Amana, Musipan, Carito, El Tejero, Muri, Pirital, etc.

El PLC estará ubicado físicamente en la sala de control de la estación. La recopilación de la información de campo asociada al proceso, se realizará por medio de "racks" remotos ubicados estratégicamente. Se dispondrá de dos (2) consolas de operación, una (1) consola de alarmas y reportes y una (1) para ingeniería y mantenimiento. En las consolas de operación se configuraran despliegues dinámicos de operación y control, por medio de las cuales el operador podrá supervisar el funcionamiento de la estación.



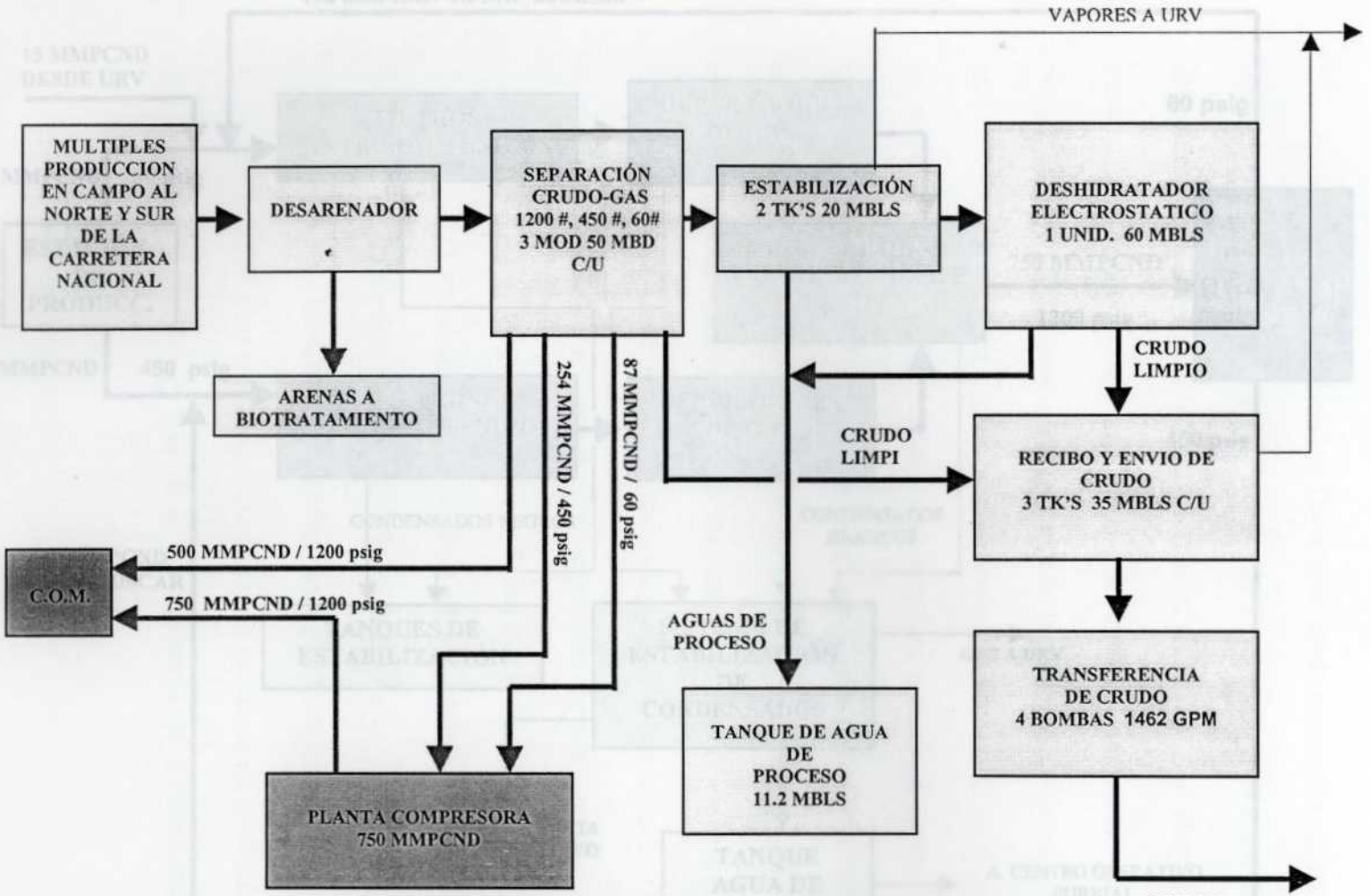


Figura 5.1.- Diagrama de Bloques "Estación de Producción".

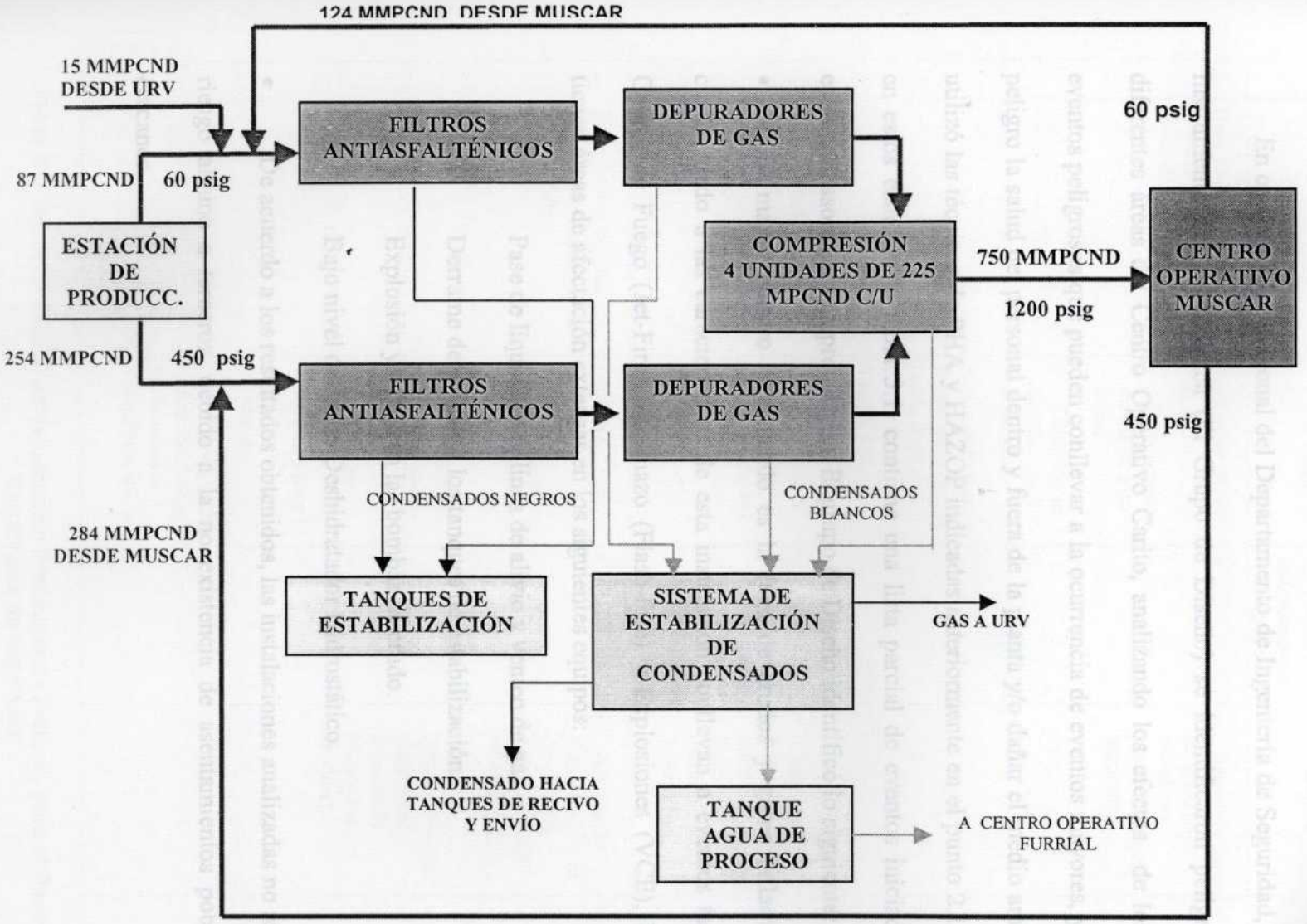


Figura 5.2.- Diagrama de Bloques "Planta Compresora ".

5.3. IDENTIFICACIÓN PARCIAL DE EVENTOS PELIGROSOS.

En conjunto con personal del Departamento de Ingeniería de Seguridad, Procesos, Instrumentación y Mecánica (El Grupo de Diseño) se identificaron peligros en las diferentes áreas del Centro Operativo Carito, analizando los efectos de los posibles eventos peligrosos que pueden conllevar a la ocurrencia de eventos mayores, y poner en peligro la salud del personal dentro y fuera de la planta y/o dañar el medio ambiente. Se utilizó las técnicas de PHA y HAZOP indicadas anteriormente en el punto 2.1., basados en estos estudios la tabla 5.1, contiene una lista parcial de eventos iniciadores y la estrategia asociada a su prevención. El grupo de Diseño identificó lo siguiente:

- El mayor peligro identificado es la fuga de crudos y gases inflamables, los cuales, dado a las características de esta instalación conllevan a eventos tales como: Chorro de Fuego (Jet-Fire), Fogonazo (Flash-Fire) y Explosiones (VCE), los cuales tienen áreas de afectación extensas en los siguientes equipos:
    - Pase de líquidos a la línea de alivio y venteo de gas.
    - Derrame de crudo en los tanques de estabilización.
    - Explosión y daños en las bombas de crudo.
    - Bajo nivel de crudo Deshidratador Hidrostático.
- De acuerdo a los resultados obtenidos, las instalaciones analizadas no representan riesgo alguno a terceros, debido a la no existencia de asentamientos poblacionales cercanos.

#	Evento Iniciador	Escenarios de Falla	Soluciones Sugeridas		
			Pasiva / Inherentemente Segura	Activa	Procedimental
1	Bajo Nivel de Crudo Separador Gas Petróleo V-02-03A	Perdida de Nivel por: • Falla Sistema de Control de Nivel. • Filtración de líquidos en el separador. Este evento puede causar pase de gas por la línea de Crudo Sucio a los Tanques de Estabilización.	•	• Alarma y paro de Bajo Bajo Nivel con válvula de cierre automático.	• Cierre manual al tener baja indicación del nivel en el separador.
2	Sobrellenado del tanque de Estabilización T-0701 A / B	Falla Sistema de Control de Nivel causando derrame	• Instalar Boquilla de Sobrellenado a un sistema cerrado.	• Alarma de Alto Alto Nivel, corte y aislamiento de alimentaciòn automática.	• Manual de instrucciones para el paro de alimentación cuando el nivel llega a cierto valor.
3	Baja Presión de Succión Bombas de Crudo Sucio P-0702 A/B.	Perdida de Nivel por: • Falla Sistema de Control de Nivel. • Filtración de líquidos en los tanques. • Cierre de válvulas motorizadas a la salida de tanques. Este evento puede causar cavitación a las Bombas de Transferencia.	•	• Alarma de Bajo Bajo Nivel con parada automática de Bombas. • Parada Automática por Baja Baja Presión de Succión a las Bombas.	• Parada manual de las Bombas al tener baja indicación del nivel en el tanque. • Parada manual de las Bombas al tener baja presión de succión.

Tabla 5.1.- Sumario Parcial de Valorización Preliminar de Peligros para el Desarrollo de Estrategias de Seguridad.

5.4. IDENTIFICACIÓN DE LOS LAZOS CRÍTICOS DEL PROCESO C.O.C.

Una vez identificados y determinados los eventos peligrosos que pueden acarrear un peligro inminente, para los efectos del presente trabajo se procedió a determinar cuatro lazos de control críticos, dependiendo de las variables que lo afectan.

- En referencia al evento peligroso de arrastre de líquido por una línea de gas, se estudio la desviación de la variable de bajo bajo nivel del separador Gas-crudo 1200 # tren A (V-02-01 A) **(Lazo Crítico: Bajo Bajo Nivel de Crudo en el Separador Gas Crudo)**
- En lo referente al evento peligroso de derrame de crudo, se estudio la desviación de la variable de alto alto nivel en los tanques de estabilización V-701A/B. **(Lazo Crítico: Alto Alto Nivel de Crudo en los Tanques V-701A/B.**
- En lo referente al evento no deseado de bajo bajo nivel de crudo en los tanques de estabilización V-701A/B, evento que afecta el funcionamiento de las bombas de transferencia de crudo sucio **(Lazo Crítico: Alto Alto diferencial de presión a la entrada de las Bombas de Transferencia (P-702 A/B) por baja baja presión de succión o bajo bajo nivel de crudo**.
- En lo correspondiente al evento no deseado de bajo bajo nivel en los Separadores Hidrostáticos se estudio la desviación de la variable de nivel del separador Crudo/Agua (SE-0801) **(Lazo Crítico: Bajo Bajo Nivel de Crudo en el Separador Hidrostático)**.

5.5. MÉTODO CUALITATIVO / CUANTITATIVO PARA LA DETERMINACIÓN DEL SIL DEL PROCESO.

5.5.1. Evento 1: Arrastre de Gas por una Línea de Liquido.

Los Separadores horizontales de petróleo/gas (V-0203 A/B/C) son la última de tres etapas de separadores operando a 75 psig y 136,5 °F. El nivel de crudo en el Separador (V-02-03A) es controlado en forma continua por el lazo de control de nivel electrónico (LC-0222A) formado por un (1) transmisor (LT-0222A), un transductor I/P (XY-0222A) y dos válvulas de control neumática en paralelo (LCV – 0222A y LCV – 0223A) (una en operación y la otra en reserva).

De los métodos cualitativos disponibles para este lazo se utilizó el "Método General de Matriz de Capas de Seguridad", los pasos descritos son los siguientes:

1.- Se identificó el evento peligroso del proceso, este es el pase de gas por una línea de crudo al tener bajo bajo nivel de crudo en el Separador Gas-Crudo.

2.- La severidad cualitativa de la consecuencia del evento descrito en el paso anterior se estableció como Alta, debido a que si ocurriese este evento, pasa gas a los tanques de Estabilización (T-701 A/B), los cuales no están diseñados para manejar grandes volúmenes de gas, sufriendo graves daños, el escape de gas al medio ambiente pudiera ocasionar un evento mayor al producirse una explosión.

3.- La probabilidad de ocurrencia del presente evento se estimo en alta ($F>10^{-2}$).

4.- La evaluación cualitativa de la efectividad de las capas de protección independiente se estimo en Moderada, al estimarse colocar como una IPL´s un Anunciador de Alarmas.

Resumiendo los parámetros utilizados en la matriz para este evento en particular es:

- Severidad de las consecuencias: Alta

- Probabilidad de Ocurrencia: Alta
- Efectividad de las IPL´s: Moderada.

El valor del SIL correspondiente a esta evaluación es: SIL 2.

Dado que la evaluación efectuada en el punto anterior es una evaluación cualitativa, se procede ahora a efectuar un análisis cuantitativo para determinar numéricamente la frecuencia de falla de los sistemas y equipos que conforman cada lazo de control crítico, el resultado nos permitirá conocer el nivel de riesgo de los mismos y validar o no el resultado obtenido cualitativamente.

5.5.1.1. Análisis Cualitativo.

Para el cálculo de la Frecuencia de Falla del Lazo de Control de nivel en el Separador Gas-Crudo aplicando la técnica de árboles de falla, denotando los elementos básicos e intermedios que pudiesen producir el evento tope (arrastre de gas por una línea de líquido), utilizando los valores de rata de falla de cada equipo extraídos de la OREDA-92.

Posteriormente y aplicando álgebra Booleana y entendiendo que función realiza cada compuerta lógica se tiene lo siguiente, ver figura 5.3.

La consecuencia del evento 1 es el Bajo Bajo Nivel de Crudo en el separador de Gas Crudo.

- Se a determinado según tabla que los separadores tienen falla de perdida de nivel de líquido por diferentes causas con una frecuencia de $8{,}30 \times 10^{-2}$ eventos/año.
- El BPCS por intermedio del lazo de control de nivel tiene una frecuencia de falla de $6{,}82 \times 10^{-2}$/año.

- La frecuencia del evento no deseado de vaciado y pase de gas por la línea de crudo es de: $(8{,}30 \times 10^{-2}) \times (6{,}82 \times 10^{-2}) = 5{,}66 \times 10^{-3}$/año.

Esta frecuencia de falla no cumple con el valor mínimo establecido de 1×10^{-5}/año, siendo necesaria la evaluación de una capa independiente de protección (IPL´s).

5.5.1.2. Determinación de las Capas Independientes de Protección Evento 1.

Para el presente lazo crítico se selecciono un Sistema de Anunciador de Alarmas con Alarma de Bajo Nivel de Crudo en el Separador Gas-Crudo, y que por acción del operador, proceda este a realizar el procedimiento necesario para evitar el pase de gas por la línea de crudo, esta tiene una frecuencia de falla de $1{,}10 \times 10^{-1}$, ver figura 5.4. Frecuencia que no cubre uno de los requerimientos mínimos como es el de la reducción de riesgo por una IPL sea de dos ordenes de magnitud, i.e., $1{,}0 \times 10^{-2}$ de PFD, descartándose la misma por considerar el costo beneficio de su instalación como no suficiente.

Al descartarse la adición de la IPL propuesta queda solamente el proceso más el BPCS con una frecuencia de falla de $5{,}66 \times 10^{-03}$. La reducción de frecuencia de riesgo necesaria es la siguiente:

$$PFD_{AVG.} = \frac{F_P}{F_{NP}} = \frac{1 \, x \, 10^{-5}}{5{,}66 \, x \, 10^{-3}} = 1{,}77 \, x \, 10^{-3}$$

El resultado mostrado indica que para cubrir el primer evento identificado de Bajo Bajo Nivel de Crudo en el Separador Gas Crudo es el indicado para un SIS con un SIL 2.

Todas las operaciones realizadas son mostradas en la tabla 5.2, de Evaluación de Riesgo del Sistema / Documentación del SIL.

5.5.2. Evento 2: Alto Alto Nivel de Crudo en los Tanques de Estabilización T-01A/B.

Los tanques de estabilización T-0701 A/B son de techo cónico y de 20 Mbls de capacidad nominal cada uno, en estos tanques ocurre la primera etapa de separación del agua libre asociada al crudo sucio, de forma que se disminuye la carga de agua que se va al sistema de deshidratación electrostática. La operación de los tanques es el de uno en línea y el otro en reserva, los dos están instrumentados idénticamente, por lo tanto se procederá a realizar la evaluación a un solo tanque. A fin de mantener constante el nivel de crudo sucio en los tanques, se contempla el siguiente esquema de control en cascada:

El control maestro de nivel LIC-0707 ubicado en los tanques de crudo sucio, fija el punto de ajuste al controlador de flujo al deshidratador FIC-0901, el cual a su vez, envía los puntos de ajuste a los controladores de flujo FC-0901A, siendo éste el que actúa sobre la válvula de control de flujo FCV-0901, ubicada en la salida de crudo deshidratado del deshidratador Electrostático SE-0901.

En operación normal, un aumento de nivel de crudo en los tanques hace que la válvula de control FCV-0901, por el esquema de maestro-esclavo, incremente su apertura a fin de aumentar el caudal hacia los tanques de crudo limpio, hasta llevar el nivel a su punto normal.

De los métodos cualitativos disponibles para la evaluación de este lazo se utilizó el "Método General de Gráfica de Riesgo" descrito en el párrafo 2.6.1.2 del capitulo 2.

Las condiciones de operación del proceso del tanque de estabilización son las siguientes:

- Es un tanque con 16" de H_2O de presión positiva por arriba de la presión atmosférica, que recibe crudo mediano liviano de 28° API de los separadores Gas-Petróleo.
- El tanque es instalado en un dique dentro de las instalaciones de la planta, la planta es 24 horas atendida.
- La operación del tanque es automática.
- El operador hace una inspección visual del tanque dos (2) veces por guardia de 8 horas.
- Siendo crudo mediano liviano, el riesgo potencial viene de derrames de crudo, escapes de gas, fuegos y explosiones.
- La presión hidrostática causada por el sobrellenado del tanque, puede resultar en la ruptura de este.

➢ Evaluación de las consecuencias del Evento Peligroso:

- El crudo liviano mediano es inflamable, y los derrames del mismo pudieran potencialmente resultar en una explosión o fuego.
- El tanque esta localizado en el medio de la planta, por lo tanto, personal de mantenimiento y de operaciones están continuamente presentes en el área del tanque.
- Siendo que los operadores hacen inspección visual en los alrededores del tanque dos (2) veces por turno, un operador esta en el área inmediata al tanque por lo menos seis (6) veces al día en tres (3) turnos diarios.

En base a lo indicado anteriormente, se concluye lo siguiente:

- Lesiones potenciales al operador deben ser consideradas, debido a que el contenido del tanque es altamente inflamable y explosivo.
- Quemaduras potenciales debido a la exposición al fuego y heridas debido a la explosión son posibles.
- El tanque esta protegido por un dique que limita los efectos potenciales a las otras unidades de proceso, por lo tanto se considera que las consecuencias se limitarían al tanque.
- El parámetro C3 de clasificación moderada es el que corresponde a este evento, se tiene daños al tanque, heridas y/o daños al personal y al ambiente, finalmente se tiene una breve parada al proceso al disponerse de un tanque en espera.

➢ Evaluación de la Frecuencia de Exposición al Evento Peligroso:

En este caso el operador esta en el área del tanque por lo menos 6 veces al día y el personal de operaciones y mantenimiento están frecuentemente en el área.

Teniendo el operador una alta probabilidad de exposición la peligro se considera el Parámetro F_2 con la una clasificación de Mayor frecuencia de exposición.

➢ Cuantificación de Posibilidades de Evitar el Riesgo

Las posibilidades de evitar el riesgo son posibles debido a que la operación del proceso es automática supervisada por personal entrenado y la facilidad de identificación del peligro al poder ser detectado por sensores de gas y fuego, las rutas de escapes son muy bien señaladas y son conocidas por el operador.

En base a lo indicado anteriormente el Parámetro de Posibilidad de Evitar el Peligro seleccionado para este caso es P_1.

➢ Cuantificación de Probabilidad de ocurrencia del Evento.

El proceso es operado automáticamente por un PLC de buena confiabilidad, la ocurrencia del evento es de baja probabilidad de ocurrencia, la cual considera una frecuencia de falla entre 10^{-4} y 10^{-2} eventos/año. Por lo tanto el rango cualitativo seleccionado es el de baja probabilidad W_2.

Resumiendo los parámetros utilizados para el Método Cualitativo de Gráfica de Riesgo para la determinación del SIL son los siguientes:

- Extensión del Daño: moderada, parámetro: C_3.
- Frecuencia de Exposición al Peligro: Menor, Parámetro: F_1.
- Posibilidad de Evitar el Peligro: Posible, Parámetro: P_1.
- La Probabilidad de ocurrencia del evento peligroso: Baja, Parámetro: W_2.

El valor del SIL correspondiente a esta evaluación es: SIL 2.

Dado que la evaluación efectuada en el punto anterior es una evaluación cualitativa, se procede ahora a efectuar un análisis cuantitativo para determinar numéricamente la frecuencia de falla de los sistemas y equipos que conforman cada lazo de control crítico, el resultado nos permitirá conocer el nivel de riesgo de los mismos y validar o no el resultado obtenido cualitativamente.

5.5.2.1. Análisis Cuantitativo.

Para el cálculo de la Frecuencia de Falla del Lazo de Control de nivel en el Tanque de Estabilización aplicando la técnica de árboles de falla, denotando los elementos básicos e intermedios que pudiesen producir el evento tope (sobrellenado del tanque y

posible derrame de crudo), utilizando los valores de rata de falla de cada equipo extraídos de la OREDA-92.

Posteriormente y aplicando álgebra Booleana y entendiendo que función realiza cada compuerta lógica se tiene lo siguiente:

La consecuencia 2 es el Alto Alto Nivel de Crudo en el Tanque de Estabilización, ver figura 5.5.

- Se a determinado según tabla que el derrame de líquido de los tanques tienen una frecuencia de ocurrencia por diferentes causas de $3,95 \times 10^{-2}$ eventos/año.
- El BPCS por intermedio del lazo de control de nivel tiene una frecuencia de falla de $6,28 \times 10^{-2}$/año.
- La frecuencia del evento no deseado de vaciado y pase de gas por la línea de crudo es de: $(3,95 \times 10^{-2}) \times (6,28 \times 10^{-2}) = 2,69 \times 10^{-3}$/año.

Esta frecuencia de falla no cumple con el valor mínimo establecido de 1×10^{-5}/año, siendo necesaria la evaluación de una capa independiente de protección (IPL´s).

5.5.2.2. Determinación de las Capas Independientes de Protección Evento 2.

Para el presente lazo crítico se pudiese seleccionar un Sistema de Anunciador de Alarmas con Alarma de Alto Nivel de Crudo en el Tanque de Estabilización, y que por acción del operador, proceda este a realizar el procedimiento necesario para evitar el derrame de crudo en el tanque de estabilización, pero tal como lo determinamos en el evento 1, este tiene una frecuencia de falla de $1,10 \times 10^{-1}$, frecuencia que no cubre uno

de los requerimientos mínimos como es el de la reducción de riesgo por una IPL sea de dos ordenes de magnitud, i.e., 1,0 x 10^{-2} de PFD, descartándose nuevamente el mismo por considerar el costo beneficio de su instalación como no suficiente.

Al descartarse la adición de la IPL propuesta queda solamente el proceso más el BPCS con una frecuencia de falla de 4,42 x 10^{-3}/año. La reducción de frecuencia de riesgo necesaria es la siguiente:

$$PFD_{AVG.} = \frac{F_P}{F_{NP}} = \frac{1\,x\,10^{-05}}{2{,}69\,x\,10^{-03}} = 3{,}72\,x\,10^{-03}$$

El resultado mostrado indica que para cubrir el segundo evento identificado de Alto Alto Nivel de Crudo en el Tanque de Estabilización es el indicado para un SIS con un SIL 2.

Todas las operaciones realizadas son mostradas en la tabla 5.2, de Evaluación de Riesgo del Sistema / Documentación del SIL.

5.5.3. Evento 3: Baja Presión de Succión Bombas de Crudo Sucio P-0702 A/B.

El crudo sucio recibido de los Tanques de Estabilización T-0701 A/B es succionado por las bombas de transferencia verticales de cuatro etapas de 1.721 G.P.M. de crudo Sucio P-0702 A/B las cuales se encargarán de transferir el mismo al sistema de deshidratación electrostática. La operación de las bombas es el de una en línea y la otra en reserva, cada una de ellas están instrumentadas idénticamente, por lo tanto se procederá a realizar la evaluación a una sola bomba. A fin de mantener una presión de succión constante a la entrada de la bomba, se tiene el siguiente esquema de control:

Al esquema de control de nivel de los tanques de estabilización descrito en el evento 2, una disminución del nivel de crudo en el tanque de estabilización hace que la válvula de control FCV-0901 disminuya en proporción su apertura a fin de reducir el flujo y mantener el nivel en el tanque. Si el flujo es menor al flujo mínimo requerido por la bomba P-0702 (Estimado en 900 GPM). determinado por la sumatoria de FIC 0901A (flujo de crudo) y FIC 0901B (Flujo de agua de proceso), el controlador FIC-0901 comienza la apertura de la válvula de recirculación a tanques FCV-0707, compensando el flujo mínimo de la bomba, e impidiendo que baje aun mas el nivel en el tanque. En la línea de succión de las bombas, se encuentra un interruptor por baja baja presión de succión PLS-0721 A/B, el cual da una señal de alarma y paro a las bombas, protegiendo a las mismas de succionar en vacío.

De los métodos cualitativos disponibles para este lazo se utilizó el "Método General de Matriz de Capas de Seguridad", los pasos descritos son los siguientes:

1.- Se identifico el evento peligroso del proceso, este es el de baja presión en la succión de la bomba de crudo sucio produciéndose cavitación en la misma.

2.- La severidad cualitativa de la consecuencia del evento descrito en el paso anterior se estableció como Alta, debido a que si ocurriese este evento, los daños a los alaves de la bomba pudieran ser extensos, sufriendo la bomba graves daños, pudiéndose producir escapes de crudo al medio ambiente que pudiera ocasionar un evento mayor al producirse un fuego y una explosión.

3.- La probabilidad de ocurrencia del presente evento se estimo en alta ($F>10^{-2}$).

4.- La evaluación cualitativa de la efectividad de las capas de protección independiente incluyendo al BPCS se estimo en Moderada, al estimarse colocar un interruptor de baja presión en la succión de la bomba.

Resumiendo los parámetros utilizados en la matriz para este evento en particular es:

- Severidad de las consecuencias: Alta
- Probabilidad de Ocurrencia: Alta
- Efectividad de las IPL´s: Moderada.

El valor del SIL correspondiente a esta evaluación es: SIL 2.

Dado que la evaluación efectuada en el punto anterior es una evaluación cualitativa, se procede ahora a efectuar un análisis cuantitativo para determinar numéricamente la frecuencia de falla de los sistemas y equipos que conforman cada lazo de control crítico, el resultado nos permitirá conocer el nivel de riesgo de los mismos y validar o no el resultado obtenido cualitativamente.

5.5.3.1. Análisis Cuantitativo.

Para el cálculo de la Frecuencia de Falla del Lazo de Control de baja presión de succión a las bombas de crudo sucio aplicando la técnica de árboles de falla, (bajo nivel en el tanque de estabilización y por lo tanto baja presión de succión a la bombas), utilizando los valores de rata de falla de cada equipo extraídos de la base de datos OREDA-92.

La consecuencia 3 es la Baja Presión de Succión a las Bombas de Crudo Sucio, ver figura. 5.6.

- Se a determinado según tabla que la tasa de fallas peligrosas por cavitación tienen una frecuencia de ocurrencia por diferentes causas de 5,05 x 10^{-2} eventos/año.

- El Proceso + el BPCS por intermedio del lazo de control nivel-flujo tienen una frecuencia de falla de 3,06 x 10^{-2}/año.

- La frecuencia del evento no deseado de cavitación de las bombas es de:

$$(5{,}05 \times 10^{-2}) \times (3{,}06 \times 10^{-2}) = 1{,}55 \times 10^{-3}/\text{año}.$$

Esta frecuencia de falla no cumple con el valor mínimo establecido de 1 x 10^{-5}/año, siendo necesaria la evaluación de una capa independiente de protección (IPL´s).

5.5.3.2. Determinación de las Capas Independientes de Protección Evento 3.

En el presente lazo critico, observamos que se le a incluido un interruptor de presión ubicado en la succión de la bomba como una protección, esta no será considerada como una capa de protección independiente debido a que esta es dependiente del BPCS, adicionalmente no se visualizaron otras IPL´s.

Al descartarse la adición de IPL´s, queda solamente el proceso más el BPCS con una frecuencia de falla de 1,55 x 10^{-3}/año. La reducción de frecuencia de riesgo necesaria es la siguiente:

$$PFD_{AVG.} = \frac{F_P}{F_{NP}} = \frac{1\,x\,10^{-05}}{1{,}55\,x\,10^{-03}} = 6{,}46\,x\,10^{-03}$$

El resultado mostrado indica que para cubrir el tercer evento identificado de Baja Presión de Succión de las Bombas de Crudo es el indicado para un SIS con un SIL 2.

Todas las operaciones realizadas son mostradas en la tabla 5.2, de Evaluación de Riesgo del Sistema / Documentación del SIL.

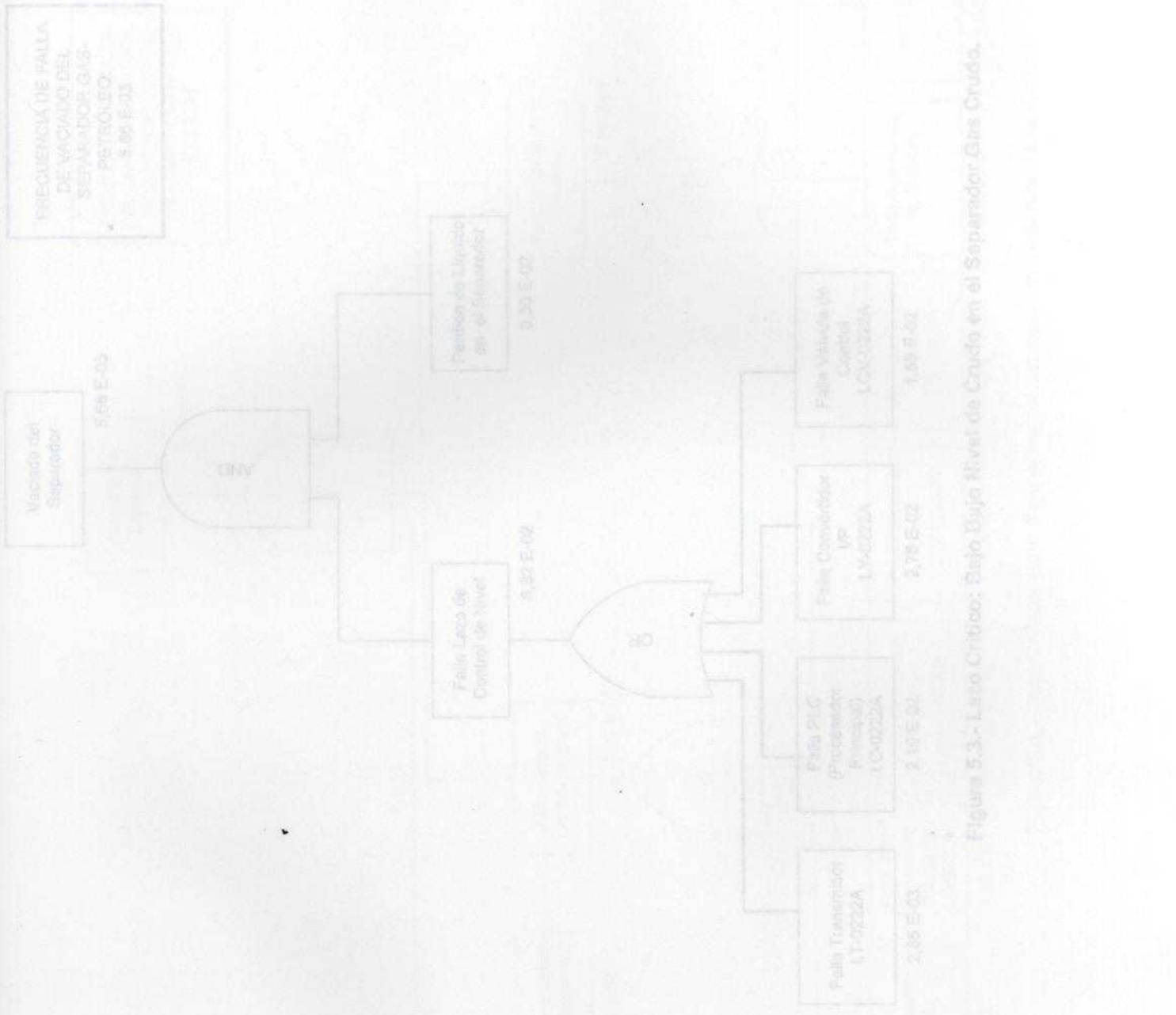


Figura 5.3.- Lazo Crítico: Bajo Bajo Nivel de Crudo en el Separador Gas Crudo.

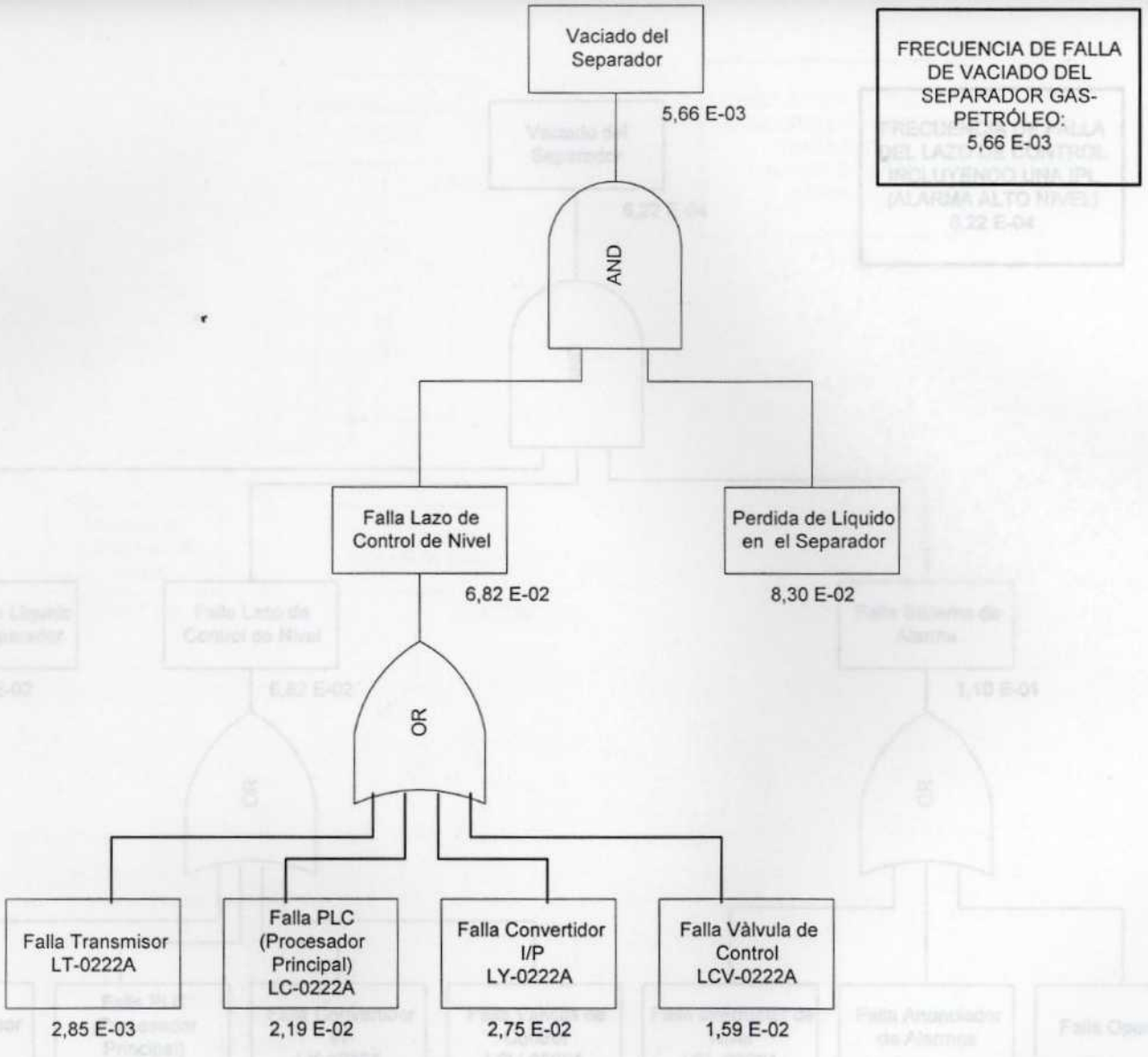


Figura 5.3.- Lazo Critico: Bajo Bajo Nivel de Crudo en el Separador Gas Crudo.

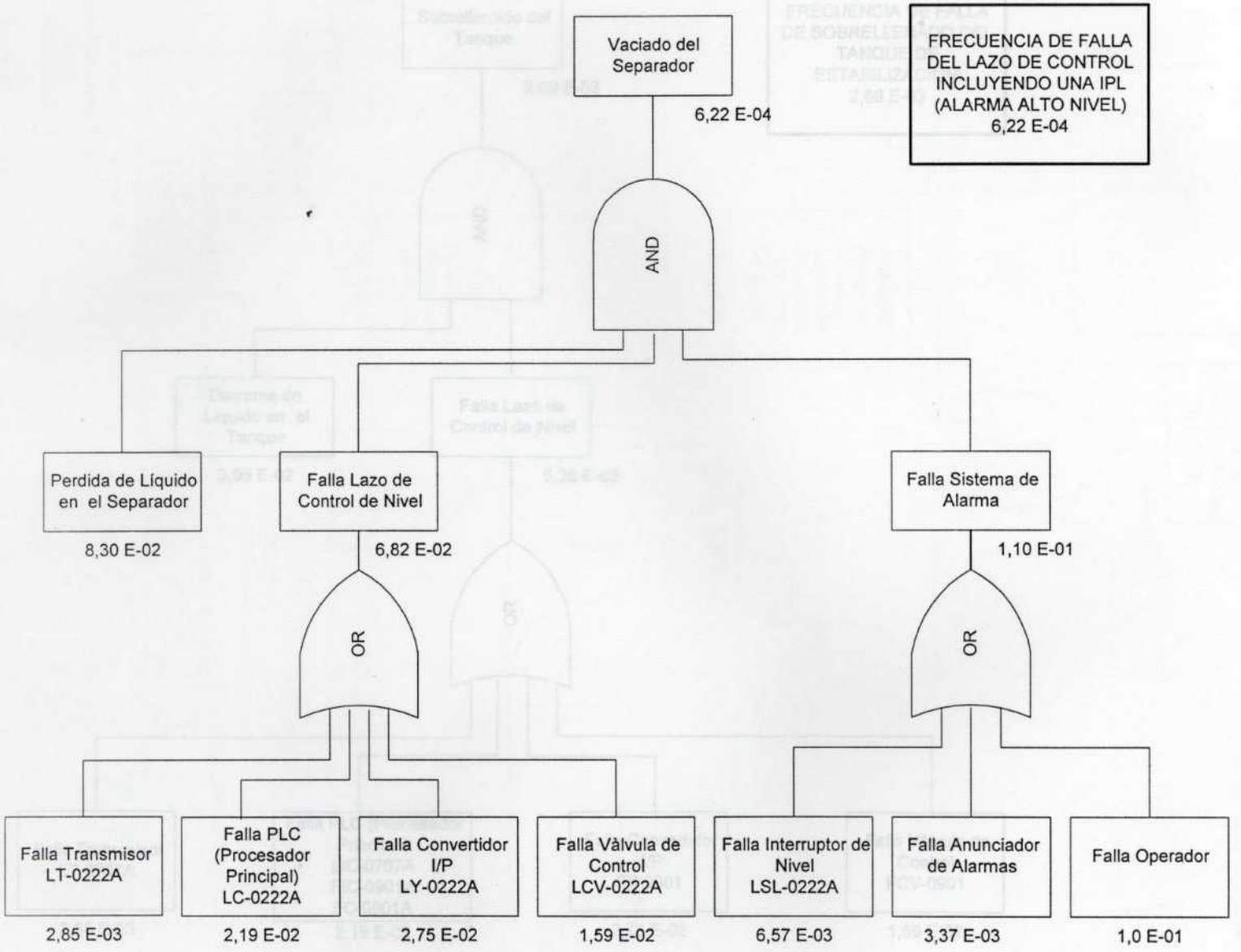


Figura 5.4.- Lazo Critico: Bajo Bajo Nivel de Crudo en el Separador Gas Crudo.

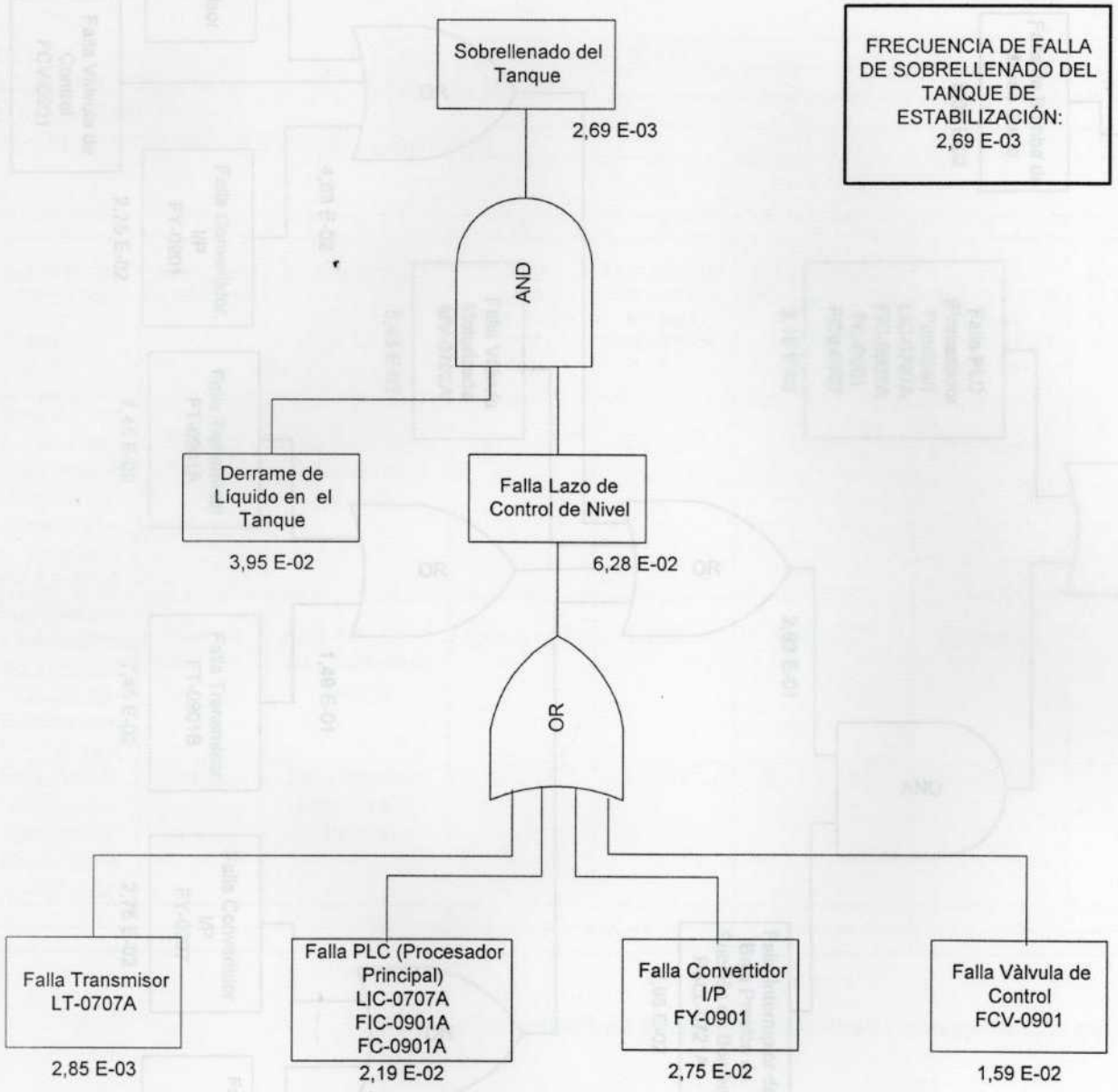


Figura 5.5.- Lazo Critico: Alto Alto Nivel de Crudo en el Tanque de Estabilización.

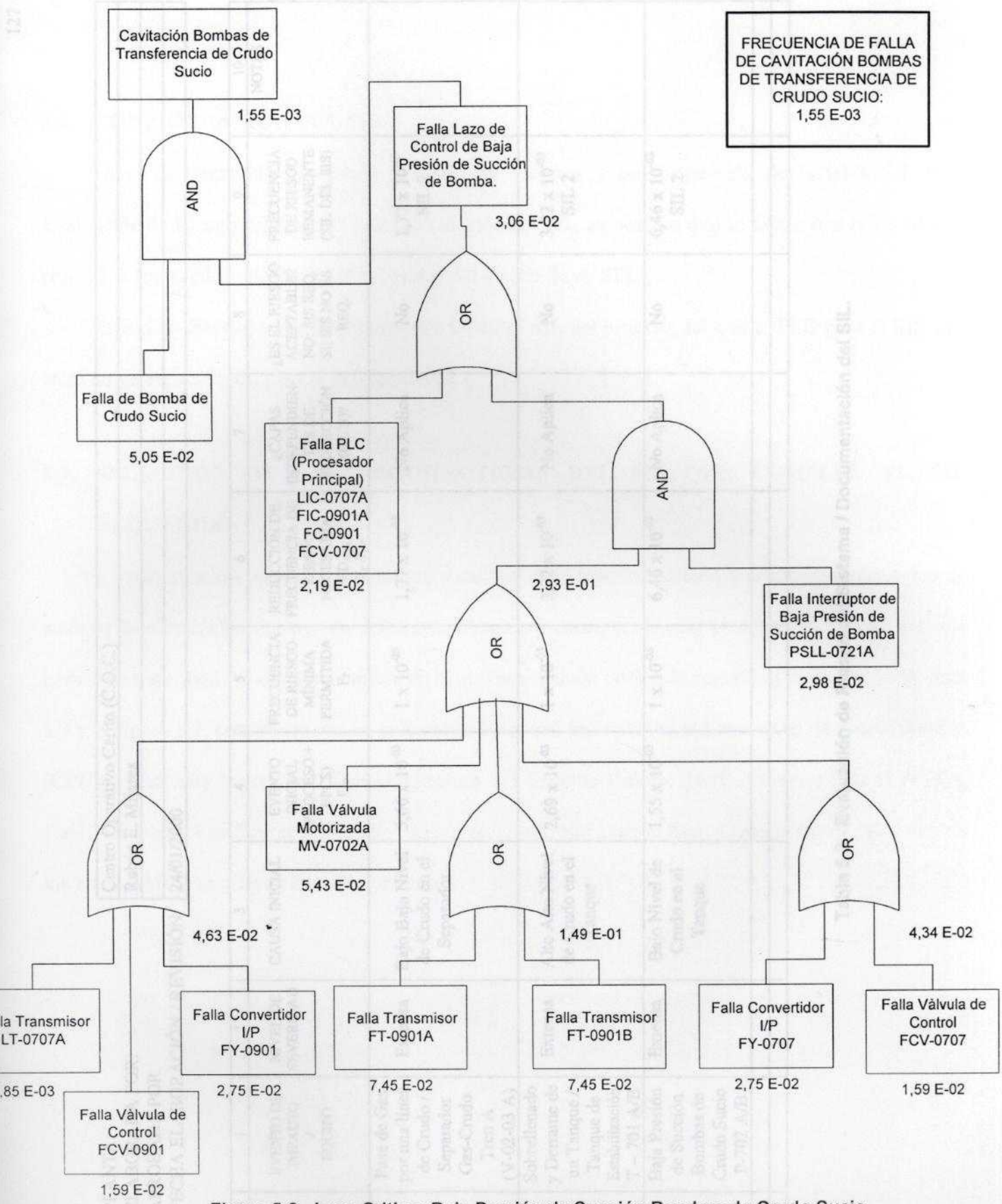


Figura 5.6.- Lazo Critico: Baja Presión de Succión Bombas de Crudo Sucio P-702A/B.

PLANTA:	Centro Operativo Carito (C.O.C.)
ELABORADA POR:	Rubén E. Mijares
APROBADA POR	
FECHA ELABORACIÓN / REVISIÓN	24/01/2000

#	1	2	3	4	5	6	7	8	9	10
	EVENTO DE IMPACTO / EQUIPO	NIVEL DE SEVERIDAD	CAUSA INICIAL	EVENTO INICIAL (PROCESO + BPCS) F_{NP}	FRECUENCIA DE RIESGO MÍNIMA PERMITIDA F_P	REDUCCIÓN DE FRECUENCIA DE RIESGO NECESARIA $PFD_{AVG} = F_P / F_{NP}$	¿CAPAS INDEPENDIENTES DE PROTECCIÓN (IPL'S)?	¿ES EL RIESGO ACEPTABLE? NO: SIS REQ. SI: SIS NO ES REQ.	FRECUENCIA DE RIESGO REMANENTE (SIL DEL SIS)	NOTAS
1	Pase de Gas por una línea de Crudo / Separador Gas-Crudo Tren A (V-02-03 A)	Extensa	Bajo Bajo Nivel de Crudo en el Separador	$5{,}66 \times 10^{-03}$	1×10^{-05}	$1{,}77 \times 10^{-03}$	No Aplica	No	$1{,}77 \times 10^{-03}$ SIL 2	
2	Sobrellenado y Derrame de un Tanque / Tanque de Estabilización T – 701 A/B	Extensa	Alto Alto Nivel de Crudo en el Tanque	$2{,}69 \times 10^{-03}$	1×10^{-05}	$3{,}72 \times 10^{-03}$	No Aplica	No	$3{,}72 \times 10^{-03}$ SIL 2	
3	Baja Presión de Succión Bombas de Crudo Sucio P-702 A/B	Extensa	Bajo Nivel de Crudo en el Tanque	$1{,}55 \times 10^{-03}$	1×10^{-05}	$6{,}46 \times 10^{-03}$	No Aplica	No	$6{,}46 \times 10^{-03}$ SIL 2	
4										
5										

Tabla 5.2.- Evaluación de Riesgo del Sistema / Documentación del SIL.

5.6. CONFIGURACIÓN DEL SIS.

Una vez terminado el cálculo del SIL del Proceso, y por inspección de la tabla 5.2 de la Evaluación de Riesgo del Sistema / Documentación del SIL, se observa que se tienen tres lazos críticos con SIL 2 todos ellos, indicando la necesidad del diseño de un SIS.

El SIS es diseñado y configurado para lograr el SIL del proceso, tal que el PFD para el SIS este en el rango especificado para el SIL requerido.

5.7. SELECCIÓN DE LAS ARQUITECTURAS DEL SIL QUE CUMPLEN EL SIL REQUERIDO.

Se tienen muchas opciones para el tipo y calidad de la instrumentación a seleccionar. En orden de analizar la efectividad del uso de diferentes arreglos y configuraciones, se comenzó con un sistema básico de seguridad. El sistema consiste de la instrumentación critica de seguridad mostrada en la tabla 5.3 y la figura 5.7, controlada por un solo controlador con una sola unidad de central de procesamiento (CPU) y una sola tarjeta de I/O. (Arquitectura del Sistema Básico: 1oo1 (Sensores), 1oo1 (CPU), 1oo1(Válvulas). Las figuras 5.8 y 5.9 representan la instrumentación básica requerida por cada uno de los lazos críticos mencionados anteriormente.

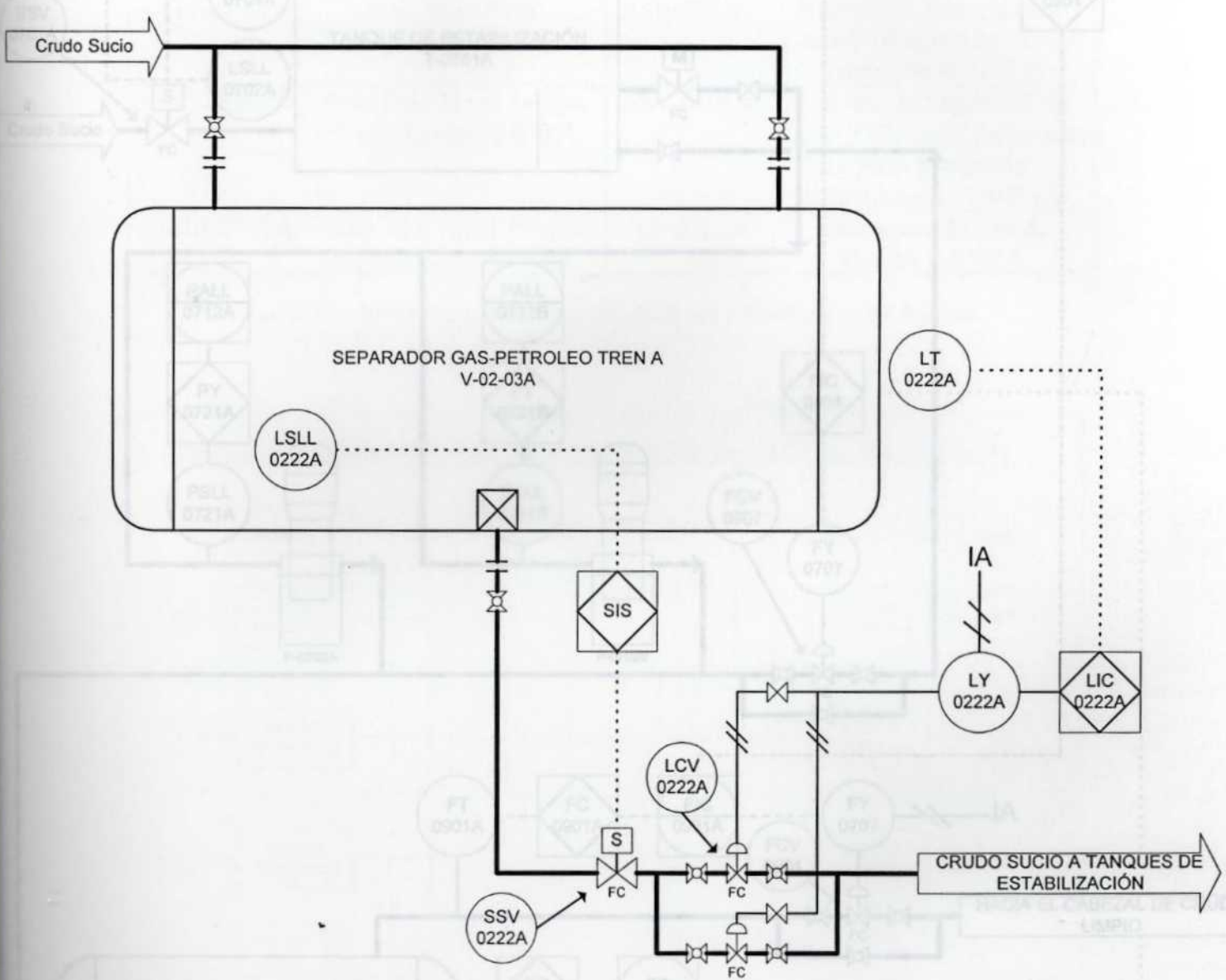


Figura 5.7.- Instrumentación Lazo Critico: Bajo Bajo Nivel de Crudo en el Separador Gas- Crudo V-02-03.

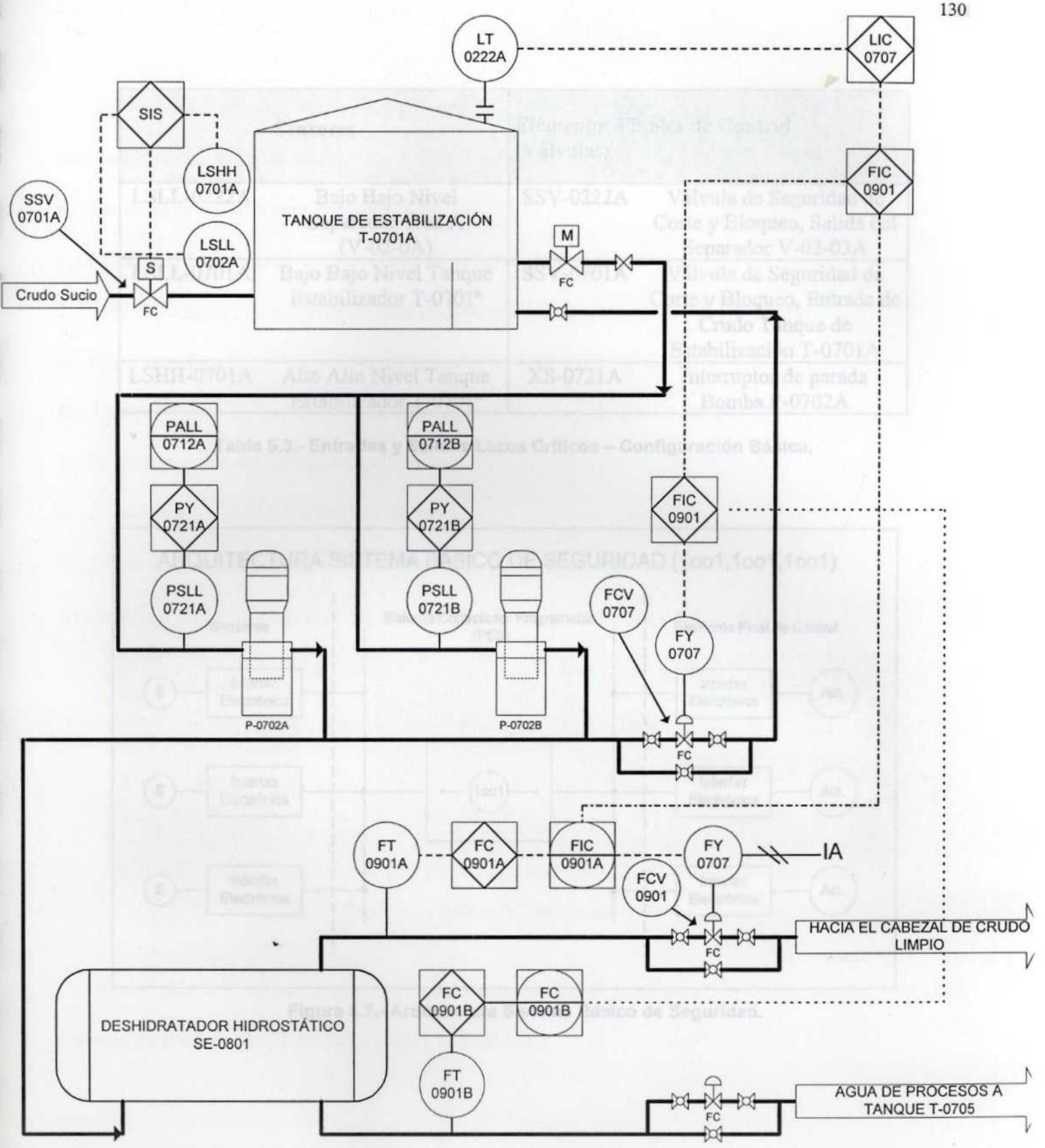


Figura 5.8.- Alto Alto Nivel de Crudo en el Tanque de Estabilización de Crudo T-0701A y Baja Presión de Succión Bombas de Crudo Sucio P-0702 A/B.

Sensores		Elementos Finales de Control (Válvulas)	
LSLL-0222A	Bajo Bajo Nivel Separador Tren A (V-02-0A)	SSV-0222A	Válvula de Seguridad de Corte y Bloqueo, Salida del Separador V-02-03A
LSLL-0701A	Bajo Bajo Nivel Tanque Estabilizador T-0701ª	SSV-0701A	Válvula de Seguridad de Corte y Bloqueo, Entrada de Crudo Tanque de Estabilización T-0701A
LSHH-0701A	Alto Alto Nivel Tanque Estabilizador T-0701ª	XS-0721A	Interruptor de parada Bomba P-0702A

Tabla 5.3.- Entradas y Salidas Lazos Críticos – Configuración Básica.

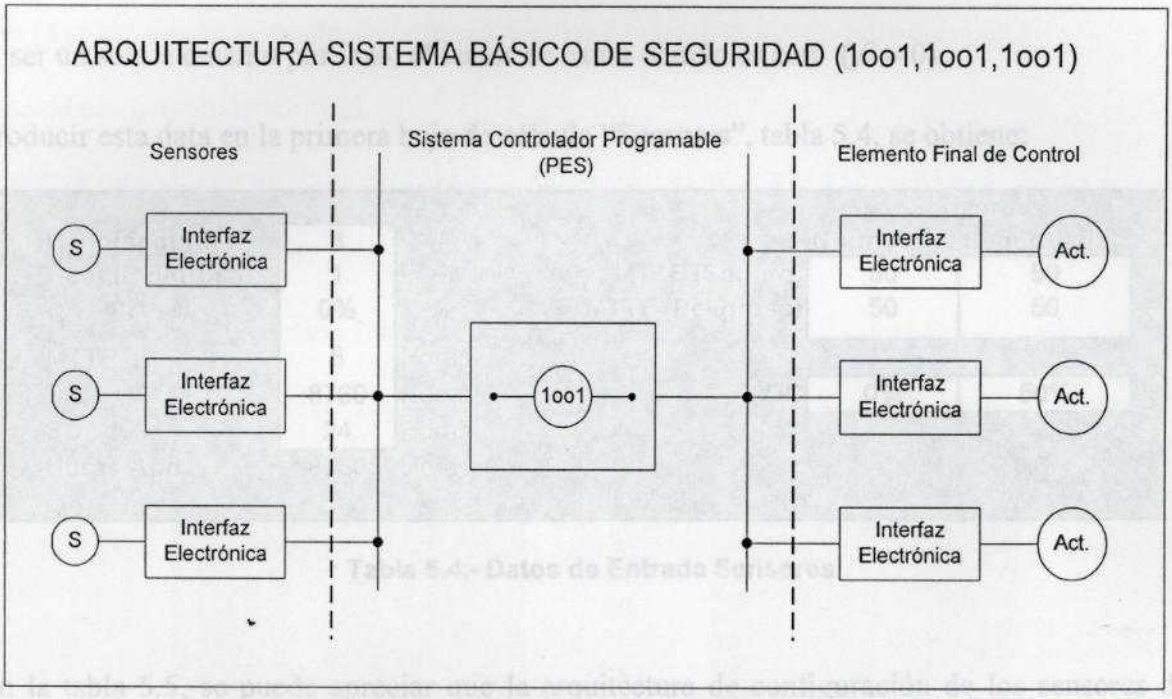


Figura 5.7.- Arquitectura Sistema Básico de Seguridad.

Para el análisis de los resultados se asumió la siguiente data para cada uno de los elementos involucrados en las arquitecturas finales del sistema:

- **Datos para los sensores de campo:**

1. MTTF = 50 años (para los dos modos de falla: seguro y peligroso).
2. Tres (3) sensores en el modo de falla segura, uno (1) en el modo de falla peligrosa.
3. Son interruptores que no poseen capacidades de diagnóstico (DC = 0).
4. Tiempo Promedio de pruebas manuales es de una vez al año (8760 horas).
5. El tiempo de reparación de ocho (8) horas.
6. Arquitectura o configuración inicial: 1oo1.
7. Al ser un solo elemento por lazo, el factor de causa común es cero ($\beta = 0$).

Al introducir esta data en la primera hoja de cálculo "Sensores", tabla 5.4, se obtiene:

				Sensores	
Cant (segura)	3	Usualmente Todos		Normal	Seguridad
Cant (Peligrosa)	1	Usualmente 1	MTTF (Seguro)	50	50
β	0%	%	MTTF (Peligroso)	50	50
MTTR	8	Horas			
T_1	8760	Horas	DC	0%	50%
SD	24	Horas			
Horas Año	8760	Horas			

Tabla 5.4.- Datos de Entrada Sensores.

En la tabla 5.5, se puede apreciar que la arquitectura de configuración de los sensores de 1oo1 presenta un RRF de 100, y un valor de MTTFS de 16,67.

RESULTADOS				
	PFD	PFS	RRF	MTTFS
1oo1	1,00E-02	1,64E-04	100	16,67
1oo2	1,33E-04	3,29E-04	7.500	8,33
2oo3	4,00E-04	5,92E-05	2.500	46,30
2oo2	2,00E-02	1,97E-05	50	138,89
1oo1D	5,00E-03	1,92E-04	200	14,29
2oo2D	1,00E-02	1,15E-05	100	237,81
1oo2D	3,33E-05	9,00E-04	30.000	3,04

Tabla 5.5.- Resultados Sensores.

- **Datos de los elementos finales de control (válvulas):**

1. MTTF = 50 años (para los dos modos de falla: seguro y peligroso).
2. Tres (3) válvulas en el modo de falla segura, tres (3) en el modo de falla peligrosa.
3. Capacidad de diagnóstico: 0%.
4. Tiempo Promedio de pruebas manuales es de una vez al año (8760 Horas/Año).
5. El tiempo de reparación de ocho (8) horas.
6. Arquitectura o configuración inicial: 1oo1.

Al introducir la data en la tercera hoja de calculo "Válvulas", tabla 5.6, se obtiene lo siguiente:

	Válvulas	
Cantidad (Segura)	3	Usualmente Todos
Cantidad (Peligrosa)	3	Usualmente Todos
MTBF (Seguro)	50	Años
MTBF (Peligroso)	50	Años
DC	0%	%
β	0%	%
MTTR (horas)	8	
T_1 (horas)	4380	
SD (horas)	8	

Tabla 5.6.- Datos de Entrada Válvulas.

En la tabla 5.7, se observa que los resultados para una configuración de 1oo1, el RRF es de 67.

RESULTADOS

	PFD	PFS	RRF	MTTFS
1oo1	1,50E-02	5,48E-05	67	16,67
1oo2	3,00E-04	1,10E-04	3.333	8,33
2oo2	3,00E-02	3,29E-06	33	277,78

Tabla 5.7.- Resultados Válvulas.

- **Datos genéricos de un PLC de Seguridad:**

1. I/O Rata de Falla de los módulos = 50 años, 75% de Falla-Segura (75% Fail-Safe).
2. Rata de Falla del CPU = 10 años, 60% de Falla-Segura (60% Fail-Safe).
3. 97% de Factor de Diagnóstico Automático.
4. 0% de Factor Beta de Causa Común (β).
5. Tiempo Promedio de pruebas manuales es de una vez al año.
6. Asumiendo el resto de los datos tales como: MTTR = 8 Horas, SD = 8 Horas.
7. Arquitectura o configuración inicial: 1oo1.

Al introducir la data en la tercera hoja de calculo "Controlador", tabla 5.8, se obtiene lo siguiente:

	Entradas Digitales	Salidas Digitales	Entradas Analógicas	CPU
Cant. Módulos (Seguros)	**3**	**3**	**0**	1
Cant. Módulos (Peligroso)	**1**	**3**	**0**	1
MTTF (Total)	**50**	**50**	**50**	**10**
% Failsafe	**75%**	**75%**	**75%**	**60%**
DC (%)	**97%**	**97%**	**97%**	**97%**
β(%)	0%	0%	0%	**0%**
MTTR (Hs)	8	8	8	**8**
$T_{1\ (Hs)}$	8760	8760	8760	**8760**
SD (Hs)	8	8	8	**8**

Tabla 5.8.- Datos de Entrada CPU.

Al observar el Factor de Riesgo (RRF) en la tabla 5.9, se tiene una reducción para esta configuración de CPU (1oo1) de 1.049, donde este valor representa un desempeño en el tope de SIL 2.

RESULTADOS				
	PFD	PFS	RRF	MTTFS
1oo1	9,53E-04	1,37E-04	1.049	6,67
1oo2	1,08E-06	2,74E-04	923.510	3,33
2oo3	3,39E-06	3,81E-06	294.813	239,83
2oo2	1,91E-03	1,27E-06	525	719,50
1oo1D	9,00E-04	1,90E-04	1.111	4,80
2oo2D	1,80E-03	1,78E-06	556	512,49
1oo2D	1,08E-06	2,03E-05	925.926	45,02

Tabla 5.9.- Resultados CPU.

Con los valores antes descritos, en la cuarta hoja de cálculo "Resumen" para la configuración de "1oo1,1oo1,1oo1" se observa lo siguiente, tabla 5.10:

Sistema Configuración	PFD	RRF	PFS	MTTFS	SIL
1oo1,1oo1,1oo1	2,6E-02	38,53	2,8E-04	5,43	1

Tabla 5.10.- Resumen Resultados Sistema Instrumentado de Seguridad.

El valor de Reducción del Factor de Riesgo (RRF) para el sistema completo (SIS) es de 38,53; esta valor representa un desempeño de SIL 1.

En resumen los resultados que se obtiene son los siguientes, tabla 5.11:

	Sensores	CPU (Logic Solvers)	Válvulas	Sistema
PFD	1,0 E-02	9,53E-04	1,5E-02	2,6E-02
RRF	100	1.049	67	38,53
PFS	1,64 E-04	1,37E-04	5,48E-05	2,8 E-04
SIL	1	2	1	1

Tabla 5.11.- Arquitectura 1oo1 (Sensores), 1oo1 (CPU), y 1oo1 (Válvulas).

Por inspección se observa que el CPU cumple el valor de SIL asignado (SIL 2), mas no así los elementos de campo (sensores y válvulas).

Al mejorar toda esta instrumentación y colocar transmisores en vez de interruptores y las válvulas en configuración dual, se obtienen s cambios considerables en los resultados.

- **Datos para los Sensores (Transmisores) de campo:**

1. MTTF = 100 años (para los dos modos de falla: seguro y peligroso).
2. Tres (3) sensores en el modo de falla segura, uno (1) en el modo de falla peligrosa.
3. Diagnóstico en línea (DC): 80.
4. Tiempo Promedio de pruebas manuales es de una vez al año.
5. El tiempo de reparación de ocho (8) horas.
6. Arquitectura o configuración: 1oo1.
7. Factor de causa común.

Al introducir esta data en la primera hoja de cálculo "Sensores", tabla 5.12, se obtiene:

				Sensores	
Cant (segura)	**3**	Usualmente Todos		**Normal**	**Seguridad**
Cant (Peligrosa)	**1**	Usualmente Todos	**MTTF (Seguro)**	**100**	**50**
β	**0%**	%	**MTTF (Peligroso)**	**100**	**50**
MTTR	**8**	Horas			
T_1	**8760**	Horas	**DC**	**80%**	**50%**
SD	**24**	Horas			
Horas Año	8760	Horas			

Tabla 5.12.- Datos de Entrada Sensores.

En la tabla 5.13 se aprecia que la arquitectura de los transmisores de 1oo1, el RRF es de 993, cumpliendo este valor el SIL asignado (SIL 2).

RESULTADOS				
	PFD	**PFS**	**RRF**	**MTTFS**
1oo1	1,01E-03	8,22E-05	993	33,33
1oo2	1,33E-06	1,64E-04	749.970	16,67
2oo3	4,02E-06	2,97E-06	248.628	922,56
2oo2	2,01E-03	9,90E-07	496	2.767,67
1oo1D	5,00E-03	1,92E-04	200	14,29
2oo2D	1,00E-02	1,15E-05	100	237,81
1oo2D	3,33E-05	9,00E-04	30.000	3,04

Tabla 5.13.- Resultados Sensores.

- **Datos para las válvulas:**

1. MTTF = 50 años (para los dos modos de falla: seguro y peligroso).
2. Tres (3) válvulas en el modo de falla segura, tres (3) en el modo de falla peligrosa.
3. Capacidad de diagnóstico: 0%.
4. Factor de Causa Común: $\beta = 10$
7. Tiempo Promedio de pruebas manuales es de una vez al año (8760 Horas/Año).
8. El tiempo de reparación de ocho (8) horas.
9. Arquitectura o configuración inicial: 1oo2.

Al introducir la data en la tercera hoja de calculo "Válvulas", tabla 5.14, se obtiene:

	Válvulas	
Cantidad (Segura)	**3**	Usualmente Todos
Cantidad (Peligrosa)	**3**	Usualmente Todos
MTBF (Seguro)	**50**	Años
MTBF (Peligroso)	**50**	Años
DC	**0%**	%
b	**10%**	%
MTTR (horas)	**8**	
T_1 (horas)	**4380**	
SD (horas)	**8**	

Tabla 5.14.- Datos de Entrada Válvulas.

Para la configuración de 1oo2 para las válvulas, el RRF es de 574, que corresponde al SIL 2, tabla 5.15:

RESULTADOS	PFD	PFS	RRF	MTTFS
1oo1	1,50E-02	5,48E-05	67	16,67
1oo2	1,74E-03	1,04E-04	574	8,77
2oo2	2,85E-02	8,14E-06	35	112,16

Tabla 5.15.- Resultados Válvulas Configuración 1oo2.

Con esta configuración del sistema 1oo1 (Sensores), 1oo1 (CPU), 1oo2 (Válvulas), en la cuarta hoja de calculo "Resumen", se observa lo siguiente, tabla 5.16:

Sistema Configuración	PFD	RRF	PFS	MTTFS	SIL
1oo1,1oo1,1oo2	3,7E-03	270,02	1,1E-04	16,22	2

Tabla 5.16.- Resumen Resultados SIS.

El valor de RRF para el sistema completo en la configuración designada de (1oo1,1oo1,1oo2) es de 270,02, este valor esta ubicado a un tercio (1/3) en el rango de RRF del SIL 2 (Rango 100 < RRF <1.000), lo cual es conveniente mejorarlo a un valor en el rango medio superior ($500 \leq RRF \geq 1.000$), para así garantizar una efectiva reducción de riesgo.

A través de la hoja de Resumen se verificó que configuración o arquitecturas cumplen este requerimiento, obteniendo lo siguiente, tabla 5.17:

Sistema Configuración	PFD	RRF	PFS	MTTFS	SIL
1oo1,1oo1,1oo2	3,7E-03	270,02	1,1E-04	16,22	2
1oo2,1oo2,1oo2	1,8E-03	561,71	1,9E-04	5,08	2
1oo2,1oo2D,1oo2	1,8E-03	562,32	1,8E-04	12,64	2
1oo2,2oo3,1oo2	1,9E-03	539,86	4,4E-04	2,76	2
1oo2D,1oo2,1oo2	1,8E-03	561,71	6,5E-05	22,33	2
1oo2D,1oo2D,1oo2	1,8E-03	562,32	5,3E-05	30,98	2
1oo2D,2oo3,1oo2	1,9E-03	539,86	3,1E-04	3,17	2
2oo3,1oo2,1oo2	1,8E-03	560,86	3,2E-05	30,56	2
2oo3,1oo2D,1oo2	1,8E-03	561,47	2,0E-05	7,98	2
2oo3,2oo3,1oo2	1,9E-03	539,08	2,8E-04	2,45	2

Tabla 5.17.- Resumen de Arquitecturas.

De las diferentes configuraciones en la tabla 5.17, se observa que al cambiar la arquitectura de los elementos Sensores y del CPU de 1oo1 a 1oo2, el RRF del sistema configuración (1oo2,1oo2,1oo2) pasa de 270,02 a 561,02; que es el valor deseado.

Lo mismo es cierto para todas las otras configuraciones mostradas que cumplen el requerimiento deseado.

CONCLUSIONES

Se logró desarrollar una metodología para el Sistema Instrumentado de Seguridad (SIS) que permite alcanzar la disponibilidad requerida para el nivel de Integridad de Seguridad (SIL) que cumplen con las Normas que aplica la Industria Petrolera Nacional tales como: Manual de Ingeniería de Riesgo (PDVSA-MIR) y el Manual de Ingeniería de Diseño (PDVSA-MID).

Esta metodología se aplicó en el estudio y diseño de la arquitectura del Sistema Instrumentado de Seguridad (SIS) de cuatro lazos de control críticos de la Estación de Producción de Carito (COC).

La metodología desarrollada permite determinar a través de métodos cuantitativos (Análisis de Árbol de Fallas y Cálculos de Confiabilidad) cual debe ser la configuración ÓPTIMA de la instrumentación de los Sistemas Instrumentados de Seguridad requeridos por la industria.

La metodología se baso en el análisis hecho por Williams Globe [2], en donde se modifican las ecuaciones de confiabilidad del sistema por ecuaciones de confiabilidad promedio del sistema.

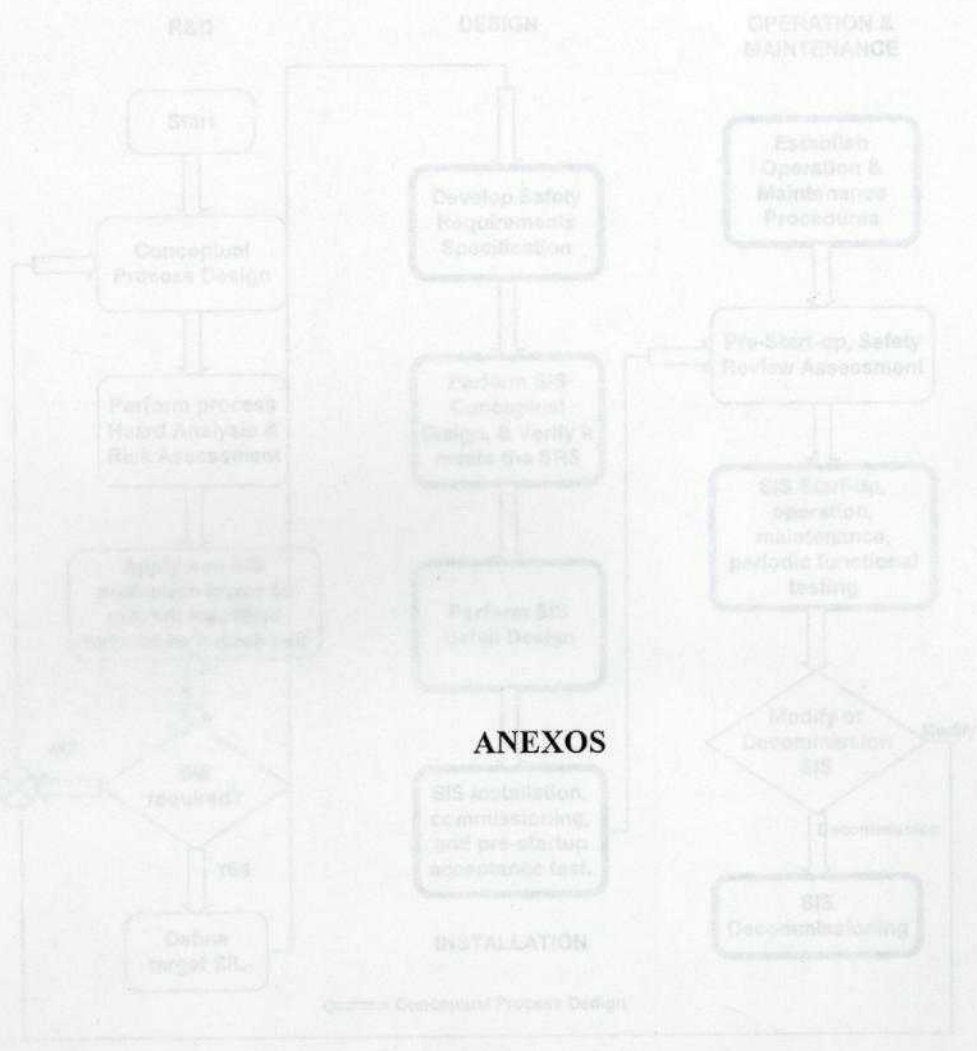
Para el momento de las primeras pruebas de la metodología desarrollada se usó la base de datos de confiabilidad de equipos indicada en la Norma PDVSA-MIR y se determinó que no era la más adecuada ya que es un anecdótico o el resultado de una data que se recoge al azar. Para solventar esta situación se probó con la base de datos suministrada por "Process Equipment Realibility Data" y fundamentalmente la "Offshore Realibility Data Hand Book (OREDA)", obteniéndose los resultados

esperados. La base de datos utilizada es la Frecuencia de Fallas Peligrosas No-detectadas.

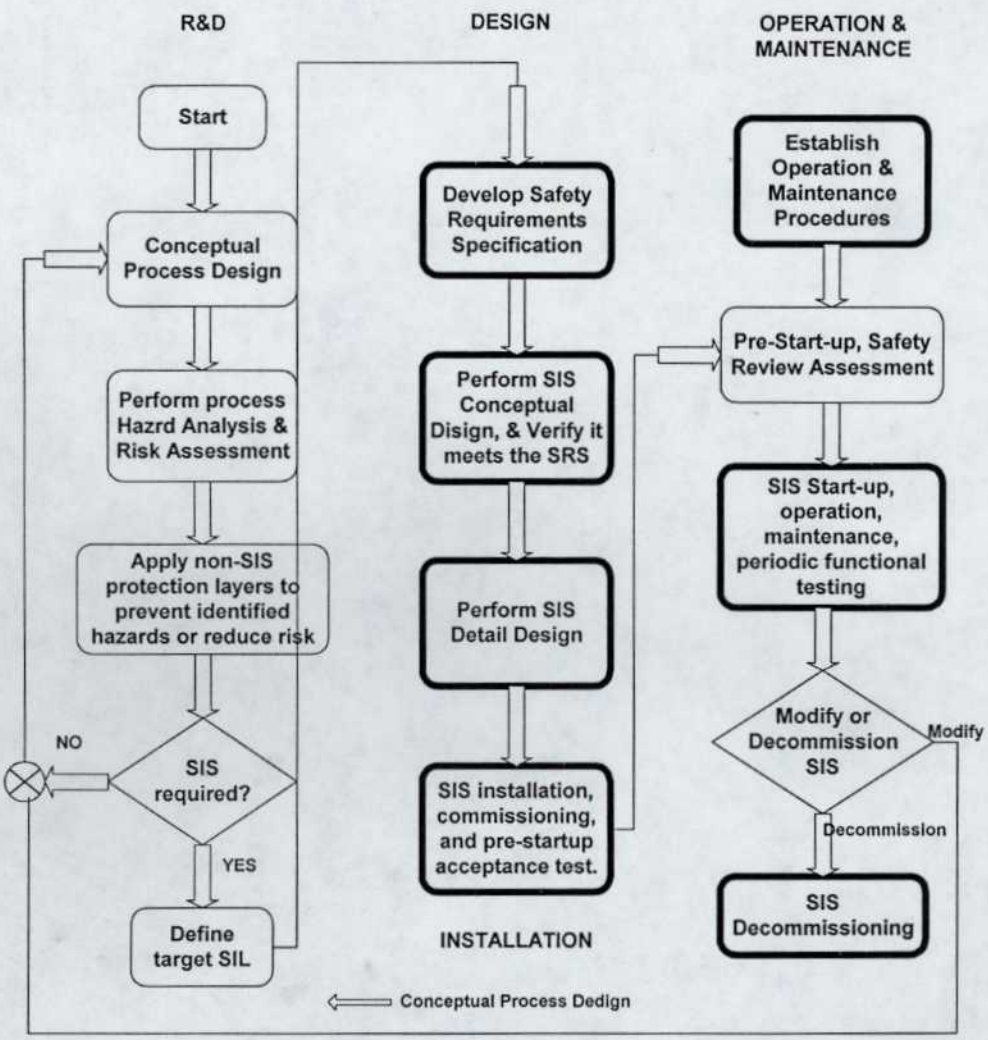
Para la aplicación de la metodología desarrollada es indispensable el conocimiento previo técnico-teórico de las Normas de Ingeniería de Seguridad e Instrumentación de la Industria.

REFERENCIAS BIBLIOGRÁFICAS

1. PDVSA (Petróleos de Venezuela).
   - IR-S-00 Definiciones
   - IR-S-02 Criterios para el Análisis Cuantitativo de Riesgos
   - IR-P-01 Safety Interlock Systems,Emergency Isolation, Emergency Despressurization and Emergency Venting Systems.
2. Goble, William M. Control Systems, Safety Evaluation & Realiability.
3. ISA – Instrument Society of América.
   - ISA S84.01; Application of Safety Instrumented Systems for the Process Industry.
   - Technical Report ISA TR84.0.02
4. Oreda-92, Offshore Reliability Data Handbook, 2nd Edition, Norway, ISBN 82-515-0188-1, 1992.
5. Dowell Arthur M. Technical Fellow, Risk Analysis, III.
6. CCPS – Center for Chemical Process Safety.
   - Guidelines for Safe Automation of Chemical Processes.
7. IEC– International Electrotechnical Commission.
   - IEC-d61508; Functional Safety of Electric/ Electronic/ Programmable Electronic Systems.


R&D
DESIGN
OPERATION &
MAINTENANCE
Start
Conceptual
Process Design
Perform process
Hazard Analysis &
Risk Assessment
Develop Safety
Requirements
Specification
Perform SIS
Conceptual
Design, & Verify it
meets the SRS
Perform SIS
Detail Design
SIS installation,
commissioning,
and pre-startup
acceptance test.
INSTALLATION
Establish
Operation &
Maintenance
Procedures
Pre-Start-up Safety
Review Assessment
SIS start-up,
operation,
maintenance,
periodic functional
testing
Modify or
Decommission
SIS
Decommission
SIS
Decommissioning
SIS
required?
YES
Define
target SIL

ANEXOS



ANEXO 1: Norma ISA-S84.01-1996, pasos para diseñar un Sistema Instrumentado de Seguridad (SIS) a partir de un Índice de Integridad (SIL).