UNIVERSIDAD POLITÉCNICA SALESIANA

UNIDAD DE POSGRADOS

MAESTRÍA EN CONTROL Y AUTOMATIZACIÓN INDUSTRIALES

Tesis previa a la obtención
del Grado de Magister
en Control y
Automatización Industriales

LA SEGURIDAD FUNCIONAL EN LA INDUSTRIA DE PROCESOS: CONCEPTOS Y METODOLOGIAS DE DISEÑO

Autor:
Fernando Venegas Riera.

Director:
Rafael Barreto Jijón

LA SEGURIDAD FUNCIONAL EN LA INDUSTRIA DE PROCESOS: CONCEPTOS Y METODOLOGIAS DE DISEÑO

LA SEGURIDAD FUNCIONAL EN LA INDUSTRIA DE PROCESOS: CONCEPTOS Y METODOLOGIAS DE DISEÑO

KLEVER FERNANDO VENEGAS RIERA
Ingeniero Electrónico Industrial
Egresado de la Maestría en Control y Automatización Industriales
Facultad de Ingenierías
Universidad Politécnica Salesiana

Dirigido por:

RAFAEL ANGEL BARRETO JIJÓN
Máster en Electrónica, Ingeniería Eléctrica, Automatización y Procesamiento de Señales
TÜV Functional Safety Professional
ISA84 SIS Fundamentals Specialist
Docente de la Universidad Politécnica Salesiana
Docente de la Universidad San Francisco de Quito
Miembro IEEE, Miembro ISA

Cuenca – Ecuador

Datos de catalogación bibliográfica

VENEGAS RIERA KLEVER FERNANDO

LA SEGURIDAD FUNCIONAL EN LA INDUSTRIA DE PROCESOS: CONCEPTOS Y METODOLOGIAS DE DISEÑO

Universidad Politécnica Salesiana, Cuenca – Ecuador, 2013.
MAESTRIA EN CONTROL Y AUTOMATIZACIÓN INDUSTRIALES

FORMATO: 170x240 Páginas: 130

Breve reseña del Autor e información de contacto:

Klever Fernando Venegas Riera.
Ingeniero Electrónico Industrial.
Graduado de la Carrera de Ingeniería Electrónica.
Facultad de Ingenierías.
Universidad Politécnica Salesiana.
kelvo763@hotmail.com

Dirigido por:

Rafael Ángel Barreto Jijón
Máster en Electrónica, Ingeniería Eléctrica, Automatización y Procesamiento de Señales.
TÜV Functional Safety Professional.
ISA84 SIS Fundamentals Specialist.
Docente de la Universidad Politécnica Salesiana.
Docente de la Universidad San Francisco de Quito.
Miembro IEEE, Miembro ISA
rafael.barreto.jijon@gmail.com

Edición y Producción:
Klever Fernando Venegas Riera.
Diseño de la portada:
Klever Fernando Venegas Riera.
IMPRESO EN ECUADOR – PRINTED IN ECUADOR

A mis padres, hermanos, sobrino y abuelos…
de ellos proviene mi esencia.

Índice General

Índice de Figuras

Índice de Tablas

PREFACIO

Esta tesis es el resultado de un proyecto de tesis de maestría en control y automatización industriales para la Universidad Politécnica Salesiana (UPS). El trabajo fue llevado a cabo entre abril de 2013 y enero de 2014, en estrecha colaboración con el director de tesis, Rafael Barreto Jijón, y su contribución se refleja a lo largo del desarrollo de este proyecto.

El Ing. Giovanny Quinde, jefe de seguridad del grupo Graiman ha contribuido como supervisor debido a su amplia experiencia en la seguridad industrial.

El proyecto de tesis de maestría ha sido una oportunidad para hacer contribuciones a un campo en el que se ha tomado gran interés, a saber, la fiabilidad de los sistemas instrumentados de seguridad. Se espera que el conocimiento aquí desarrollado sea utilizado como base para el avance e implementación de sistemas instrumentados de seguridad en la industria de procesos, desarrollando diseños fiables y garantizando el funcionamiento de tales sistemas.

AGRADECIMIENTOS

En primer lugar quiero agradecer a Dios por bendecirme y permitirme llegar hasta donde he llegado, porque hizo realidad este sueño anhelado.

A mi director de tesis, Rafael Barreto J, quien con sus conocimientos, su experiencia, su paciencia y su motivación contribuyó a que pueda terminar mis estudios con éxito.

Al Ing. Giovanny Quinde, jefe de seguridad del grupo Graiman por todo el apoyo brindado.

A todas las personas que participaron e hicieron posible este proyecto, muchas gracias por su apoyo y enseñanzas. Pero sobre todo, gracias a mi familia que a pesar de todas las adversidades nunca soltaron mi mano y me motivaron a seguir.

Capítulo 1

INTRODUCCIÓN

El avance tecnológico está presente en muchos campos tales como aviación, comunicaciones y procesos industriales, pero así como se da dicho avance, el riesgo de presentarse una catástrofe en cualquier campo también se incrementa. En muchas industrias se ha remplazado personal por sistemas automatizados para obtener un aumento en la producción, pero en la mayoría de las ocasiones no se considera el nivel de seguridad que debe mantenerse al realizar una automatización ya que los procesos industriales tienen el potencial de provocar catástrofes a gran escala.

Las situaciones de riesgo deben anticiparse y prevenirse ya que pueden afectar el desarrollo sostenible, es decir, producir muertes, daños a la maquinaria, afectar el medio ambiente y generar pérdidas económicas considerables. Por otra parte el concepto de seguridad industrial se ha limitado a la seguridad ocupacional, refiriéndose al equipamiento del cual se dispone al presentarse una emergencia como extintores, cascos, chalecos reflectivos y arnés de seguridad. Pocos profesionales en seguridad tienen conocimiento del tema de Sistemas Instrumentados de Seguridad (SIS) pero no lo ponen en práctica, lo que demuestra la falta de interés, falta de conocimiento o falta de recursos económicos en la aplicación de estos sistemas en los procesos industriales.

Los ingenieros responsables en seguridad en algunas industrias de procesos de la ciudad, regularmente se enfocan en lo que se refiere a seguridad y salud ocupacional, es decir, codificación y delimitación de zonas. Por ejemplo, en la localidad en una fábrica textil y una fábrica de pinturas y solventes se concentran en pintar las zonas de cruce de personal, desembarque de materiales, áreas para extintores, mientras que la ejecución de los sistemas de seguridad y de la seguridad funcional no son tomados en cuenta.

Se ha documentado algunos accidentes menores y otros mayores, que podrían haber sido evitados si en la instalación en donde se suscitaron los incidentes se hubieran dispuesto sistemas instrumentados de seguridad, pero como se citó anteriormente, el tema no es aplicado o se desconoce de él.

No se debe confundir seguridad industrial con seguridad funcional ya que son dos temas muy diferentes. La seguridad industrial es un conjunto de técnicas que se encarga de identificar el riesgo y evaluar las medidas correctivas disponibles enfocándose en la protección del operador, mientras que, la seguridad funcional cubre una amplia gama de

dispositivos que se interconectan para formar un sistema de seguridad que se encarga de llevar el proceso a su estado seguro. Algunas ventajas de implementar seguridad funcional en una instalación de procesos son:

- Garantizar que las decisiones de reducción de riesgo se basan en análisis y no en percepción.
- Prevenir eventos antes de que ocurran, evitar lesiones y salvar vidas.
- Alcanzar el desarrollo sostenible.
- Reducir las activaciones esporádicas evitando pérdida de producción.

Con la presente investigación se pretende obtener una idea concreta del estado actual de los SIS en la industria de la ciudad, para ello es necesario conocer su grado de aplicación en la industria de procesos debido a que muchas industrias no disponen de sistemas de seguridad encargados del monitoreo de variables de proceso que puedan resultar en eventos con graves consecuencias.

Se busca demostrar el beneficio de implementar SIS en la industria de procesos, para ello es preciso disponer de información que nos proporcione datos acerca de su utilización, de los niveles de seguridad funcional que se mantienen en la industria y eventos que pudieron convertirse en una catástrofe para prevenir futuras situaciones de riesgo.

Con la implementación de SIS se espera alcanzar el desarrollo sostenible deseado, es decir, precautelar el bienestar del personal, de la maquinaria, del ambiente y el nivel de producción.

Además, se desea proporcionar lineamientos fundamentales para el análisis y diseño de un SIS para el área de almacenamiento de combustibles en TUGALT, el mismo que cumpla con los requisitos de seguridad deseados, es decir, que sea capaz de mitigar las consecuencias que pudieran resultar de un evento inesperado, pero sobre todo, sea idóneo para evitar pérdidas considerables tanto económicas como materiales, así como las vidas de los empleados de la empresa.

Mediante esta investigación se busca evidenciar el ahorro benéfico para la empresa al invertir en el sistema de seguridad para prevenir accidentes o eventos inesperados que pudieran evitarse por la aplicación del SIS. Para ello se considerarán los gastos que la empresa sufre por daños en la línea de producción, así como, indemnización por muerte del personal involucrado en dicho proceso.

Esta tesis es desarrollada para la maestría en control y automatización industrial realizada en la Universidad Politécnica Salesiana. Está orientada para personal con conocimientos o interés en las evaluaciones de seguridad y confiabilidad. También busca proporcionar los conceptos y principios fundamentales de las normas IEC 61511 y IEC 61508.

La tesis consta de cinco capítulos:

1. Capítulo 1: Breve introducción a los sistemas instrumentados de seguridad y por qué son importantes en la industria. Se definen conceptos fundamentales, técnicas de análisis e identificación de riesgos y se realiza una introducción a la normas IEC 61508 e IEC 61511.
2. Capítulo 2: Se revelan nuevos avances y técnicas utilizadas en el desarrollo de los sistemas instrumentados de seguridad. Se analizan las tecnologías aplicadas actualmente así como las tendencias futuras en el desarrollo de nuevas tecnologías.
3. Capítulo 3: Se proporciona información estadística acerca de eventos peligrosos registrados en la industria de procesos en la ciudad de Cuenca, las medidas de prevención de las que disponen las diferentes industrias y se busca evidenciar el beneficio de la aplicación de sistemas instrumentados de seguridad.
4. Capítulo 4: Diseño de un sistema instrumentado de seguridad para el área de almacenamiento de combustible en TUGALT (Fábrica de acero).
5. Capítulo 5: Conclusiones y estudios a futuro.

1.1 Eventos catastróficos registrados a nivel mundial en la industria de procesos.

Son muchos los accidentes que se han presentado en la trayectoria industrial de la humanidad, algunos de los cuales han dejado huellas imborrables en la historia por sus consecuencias. Los accidentes de los que trata este documento son aquellos cuya magnitud y gravedad han sido bastante considerables con respecto a los daños materiales y víctimas fatales. Algunas instalaciones disponían de sistemas instrumentados de seguridad, pero debido a operaciones de mantenimiento o malos procedimientos de operación dichos sistemas fueron anulados, dando lugar a eventos peligrosos que tuvieron consecuencias fatales. Estos accidentes tienen una especial repercusión en la sociedad debido a la gravedad de sus consecuencias y al elevado número de víctimas, heridos, pérdidas materiales y graves daños al medio ambiente.

En la mente de las personas están presentes algunos accidentes ocurridos no hace muchos años y aún ahora en la actualidad, y de los que todavía se están notando sus consecuencias en individuos y medio ambiente.

Algunos ejemplos de ellos son:

FUGA DE GAS TOXICO EN FABRICA DE PESTICIDAS, BHOPAL (DICIEMBRE 1984)

El accidente se produjo al no tomar las debidas precauciones durante las tareas de limpieza y mantenimiento de la planta, lo que hizo que el agua a presión utilizada, cristales de cloruro sódico, restos metálicos y otras impurezas que la misma arrastraba, entraron en contacto con el gas almacenado, iniciando una reacción exotérmica que provocó la apertura por sobrepresión de las válvulas de seguridad de los tanques y con ello la liberación a la atmósfera de gas tóxico; con el agravante de que el sistema de refrigeración de los tanques y el catalizador de gases previo a la salida a la atmósfera, se habían desactivado al mismo tiempo por ahorro de costos.

Al entrar en contacto con la atmósfera, el compuesto liberado comenzó a descomponerse en varios gases muy tóxicos que formaron una nube letal que recorrió a ras de suelo toda la ciudad. Miles de personas murieron de forma casi inmediata asfixiadas por la nube tóxica y otras muchas fallecieron en accidentes al intentar huir de ella durante la desesperada y caótica evacuación de la ciudad. Además, perecieron también miles de cabezas de ganado y animales domésticos y todo el entorno del lugar del accidente quedó seriamente contaminado por sustancias tóxicas y metales pesados que tardan muchos años en desaparecer [2].

EXPLOSIÓN EN PLANTA NUCLEAR, CHERNOBYL (ABRIL 1986)

Es considerado uno de los mayores desastres medioambientales de la historia. Durante una prueba en la que se simulaba un corte de suministro eléctrico, un aumento súbito de potencia en el reactor 4 de esta central nuclear produjo el sobrecalentamiento del núcleo de dicho reactor, lo que terminó provocando la explosión del hidrógeno acumulado en su interior. La cantidad de dióxido de uranio, carburo de boro, óxido de europio, erbio, aleaciones de circonio y grafito expulsados, materiales radiactivos y/o tóxicos que se estimó fue unas 500 veces mayor que el liberado por la bomba atómica arrojada en Hiroshima en 1945, causó directamente la muerte de 31 personas y contaminó a otras 75000, forzó al gobierno de la Unión Soviética a la evacuación de 116 000 personas provocando una alarma internacional. Después del accidente, se inició un proceso masivo de descontaminación, contención y mitigación en las zonas circundantes al lugar del

accidente y se aisló un área de 30 km de radio alrededor de la central nuclear conocida como “Zona de Alienación”, que sigue aún vigente [14].

INCENDIO REFINERÍA DE CHEVRON, CALIFORNIA (AGOSTO 2012)

Se produjo un incendio en la Unidad de Crudo de una de las refinerías. El evento se debió a que el operador de la planta detectó una fuga en una línea de salida de la torre de destilación de crudo, mientras localizaban e intentaban eliminar la fuga la unidad siguió en marcha. De repente, la fuga aumentó provocando la salida de gran cantidad de gasoil a una temperatura de 320ºC lo que provocó una nube de gases y la posterior explosión e incendio [8].

EXPLOSIÓN EN REFINERÍA FRANCISCO MADERO, TAMAULIPAS, MÉXICO (AGOSTO Y SEPTIEMBRE 2012)

Se registró una explosión en donde se produce gas licuado, gasolina magna y premium, además de diésel y turbosina. “El flagelo involucró dos tanques de almacenamiento de gas debido al sobrecalentamiento de una caldera de la planta hidrodesulfuradora en la refinería”. ("Incendio en refinería de ciudad Madero, no hay lesionados" [7]). Un segundo incidente ocurrió en un lapso de poco más de 15 días. Se produjo un incendio en la línea de desfogue de la refinería, este evento dejó a cuatro trabajadores de Petróleos Mexicanos (Pemex) lesionados (“Cuatro heridos durante incendio en refinería Madero” [16]).

INCENDIO EN PLANTA PETROLERA, TAMAULIPAS, MÉXICO (SEPTIEMBRE 2012)

Se produjo un incendio en un centro receptor de gas y condensados de Pemex Exploración y Producción (PEP). Las instalaciones afectadas no estaban operando, Pemex dijo que el incendio había dañado un ducto y algunas válvulas de control. Este acontecimiento dejó un saldo de 26 personas fallecidas y 46 lesionados [7].

EXPLOSIÓN EN REFINERÍA AMUAY, VENEZUELA (AGOSTO 2012)

Se produjo una explosión en la refinería Amuay debido a una fuga de gas proveniente de la bomba que abastecía a un tanque de almacenamiento que no fue reparada a tiempo.

En un intento de mantener la producción, los técnicos de planta decidieron apoyarse en el viento que soplaba en el área para disipar los gases provenientes de la fuga, pero debido a lluvias presentes en días anteriores la velocidad del viento disminuyó. Esto permitió que se forme una nube de gas que el día previo al evento se propagó por las instalaciones de la refinería. Además los gases alcanzaban niveles superiores a los tolerables (concentraciones superiores al 2% en peso con respecto al aire).

Cerca de la media noche de ese día, la velocidad del viento disminuyó aún más permitiendo que la concentración de gases se incremente, alcanzando casas, edificios cercanos y una planta aledaña en la que se procesaban lubricantes. La explosión abarcó un área muy extensa lo que produjo daños a propiedades y la pérdida de vidas.

Figura 1.1.1: *Concentración de gases debido a disminución de velocidad del viento.*

Figura 1.1.2: *Propagación de nube de gas en la refinería e instalaciones aledañas.*

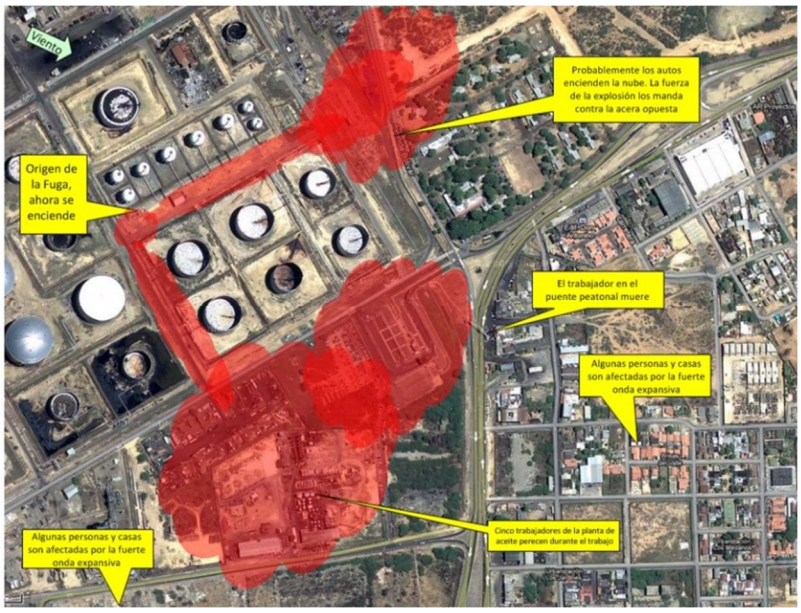


Figura 1.1.3: *Nube de gas con una concentración superior a la tolerable.*

CONATO DE INCENDIO EN LAFABRIL, ECUADOR (NOVIEMBRE 2012)

Se produjo un conato de incendio en la empresa ubicada en la vía Manta-Montecristi debido a una supuesta explosión que se produjo en un tanque de metanol en el interior de la misma. El vocero de comunicación de la empresa citó "Solamente fue un conato de incendio debido a la salida de vapor de un caldero. Al ser una empresa que maneja seguridad industrial hemos evacuado al personal sin problemas" [24]. El momento de la emergencia, el personal contaba con procedimientos de evacuación y acciones de mitigación fueron puestas en marcha. No se reportaron víctimas graves.

EXPLOSIÓN EN PLANTA DE FERTILIZANTES, TEXAS, EE.UU (ABRIL 2013)

Una gran explosión tuvo lugar en la Empresa *West Fertilizer* ubicada en el pequeño pueblo de West, Texas. La explosión provocó daños en 150 edificios, incluyendo tres de las cuatro escuelas del poblado, murieron 14 personas y más de 160 resultaron heridas. Fue tan potente que provocó un temblor de magnitud 2,1 en la escala de Richter.

Las primeras hipótesis apuntan a que se produjo un incendio en uno de los edificios de la planta que entró en contacto con un tanque contenedor de amoníaco y produjo la gran explosión [5].

INCENDIO EN BODEGA DE FIBRO ACERO, CUENCA, ECUADOR (MAYO 2013)

Una nube de humo negro sobre el Parque Industrial alertó sobre el flagelo que ocurría en una bodega de la empresa Fibro Acero. A la emergencia se movilizaron 35 bomberos, cinco vehículos de ataque, cuatro de abastecimiento y tres ambulancias. Al inicio se declaró como un incendio de clave 8 [6], porque se conocía que alrededor de la bodega, existían otras con materiales inflamables, sin embargo, conforme pasó el tiempo la alerta disminuyó. Se informó que al interior de la bodega se encontraba material para el embalaje de acero que consistía en rollos de papel, cartón y plástico, además el fuego se originó por una esquirla de suelda producto de trabajos que se realizaban en la misma.

Hubo un momento en que la seguridad en la electrónica, en particular en el mercado doméstico, significaba poco más que el riesgo de descargas eléctricas y fijar la potencia nominal para evitar el sobrecalentamiento y que se quemaran los componentes. Por ejemplo, no hace mucho el único equipo electrónico de un vehículo era la radio y no era necesario que fuera "funcionalmente segura".

Por otro lado, resultados extraños e inesperados en el sistema de control dinámico de frenado es probable que tengan consecuencias fatales. Situaciones similares pueden vivirse al interior de fábricas e instalaciones industriales, es por ello que surge la necesidad de implementar la seguridad funcional en la industria de procesos.

1.2 Seguridad Funcional.

La seguridad funcional hace referencia a la respuesta de forma adecuada de componentes o subsistemas eléctricos, electrónicos y electrónicos programables implicados en materia de seguridad ante cualquier estímulo externo, incluyendo errores humanos, fallos de hardware o cambios en su entorno para llevar el proceso a un estado seguro. El objetivo último es minimizar el riesgo.

1.3 Funciones Instrumentadas de Seguridad (*Safety Instrumented Function*, SIF).

Según la norma IEC 61511 "Es una función de seguridad con un nivel de integridad de seguridad especificado que es necesario para alcanzar la seguridad funcional y que puede ser una función de protección de seguridad instrumentada (Modo bajo demanda.- Cuando la demanda ocurre una vez al año) o una función de control de seguridad instrumentada (Modo continuo.- Cuando la demanda ocurre dos o más veces al año)". [4].

1.4 Nivel de Integridad de Seguridad (*Safety Integrity Level*, SIL).

Se define como un nivel relativo de reducción del riesgo que provee una función de seguridad, o bien para especificar el nivel objetivo para la reducción de riesgo. También podría definirse simplemente como una medida de la prestación requerida para una SIF. [22, 10].

1.5 Sistemas Instrumentados de Seguridad (*Safety Instrumented System*, SIS).

Un SIS es un sistema cuyo propósito es implementar las funciones de seguridad (SIF) necesarias para llevar a la planta o un proceso a un estado seguro en caso de presentarse un evento de riesgo o cuando se han violado las condiciones de funcionamiento predeterminadas de una variable. Se puede considerar como eventos de riesgo: nivel, concentración, presión y temperatura de líquidos fuera del rango considerado normal.

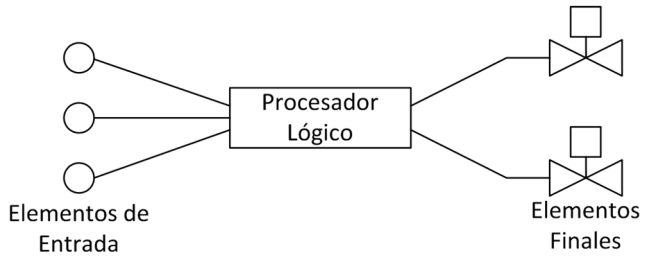


Figura 1.5.1: *Sistema Instrumentado de Seguridad (SIS) [17]*

La Figura 1.5.1 muestra un esquema simplificado de un sistema instrumentado de seguridad. Está compuesto por tres subsistemas fundamentales: elementos de entrada (sensores), solucionador lógico y elementos finales de control (actuadores). Un sistema de control básico de procesos (*Basic Process Control System*, BPCS) consta también de los mismos elementos, pero actúan de diferente manera: El sistema de control regula y controla el proceso mientras que el SIS brinda seguridad al proceso [10, 17, 33, 34].

1.6 Sistemas de Control como Sistemas Relacionados con Seguridad.

Aunque hay definiciones más amplias de este tema, se define un sistema de control como un sistema que responde a las señales procedentes de la planta y/o un operador, haciendo que los equipos de planta funcionen de la manera deseada. La planta o equipo que se está controlando se designa como el equipo bajo control (*Equipment Under Control*, *EUC*). Si el sistema de control desempeña un rol de seguridad, ya sea como una parte integral de

la EUC o como un sistema de protección por separado, será un sistema relacionado con la seguridad.

Ejemplos típicos de los sistemas de control utilizados para seguridad en la planta y equipos son sistemas de "protección" y “bloqueo (*Interlock*)”, pero en ciertos casos se puede necesitar una combinación de ambos con el sistema de control de la máquina o proceso [1].

1.6.1 Sistemas de Bloqueo.

El bloqueo es un medio para impedir el acceso a un lugar que contiene una parte o proceso peligroso, mientras que permite el acceso cuando el peligro no está presente. Dicho sistema puede ser totalmente mecánico o una parte integral del sistema de control, y a menudo es implementado utilizando componentes robustos simples como switches y relés limitadores [1].

1.6.2 Sistemas de Protección.

Un sistema de protección es una forma particular de sistema de control, a menudo incorpora el monitoreo continuo de estado de la planta. Puede ser un simple dispositivo mecánico, tal como una válvula de seguridad o un SIS por separado, por ejemplo, el sistema de parada de emergencia de una gran instalación petroquímica. Son sistemas que operan bajo demanda y su principal objetivo es llevar la planta o el equipo a un estado seguro cuando un parámetro de funcionamiento excede los límites de seguridad. Es importante que estos sistemas sean probados frecuentemente para asegurar su disponibilidad para llevar a cabo su función de seguridad.

Técnicas programables permiten realizar un autodiagnóstico automático, se aplica ampliamente con los sistemas electromecánicos. Sensores, actuadores, controladores y cableado de interconexión, todo se pueden monitorizar continuamente durante la operación de la máquina o proceso. El autodiagnóstico automático se está empleando cada vez más en sistemas que requieren una alta integridad de seguridad [1].

1.7 Evaluación de seguridad y confiabilidad.

Durante las etapas de diseño, construcción y operación de un SIS, la evaluación de seguridad y confiabilidad es importante ya que en base de ella se puede seleccionar el SIS adecuado que cumpla con los requisitos de funcionalidad y confiabilidad dados para una aplicación en particular.

Durante la etapa de operación del SIS la recolección de datos es fundamental para actualizar la evaluación de seguridad y confiabilidad, además de verificar que el SIS continúe cumpliendo los requisitos especificados para los que fue diseñado. Algunas de las actividades de la evaluación de seguridad y confiabilidad son:

1. **Modelado y cálculo de la confiabilidad.-** Para el modelado se puede utilizar diagramas de bloque de confiabilidad (*Reability Block Diagrams*, RBD), modelos de Markov y análisis mediante árboles de falla (*Fault Tree Analysis*, FTA). Los cálculos pueden ser obtenidos de fórmulas exactas o aproximaciones de las mismas.

2. **Revisión del diseño.-** Consiste en revisar la documentación del hardware y del software, así también en evaluar si se cumplen todos los requerimientos establecidos.

3. **Etapa de prueba.-** Se ejecuta una vez que el hardware y el software han sido implementados, iniciando con elementos individuales hasta llegar a los lazos de la SIF. Durante la etapa de operación se puede revelar fallas ocultas en el SIS y verificar si se han realizado cambios en el hardware o software del mismo.

4. **Análisis de fallas.-** Consiste en asegurar que todas las causas de falla y sus efectos son identificados y tratados en el diseño del SIS. En la etapa de operación puede utilizarse para determinar acciones correctivas para prevenir fallas similares a futuro.

Los requerimientos establecidos para el diseño de un SIS están dados en regulaciones y estándares que son provistos por autoridades regulatorias nacionales e internacionales [10].

1.8 Guías Industriales, Estándares y Regulaciones

1.8.1 IEC 61508.

La Comisión Electrotécnica Internacional lanzó este estándar global para sistemas instrumentados de seguridad que abarca múltiples industrias como transporte, médica, nuclear y de procesos.
Su objetivo principal es servir de guía para que otras industrias individuales puedan desarrollar sus propios estándares para que cumplan los requerimientos de esta norma. Otra aplicación de este estándar es la validación de nuevas tecnologías desarrolladas para aplicaciones relacionadas con seguridad, por ello a esta norma también se la conoce como el "estándar de los vendedores".

Este documento consta de siete partes:

1. **Requerimientos generales.-** Describe los pasos que son necesarios para la identificación de peligros y riesgos, para de esta manera definir la reducción de riesgo necesaria para diferentes sistemas y las actividades necesarias para realizar la integración total del sistema.

2. **Requerimientos para sistemas Eléctricos/Electrónicos/Electrónicos Programables (E/E/PE) relacionados con seguridad.-** Provee los requisitos para el diseño del hardware y su integración con el software.

3. **Requerimientos de software.-** Define los requerimientos para la selección, implementación y verificación de las herramientas de software, aplicaciones y lenguajes de programación.

4. **Definiciones y Abreviaciones.-** Es una lista de definiciones y abreviaciones utilizadas en el estándar.

5. **Ejemplos de métodos para la determinación de los niveles integrados de seguridad.-** Hace referencia a métodos para determinar el SIL.

6. **Guías en la aplicación de IEC 61508-2 y IEC 61508-3.-** Se refieren a lineamientos para aplicación de la parte 2.

7. **Revisión de técnicas y medidas.-** Recomendaciones específicas.

Las primeras tres partes son normativas mientras que las otras cuatro partes proveen anexos informativos al estándar
[3, 29].

1.8.2 IEC 61511.

La norma IEC 61511 denominada “Seguridad Funcional: SIS para el Sector de la Industria del Proceso” fue desarrollada para el sector de las industrias de proceso y aplicable, no solo a fabricantes y suministradores, sino también a diseñadores del nivel de seguridad, integradores y usuarios. Fue publicada en el 2003 y en ocasiones es llamada “El estándar de los usuarios”. Esta norma aplica los mismos conceptos de la IEC 61508 con algunos cambios en la práctica, conceptos y términos en la industria de procesos.

Consta de tres partes:

1. Marco, definiciones, sistema, requisitos de hardware y software.
2. Guías para la aplicación de la IEC 61511, parte 1.
3. Guía para la determinación de los niveles de integridad de seguridad requeridos.

Es una norma técnica que establece las prácticas en la ingeniería de sistemas que garantizan la seguridad de un proceso industrial mediante el uso de la instrumentación, estos sistemas se denominan SIS. El sistema de gestión del SIS debe definir cómo un propietario/operador tiene intención de evaluar, diseñar, verificar, instalar, validar, operar, mantener y mejorar continuamente sus SIS. Las funciones esenciales del personal asignado a la gestión del SIS deben estar contempladas y bien definidas en procedimientos, según sea necesario, para apoyar la ejecución coherente de sus responsabilidades.

El sector de la industria de procesos incluye muchos tipos de procesos de fabricación, tales como refinerías, petroquímicas, químicas, energía, farmacéuticas de pasta y papel, por ello la norma IEC 61511 cubre el uso de equipos eléctricos, electrónicos y electrónicos programables, así también es aplicable a los equipos que utilizan sistemas hidráulicos o neumáticos para manipular elementos finales, pero no cubre el diseño e implementación de la lógica neumática o hidráulica [4, 29].

1.9 Capas de protección

En muchos casos, una medida de seguridad individual no puede por sí sola reducir el riesgo a niveles tolerables, proteger una planta y a su personal contra daños o mitigar la propagación de los mismos si ocurre un incidente peligroso. Por esta razón, la seguridad se implementa en forma de capas protectoras: una secuencia de dispositivos mecánicos, controles de proceso, sistemas de parada y medidas de respuesta externas que previenen o mitigan un evento peligroso. Si llegara a fallar una capa de protección, las sucesivas capas estarán disponibles para llevar el proceso a un estado seguro. A medida que aumenta el número de capas de protección y su confiabilidad, también aumenta la seguridad del proceso. En la figura 1.9.1 se muestra la sucesión de capas de seguridad en el orden de su activación:

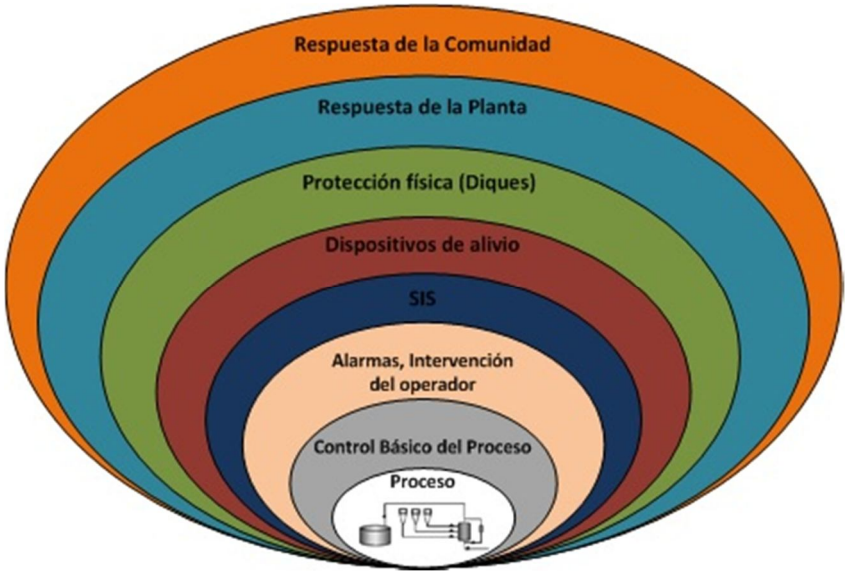


Figura 1.9.1: *Capas de Protección (Modelo de la Cebolla) [10]*

Capas de Prevención:

1. **Proceso.-** El proceso por sí mismo debe ser intrínsecamente seguro, es decir, proporcionar seguridad al operador.

2. **Sistema de Control Básico de Procesos (BPCS).-** El BPCS brinda seguridad a través del diseño apropiado del control de proceso. Este nivel consiste de controles básicos, alarmas y supervisión del operador.

3. **Alarmas, Intervención del Operador.-** Esta capa aporta alarmas críticas que alertan a los operadores acerca de una condición en la cual una medición ha excedido sus límites especificados y podría requerir intervención.

4. **Sistema Instrumentado de Seguridad.-** El SIS opera independientemente del BPCS para brindar seguridad. El SIS realiza acciones de parada cuando las capas previas no pueden resolver una emergencia.

5. **Dispositivos de alivio.-** Esta capa activa, emplea válvulas, dispositivos de alivio de presión o un sistema de antorcha (si hay presencia de combustibles) para impedir una ruptura, derrame u otro escape no controlado.

Capas de Mitigación:

6. **Protección Física.-** Esta capa de protección es pasiva ya que hace referencia a la infraestructura física de la planta que se encarga de contener derrames (combustibles o sustancias químicas) que pudieran darse. Por ejemplo: Diques.

7. **Respuesta de la planta.-** Esta capa al igual que la anterior también es pasiva consiste de barreras de contención contra fuego o explosiones como así también procedimientos para evacuación.

8. **Respuesta de la comunidad.-** El nivel final (externo) de protección es la acción de respuesta de emergencia implementada por la comunidad y se refiere a bomberos y otros servicios de emergencia.

La reducción del riesgo mediante la selección cuidadosa de parámetros operacionales básicos del proceso constituye una pieza clave en el diseño de un proceso seguro. Cada capa de protección adicional consiste de un conjunto de equipos y/o controles administrativos, que interactúan con otras capas de protección, reduciendo de esta manera el riesgo [10].

1.10 Diseño del Ciclo de Vida de Seguridad.

El objetivo principal del ciclo de vida es la reducción de riesgos a niveles tolerables. Se trata de una metodología práctica que delimita los pasos necesarios a seguir para alcanzar la seguridad integral de las plantas de proceso, definiendo la secuencia a seguir y la documentación de cada fase. Para ello la normativa IEC 61511 establece una serie de etapas que ayudan y sirven de guía para conseguir este objetivo.

Representa una descripción simplificada de los pasos que deben seguirse para desarrollar un SIS según la norma actual, pero no necesariamente representa el proceso funcional necesario que una compañía o empresa deba implementar para el diseño de un SIS en particular.

Lo que se busca establecer es que cada empresa tenga un procedimiento formal y organizado para el diseño de sistemas de seguridad que debe cumplir con los requerimientos fundamentales de seguridad de la empresa, con el ciclo de vida, con las normas y regulaciones de seguridad establecidas por el país y procedimientos de ingeniería. La figura 1.10.1muestra el ciclo de vida de un SIS según la norma IEC 61511 [4].

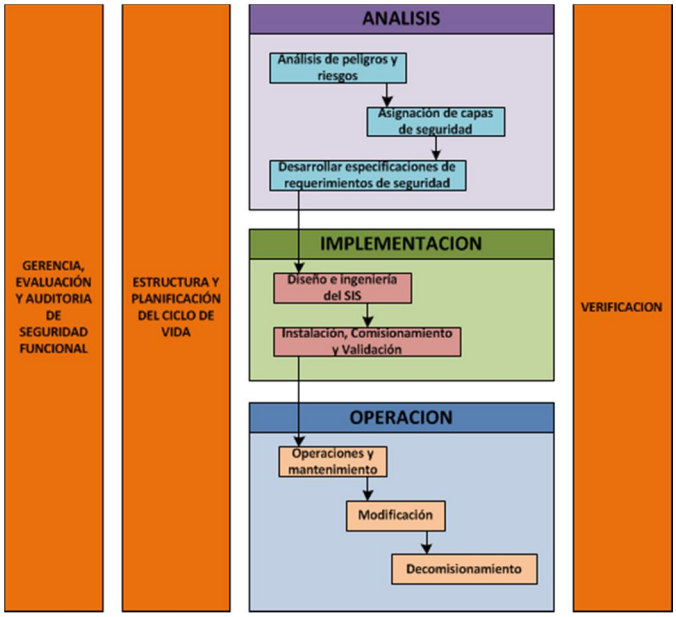


Figura 1.10.1: *Ciclo de Vida según norma IEC 61511 [4]*

En la Figura 1.10.2 se define el "Ciclo de Vida de Seguridad" según la norma IEC 61511, aquí se especifican todos los pasos a seguir desde el inicio y desarrollo conceptual del proyecto hasta el fin de la instalación y su desmantelamiento [4].

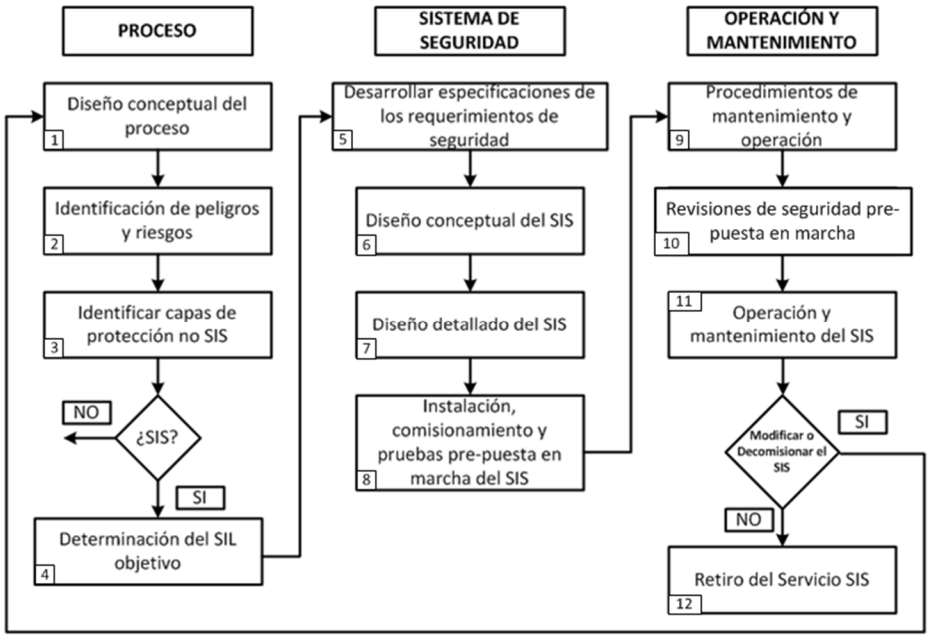


Figura 1.10.2: *Ciclo de Vida Segura [4]*

1. **Diseño conceptual del proceso.-** Esta primera etapa se refiere a la información del proceso, es decir, el conocimiento del proceso entrega una idea preliminar de los peligros y riesgos potenciales del proceso, de los equipos y materiales, que serán estudiados y desarrollados en futuras etapas del ciclo de vida.

2. **Identificación de peligros y riesgos.-** En esta etapa se requiere una detallada información para identificar los peligros y riesgos potenciales de daño asociados al proceso. Una vez identificados los peligros y riesgos, se aplicará la tecnología y medidas adecuadas para eliminar la amenaza, reducir sus consecuencias o la ocurrencia del evento peligroso.

3. **Identificar capas de protección no SIS.-** En esta etapa se consideran las capas de protección necesarias para mitigar los efectos de un evento peligroso, dichas capas deben actuar antes que el SIS.

4. **Determinación del SIL objetivo.-** Esta etapa se establece el SIL para cada SIF. La asignación del nivel SIL de una SIF se basa en el análisis de riesgos, mientras que el nivel de riesgo tolerable es una decisión corporativa basada en una filosofía de gestión de riesgos y de su tolerancia.

5. **Desarrollar especificaciones de requerimientos de seguridad (*Safety Requirements Specification*, SRS).-** En esta etapa se desarrollan las SRS, documento en donde se recogen todos los resultados de la fase de análisis del ciclo del vida. No hay reglas generales que puedan aplicarse en forma global ya que los requerimientos de seguridad dependerán del proceso analizado.

6. **Diseño conceptual del SIS.-** En esta etapa, se desarrolla un diseño inicial para verificar si se cumple con los SRS y SIL de operación. Se debe inicialmente seleccionar una tecnología, arquitectura e intervalo de prueba. Posteriormente se debe proceder a la verificación cuantitativa para ver si el sistema propuesto cumple los requerimientos de operación.

7. **Diseño detallado del SIS.-** El objetivo de esta etapa es finalizar y documentar el diseño conceptual. Se elaboran planos eléctricos, protocolo de pruebas, diseño de programación, es decir, toda la documentación entregada al constructor.

8. **Instalación, comisionamiento y pruebas pre-puesta en marcha del SIS.-** En esta etapa se debe asegurar que el sistema sea instalado de acuerdo al diseño conceptual elegido siguiendo procedimientos estrictos para evitar errores en su implementación y que opere de acuerdo a la SRS. Antes de que el sistema sea llevado a su emplazamiento debe ser probado hasta su correcta operación (pruebas *Factory Acceptance Test*, FAT). Una vez instalado se debe verificar que el sistema esté de acuerdo al diseño detallado incluyendo los dispositivos de campo (pruebas *Site Acceptance Test*, SAT).

9. **Procedimientos de mantenimiento y operación.-** Son importantes para mantener la integridad del SIS. Deben incluir detalles de cómo operar y mantener el SIS, procedimientos alternativos de operación del SIS en una condición de disminución de seguridad, procedimientos operativos en condiciones normales y

de emergencia, mantenimiento preventivo, repuestos y procedimientos para la administración de cambios.

10. **Revisiones de seguridad pre-puesta en marcha.-** En esta etapa se realiza un estudio funcional y una inspección completa del SIS con el fin de demostrar que cumple con los requerimientos de la especificación de diseño y asegurar así su integridad, permitiendo validar el SIS.

11. **Operación y mantenimiento del SIS.-** Esta es la etapa más larga del ciclo de vida del SIS, es el período durante el cual la planta es operativa. Es importante una política de operación y mantenimiento adecuada que garantice que el SIL de cada SIF no se degrade y se mantenga dentro de los límites especificados, además que la seguridad funcional del SIS se mantiene dentro de las SRS.

12. **Retiro del servicio del SIS.-** La etapa final del ciclo de vida se refiere a las precauciones que deben ser tomadas cuando el SIS es decomisionado y desmantelado.

El primer paso descrito en el estándar es comprender los peligros y riesgos asociados al proceso, éste análisis se debe llevar a cabo en los procesos de instalaciones tanto nuevas como existentes en donde se realicen modificaciones en su proceso o en aquellas que no cuentan con dicho análisis. Para poder realizar esta tarea, se requiere detallada información para poder identificar los peligros y causas potenciales de daño asociados al proceso. Se debe considerar el riesgo sobre el personal, producción, equipos, medio ambiente y poblaciones circundantes.

Existen diferentes métodos para la identificación de peligros, tales como HAZOP, "¿Qué pasa si?", Árbol de Fallas y Lista de Verificación (*Checklist*). El método HAZOP se presenta como una de las técnicas más rigurosas y estructurada para la identificación de los peligros asociados a una planta de proceso. La norma IEC 61511-3 recoge diferentes métodos de análisis de riesgos útiles para encontrar el valor objetivo SIL [22, 10].

1.11 Ejemplos de Fallas Ocurridas en Diferentes Fases del Ciclo de Vida.

La falla de un sistema de control puede ser atribuida a errores u omisiones cometidos en una de las fases del ciclo de vida (1.10.1). Un esquema de clasificación simple ha sido desarrollado para el análisis de las causas de los incidentes que se incluyen en esta sección a partir del ciclo de vida de seguridad.
La mayoría de los incidentes ocurren a causa de errores en más de una fase, y con frecuencia es difícil juzgar qué error es el más significativo. Algunos ejemplos se incluyen a continuación [1].

1.11.1 Falla en la especificación de los requisitos de seguridad.

Error en la especificación provoca descarga a la atmósfera.- En una planta con un reactor controlado por una computadora, la especificación para el programa informático para el manejo de las alarmas de la planta tenía un error fundamental. La computadora fue programada de manera que si una falla se produjo en la planta, todas las variables controladas, por ejemplo, tasa de flujo de agua de refrigeración, mantengan su estado actual y una alarma se apagaría. La computadora también había sido programada para aumentar el flujo de agua de refrigeración para el condensador de reflujo inmediatamente después de que un catalizador había sido añadido al reactor. Cuando una falla surgió después de que se había añadido el catalizador, la computadora falló al aumentar el flujo de agua de refrigeración, el reactor se sobre calentó, la presión aumentó y causó que el contenido sea descargada a la atmósfera cuando la válvula de alivio se abrió.

Este incidente se produjo a pesar de que un análisis de riesgos se había realizado. Este análisis no fue lo suficientemente completo, o las personas que llevaron a cabo dicho análisis hicieron suposiciones erróneas acerca de cómo el programador interpretaría los requisitos del diseño en la fase de detalle de diseño. Cualquiera que sea la razón, los interesados tanto en el diseño del sistema de control como en la programación de la computadora, se presentaron con una especificación inadecuada de las funciones de seguridad de la planta. El propósito principal de una especificación es proporcionar una forma muy clara de comunicar las necesidades del usuario. El efecto de esta combinación particular de eventos probablemente habría sido revelado si la especificación había sido analizada con respecto a los modos de falla del sistema de control [1].

1.11.2 Falla en la especificación de integridad de seguridad.

Falla en la computadora resulta en un riesgo potencial para los operadores.- Una de un grupo de computadoras que controlan una planta química fracasó, produciendo un inapropiado ajuste de un número de válvulas de proceso. El personal operativo fue potencialmente puesto en riesgo, oportunamente el polímero fundido fue descargado de los autoclaves presurizados sobre el suelo antes de la operación normal. La investigación reveló que un circuito integrado falló en el microprocesador que controla el funcionamiento de una interfaz de entrada/salida.
La falla fue tal que el procesador establece en uno (todas las válvulas abiertas) todas las señales de los dispositivos de salida. La fuente principal de alimentación sufrió altos niveles de interferencia transitoria que el regulador de voltaje no pudo manejar. El regulador de voltaje eventualmente falló, causando la falla en el circuito integrado.

La falla del microprocesador se había previsto en el diseño original del sistema de la computadora, pero el mecanismo de detección de fallas tenía errores de diseño. La detección de fallas fue realizada por un circuito de "perro guardián (*watchdog*)" configurado para activarse cuando un bit de estado cambie a cero, lo que indica una falla del procesador. Sin embargo, cuando el circuito integrado falló, configuró todos los bits, incluyendo el bit de estado en uno, lo opuesto al estado necesario para disparar el perro guardián. Por ello la falla no fue reconocida. La investigación posterior reveló que había más de 90 defectos en el software, aunque ninguno tuvo lugar en este incidente en particular.

La causa raíz de este incidente fue que el control de la computadora había sido implementado a una planta existente, anteriormente controlada por la tecnología tradicional. Ningún análisis de peligros y riesgos se había realizado antes de este cambio, y no se había desarrollado una especificación de requerimientos de integridad de seguridad. La compañía llevó a cabo una investigación detallada sobre este incidente con un HAZOP, que incluyó el examen en detalle los modos de falla del equipo, y sus efectos sobre el sistema de control como un conjunto.

Un importante hallazgo de este HAZOP fue que la computadora o sistema programable debieron estudiarse al mismo tiempo con el diseño del proceso, no en forma aislada o retrospectivamente. Además, los costos de este estudio y los de aplicación de sus resultados fueron estimados en ser diez veces superiores a las que se habría incurrido si el trabajo se hubiera hecho en el proyecto original.

La planta fue re-comisionada bajo control de la computadora solamente después de que se ha mejorado la calidad de las fuentes de alimentación, los defectos detectados en el

software fueron corregidos, y el sistema de detección de fallos fue mejorado. El circuito de vigilancia fue configurado para reconocer una secuencia de bits generados específicamente en cada ciclo para comprobar el funcionamiento del procesador de interfaz [1].

1.11.3 Falla en el diseño e implementación.

Falla en el diseño del sistema de ventilación de un puente grúa.- Un puente grúa con una capacidad de 450 toneladas estaba siendo controlado desde el control colgante suspendido del carro principal. Los operadores se fueron al descanso, dejando la grúa estacionaria, pero energizada. A su regreso, los operadores encontraron que la grúa se había movido sin que alguien la opere. Afortunadamente, el puente grúa fue detenido por el interruptor final. Si se hubiera movido en la dirección opuesta, habrían tenido serias consecuencias. La grúa utilizó motores de corriente continua controlados por tiristores en un sistema de control de velocidad en lazo cerrado, además utilizaba amplificadores electrónicos y magnéticos. El sistema de control y los amplificadores de tiristores eran sensibles a la temperatura y requerían enfriarse por ventiladores que eran alimentados a través del contactor principal.

Cuando se detuvo el puente grúa, el contactor principal quedó energizado debido a la necesidad de mantener los ventiladores funcionando. Una falla en los componentes electrónicos que forman parte del sistema de control de velocidad generó una señal de velocidad y, como resultado, el puente grúa se movió.

Este incidente muestra la necesidad de considerar los requerimientos de seguridad para todos los modos de operación, incluyendo los modos de espera, durante el proceso de diseño. Hubo una serie de características insatisfactorias del diseño de este sistema de control:

1. Se trataba de un solo canal, por lo que la falla de un solo componente podría afectar a la seguridad, por ejemplo, pérdida de la señal de realimentación, y

2. El sistema de control no se pudo aislar desde el lado de alimentación debido a la necesidad de refrigeración.

La solución involucró cambios en los acuerdos de distribución de energía para que el sistema de control y los ventiladores puedan ser alimentados por circuitos separados. Entonces fue posible dejar al puente grúa sin vigilancia de manera segura con los ventiladores encendidos, pero con el sistema de control desenergizado [1].

1.11.4 Falla en la instalación y comisionamiento.

Liberación de gas en una planta química.- En una fábrica de productos químicos controlada por computadora, una válvula de gas del reactor se abrió involuntariamente, causando que la línea de ventilación de gas residual se rompa y libere gases nocivos a la atmósfera. Las investigaciones establecieron que no hubo ninguna operación programada o manual de la válvula, la cual fue posteriormente encontrada funcionando de manera correcta. La investigación, sin embargo se concentró en el sistema de control y finalmente en la interfaz de salida de la computadora. La interfaz de salida contenía tres tipos de tarjetas de comunicación a través de direcciones comunes y autopistas de datos para el sistema de control principal.

Una amplia investigación del incidente determinó que una falla en la tarjeta del controlador causó la apertura de la válvula de gas. El error fue identificado como la omisión de una conexión a tierra para el bit número 15 en el terminal de datos, el cual en este caso fue utilizando como una línea adicional de dirección. Esto significaba que la dirección de la tarjeta no era única, por ello estaba respondiendo a los comandos y los datos del sistema de control que estaban destinados a una tarjeta diferente. Se descubrió que esta falla afectó a dos de estas válvulas de gas y que había estado presente durante los seis años desde que el sistema de control fue instalado. Su presencia fue revelada solamente por la combinación particular de estados de la planta antes del incidente.

La válvula de gas del reactor fue requerida para “congelar” si la salida de la tarjeta del controlador falló, la válvula fue controlada desde una tarjeta de salida que provee un tren de pulsos. Estas tarjetas permiten seleccionar entre una secuencia de pulsos positivos o negativos, proporcionando dos conexiones de entrada para el bit 15 en la terminal de datos, la entrada no utilizada requiere ser conectada a tierra. Esta fue la omisión de esta conexión que provocó que la tarjeta de salida de pulsos respondiera a los mensajes orientados a la tarjeta de salida de estado encendido / apagado.

Otros factores incluyen la inadecuada inspección previa a la entrega, la cual no detectó la conexión faltante y la cuestionable decisión de diseño que confió en el estado de un solo bit en la secuencia de direccionamiento del sistema relacionado con la seguridad. Este incidente demuestra la importancia de la instalación detallada y los procedimientos de comisionamiento, de manera que no se comprometa la integridad de seguridad incorporada en el sistema. Los procedimientos de instalación y comisionamiento necesitan ser especificados de la forma más explícita posible, con los documentos de apoyo que están firmados por el técnico de instalación después de las inspecciones exhaustivas y pruebas funcionales [1].

1.11.5 Falla en la operación y mantenimiento.

Hombre muere aplastado por elevador de carga en fábrica de alimentos.- En una fábrica de alimentos se utilizó un sistema de cintas transportadoras para mover las bandejas de comida preparada desde y hasta una sala de refrigeración. Esta habitación fue equipada con elevadores de entrada y salida, y el sistema completo fue controlado por computadora. Se ha reportado que un elevador estaba defectuoso, fue durante la investigación y reparación de este elemento que un hombre murió aplastado mientras intentaba re-conectar un sensor de proximidad al sistema de control.

La información se introducía en la computadora utilizando un código para el producto y un código adicional para su destino dentro de la planta. La computadora también utilizaba las salidas de los sensores de proximidad y dispositivos detectores de posición, para determinar en dónde estaban las bandejas de comida dentro del sistema.

Se había proporcionado un dispositivo de aislamiento de energía para el motor de izaje de la unidad, pero no se utilizó y el hombre estaba tratando de volver a conectar los cables sueltos de un detector de proximidad mientras la computadora estuvo en modo operativo. Dos de los tres cables necesarios habían sido re-conectados con éxito, pero re-conectar el cable final tenía el efecto de enviar una señal a la computadora, la cual inicia un movimiento descendente del elevador, aplastando al hombre mientras realizaba la conexión.

Las partes peligrosas de la maquinaria deben estar siempre encerradas para evitar el acceso del personal. Cuando es necesario el acceso, como en las operaciones de mantenimiento, un sistema de bloqueo debe utilizarse para desconectar la alimentación de los actuadores antes de que el personal de mantenimiento pueda acceder a los equipos. Un sistema seguro de trabajo, por ejemplo, un procedimiento de “permiso de trabajo”, también habría sido apropiado en estas circunstancias, asegurar que la alimentación fue apagada. Cuando se requiere el acceso a un sistema de control energizado, como en la configuración de la máquina o en la búsqueda de errores, entonces aún debe mantenerse la seguridad.

Una solución es diseñar el sistema de bloqueo que protege al operador de tal manera que cuando se coloca en su modo de “configuración”, que active automáticamente un modo restringido de operación que no pueda ser anulado. Algunos ejemplos son los modos de “marcha lenta” y de diagnóstico controlados por una computadora en la cual se ejecutan programas especiales para diagnosticar fallas. En este caso, debido a la posibilidad de lesiones graves, el equipo debió haber sido desconectado de la alimentación.

El aislamiento y bloqueo de equipos por medios mecánicos son los mejores métodos para garantizar la seguridad durante las operaciones de mantenimiento [1].

1.11.6 Falla en debido a cambios realizados después del comisionamiento.

Lista de equipos de perforación del Mar del Norte.- Los nuevos propietarios de una plataforma de perforación semi-sumergible querían que se lleven a cabo grandes modificaciones. Una vez terminadas las modificaciones, la plataforma realizó diversas tareas de perforación en el Mar del Norte. Después fue colocada en un área de almacenamiento durante seis meses debido a la falta de trabajo. Cuando el buque se puso en servicio durante el próximo contrato de perforación, se detectó un inclinación debido a pérdida de energía.

Después de que se restableció el suministro eléctrico se encontró que algunas de las válvulas de control del sistema de lastre no estaban totalmente cerradas y esa fuga estaba causando una inclinación en la plataforma. La tripulación estaba aguardando junto a botes salvavidas y la inclinación de la plataforma era de 16 grados al momento en que se encontró la falla.

En operaciones normales, el equipo de perforación se mantuvo a nivel mediante el bombeo de agua entre varios tanques de lastre y las válvulas entre los tanques de lastre fueron controladas eléctricamente y operadas hidráulicamente. Durante modificaciones a la plataforma, las válvulas de control de lastre fueron hechas totalmente hidráulicas. Además, dos válvulas de cierre de seguridad operadas eléctricamente, se instalaron en la línea principal de suministro hidráulico en cada una de las dos consolas de mando para proteger el sistema de lastre. En el caso de que la alimentación eléctrica falle, se esperaba que estas válvulas liberaran la presión hidráulica en todas las líneas de operación de las válvulas de lastre, haciendo que las válvulas de lastre de cierren por lo que el exceso sería “congelado”.

Una investigación encontró que un filtro fundamental en el sistema hidráulico no se había arreglado y esto permitió que los desechos en tubería se alojaran en las válvulas de apagado de seguridad. Las juntas de estas válvulas se dañaron cuando las válvulas operaron durante el corte de energía, esto permitió que el fluido hidráulico ingres a las líneas de retorno cuando se restablezca el suministro eléctrico. Esto a su vez provocó una contrapresión en los actuadores de las válvulas de control de lastre que se abrieron parcialmente y causaron la inclinación de la plataforma.

La causa primaria del incidente fue la omisión del filtro. Sin embargo, la investigación también mostró que los procedimientos de lavado de residuos en la tubería del sistema hidráulico eran inadecuados después de la modificación. Además, el diseño del sistema de control modificado no había sido validado correctamente y era intrínsecamente inseguro.

Aunque el sistema hidráulico había sido purgado, la forma y la secuencia de lavado no fueron especificadas, por lo que se cree que los desechos y materiales extraños se quedaron en el sistema. Cuando un sistema complejo está siendo re-comisionado, es particularmente importante que una especificación del trabajo esté definida e implementada.
Aparentemente tareas simples como el ajuste de un filtro y el lavado de un sistema de tuberías pueden ser ineficaces por falta de atención a los detalles y la ausencia de procedimientos del proyecto.

La necesidad de un filtro fue reconocida, lo que debería haberse esperado es que los desechos inevitablemente se acumularían en el sistema hidráulico y la capacidad de la línea de retorno debió haberse diseñado considerando esta falla. Estas deficiencias serían rebeladas si una validación formal de la seguridad se hubiera llevado a cabo sobre las modificaciones propuestas. Los controles sobre el diseño eran en realidad muy pobres y ni siquiera incluyen los cálculos del flujo o presión.

Cuando se contempla una modificación de un sistema de control relacionado con la seguridad, la especificación de requisitos de seguridad debe ser revisada para confirmar que la modificación propuesta no reducirá la integridad de seguridad original del diseño [1].

1.12 Definiciones Generales en Análisis de Riesgos.

El objetivo de un análisis de riesgos es la identificación de los peligros del proceso, estimar su riesgo y decidir si el riesgo es tolerable. Para reducir su riesgo a un nivel tolerable, el primer recurso son las capas de protección, en caso de no alcanzar un nivel de riesgo deseado después de aplicar dichas capas, se requerirá implementar un SIS.

En caso de precisar un SIS, los resultados del análisis de riesgos deben estar constituidos por los datos de entrada para la determinación del SIL buscado de las SIF identificadas. Este análisis por lo tanto incluye la identificación de las SIF que son necesarias para detectar un inminente daño y llevar al proceso a un estado seguro.

Algunos términos relacionados al análisis de riesgos se definen a continuación:

- **Peligro**
  Según la norma IEC 61511 se define como: “Fuente potencial de daño”. El término incluye daños a las personas que surgen a corto plazo, por ejemplo, incendio y explosión, así también los que tienen un efecto a largo plazo, por ejemplo, la liberación de una sustancia tóxica [4].

- **Evento**
  La norma IEC 61511 lo define como: “una acción que puede causar lesiones físicas o daños a la salud de las personas directa o indirectamente, como resultado de los daños a la propiedad o al medio ambiente” [4].

- **Incidente**
  Se considera a cualquier evento que no forma parte del desarrollo habitual de un proceso y que causa, o puede causar una interrupción del mismo. Puede considerarse una falla segura (ver sección 1.13.3).

- **Accidente**
  Es un acontecimiento que sucede sin intención alguna produciendo daños al personal, infraestructura y maquinaria.

- **Consecuencia**
  Se refiere a la situación resultante al desatarse un evento.

- **Severidad**
  Hace referencia al nivel de gravedad que puede tener un evento (Figura 1.12.1).

Categoría	Valor	Descripción
Catastróficas	5	Pérdida patrimonial, paro total de producción. Múltiples muertes como consecuencia.
Mayores	4	Daños significativos al patrimonio. Una muerte como consecuencia.
Moderadas	3	Podría causar pérdidas importantes en el patrimonio, tomaría mucho tiempo corregirlo (Daños superiores a $100000)
Menores	2	Causa daño en el patrimonio, se puede corregir en corto tiempo (Daños entre $2500 y $100000).
Insignificantes	1	Pequeño o nulo efecto en la institución.

Figura 1.12.1: *Categorización de la Severidad [10]*

- **Frecuencia**
  Hace referencia a la cantidad de veces que se repite un evento dentro de un intervalo de tiempo (Figura 1.12.2).

Categoría	Valor	Descripción
Casi certeza Continuamente	5	Riesgo de ocurrencia **muy alta** (tiende al 100%)
Probable Frecuente	4	Riesgo de ocurrencia **alto** (75% a 95%)
Moderado Ocasional	3	Riesgo de ocurrencia **medio** (51% a 74%)
Improbable Poco ocasional	2	Riesgo de ocurrencia **bajo** (26% a 50%)
Muy improbable Casi nunca	1	Riesgo de ocurrencia **muy baja** (1% a 25%)

Figura 1.12.2: *Determinación de Probabilidad o Frecuencia [10]*

- **Riesgo**
  Según la norma IEC 61511 “es la combinación de la frecuencia de ocurrencia de un evento y la severidad de dicho evento” [4].

Usualmente el riesgo se define como una medida que resulta de la combinación de la probabilidad de que se produzca un evento peligroso y la severidad de dicho evento; en otras palabras cuan a menudo puede suceder y que tan malo puede ser. Puede ser evaluado cuantitativamente o cualitativamente

$$Riesgo = Frecuencia * Severidad \quad (1.12.1)$$

Aunque en las normas de seguridad como la IEC 61511, el riesgo se centra en riesgo personal y riesgo para el medio ambiente; la mayoría de compañías extienden las categorías y factores de riesgo e incluyen seguridad y salud públicas, costos de responsabilidad civil, daños a equipos y pérdida de imagen de la empresa [28].

1.12.1 Técnicas de Análisis e Identificación de Riesgos

Algunas de las técnicas más utilizadas se definen a continuación [21]:

1. **Revisión o Auditorías de Seguridad.-** Se enfocan en la implementación adecuada de programas y normas de Seguridad.

2. **Investigación de Accidentes/Incidentes.-** Su propósito es descubrir las causas básicas de los accidentes y establecer medidas correctivas para evitar su repetición.

3. **Lista de verificación (*Checklist*).-** Aplica listas de verificación previamente desarrolladas. Registra acciones y sus consecuencias.

4. **¿Qué pasa si?.-** Utiliza un equipo de personas con experiencia para poner a prueba los peligros mediante preguntas: ¿Qué pasa si?.

5. **Estudio de Peligros y Operabilidad (*Hazards and Operability*, HazOp).-** Identifica sistemáticamente peligros o problemas de operabilidad a través del diseño de una instalación.

6. **Análisis de Modo y Efecto de Falla (*Failure Mode and Effects Analysis*, FMEA).-** Consiste en revisar tantos componentes, ensamblajes y subsistemas como sea posible para identificar modos de falla, sus causas y efectos.

7. **Análisis de Árbol de Fallas (*Fault Tree Analysis*, FTA).-** Analiza, no identifica riesgos. Es útil en la identificación de causas de accidentes

La presente investigación se enfocará en el método de HazOp.

1.12.2 HazOp

Es una técnica de identificación de riesgos basada en la premisa de que los riesgos, los accidentes o los problemas de operabilidad, se producen como consecuencia de una desviación de las variables de proceso con respecto a los parámetros normales de operación en un sistema dado y en una etapa determinada. Por lo tanto, consiste en evaluar, las consecuencias de posibles desviaciones en todas las unidades de proceso. La técnica consiste en analizar sistemáticamente las causas y las consecuencias de unas desviaciones de las variables de proceso, planteadas a través de "palabras guía" [21].

Los principales objetivos de un HAZOP son:

1. Identificar y evaluar los peligros dentro de un proceso planificado u operación.

2. Identificar los problemas significativos de funcionamiento o calidad.

3. Identificar los problemas prácticos asociados con las operaciones de mantenimiento.

Etapas de un HazOp

1. **Definición del área de estudio.-** Consiste en delimitar las áreas a las cuales se aplica la técnica. En una determinada instalación de proceso, considerada como el área de objeto de estudio, se definirán subsistemas o líneas de proceso que correspondan a entidades funcionales propias, por ejemplo, una línea de descarga a un depósito y reactores.

2. **Definición de los nodos.-** En cada uno de los subsistemas o líneas de proceso se identifican puntos localizados en el proceso llamados nodos, por ejemplo, un depósito de almacenamiento de combustibles. La técnica HAZOP se aplica a cada uno de estos nodos. Cada nodo está caracterizado por variables de proceso como presión, temperatura, caudal, nivel y viscosidad.

El documento de soporte principal de esta técnica es el diagrama de tuberías e instrumentación (*Piping and Instrumentation Diagram*, P&ID).

3. **Aplicación de las palabras guía.-** Las "palabras guía" se utilizan para indicar la ocurrencia de un evento en uno de los nodos definidos anteriormente. Se aplican tanto a acciones (reacciones y transferencias) como a parámetros específicos (presión, caudal, y temperatura). La Tabla 1.1 presenta algunas palabras guía y su significado.

Palabra guía	Significado	Ejemplo de un evento	Ejemplo de causas originadoras
NO	Ausencia de la variable a la cual se aplica	No hay flujo en la línea	Bloqueo, válvula cerrada, atascada o abierta, fuga, falla en el BPCS
MAS	Aumento cuantitativo de una variable	Más flujo (más caudal)	Presión de descarga reducida, lectura errónea de instrumentos
		Más temperatura	Puntos Calientes, explosión, reacción descontrolada
MENOS	Disminución cuantitativa de una variable	Menos caudal	fuga; bloqueo parcial, línea obstruída, bloqueo de válvulas
		Menos temperatura	Pérdidas de calor, falla de sellado
INVERSO	Analiza la inversión en el sentido de la variable.	Flujo inverso	Inversión de bombeo, válvula antirretorno mal colocada o deteriorada
ADEMAS DE	Aumento cualitativo. Se obtiene algo más de lo esperado	Impurezas o una fase extraordinaria	Entrada de contaminantes del exterior, presencia de materiales por fugas interiores, fallos de la puesta en marcha
PARTE DE	Disminución cualitativa. Parte de lo que debería ocurrir sucede según lo previsto	Disminución de la composición en una mezcla	Concentración demasiado baja en la mezcla, reacciones adicionales, cambio en la alimentación
DIFERENTE DE	Actividades distintas respecto a la operación normal	Cualquier actividad	Puesta en marcha y parada, pruebas e inspecciones, mantenimiento, corrosión.

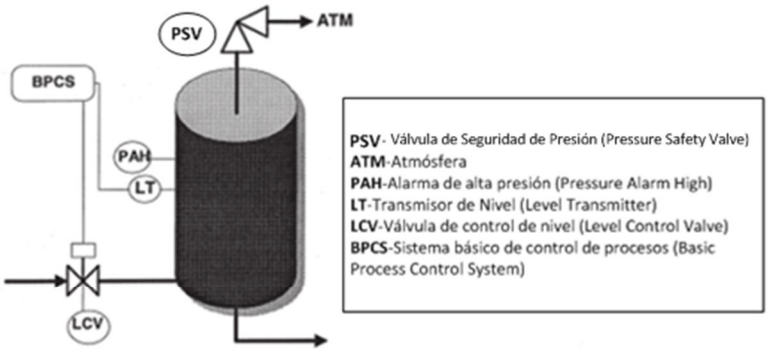
Tabla 1.1: *Palabras Guía [21]*

4. **Definición de los eventos a estudiar.-** Para cada nodo se plantea de forma sistemática todos los eventos que implican el uso de cada palabra guía a una determinada variable o actividad. Para realizar un análisis exhaustivo, se deben aplicar todas las combinaciones posibles entre palabra guía y variable de proceso. También se deben indicar las posibles causas de dichos eventos así como sus consecuencias.

5. **Sesiones HazOp.-** Tienen como objetivo la realización sistemática del proceso descrito anteriormente, analizando los eventos en todos los nodos seleccionados a partir de las palabras guía aplicadas a determinadas variables o procesos. Se determinan las posibles causas, consecuencias, respuestas que se proponen y las acciones a tomar. Dichas sesiones se llevan a cabo por un equipo de trabajo multidisciplinario.

6. **Informe final.-** Consta de los siguientes documentos:

- Esquemas simplificados con la situación y numeración de los nodos de cada subsistema.
- Formatos de recopilación de las sesiones con indicación de las fechas de realización y composición del equipo de trabajo.
- Análisis de los resultados obtenidos. Se puede llevar a cabo una clasificación cualitativa de las consecuencias identificadas.
- Listado de las medidas a tomar.
- Lista de los eventos iniciadores identificados.



Item	Evento	Causas	Consecuencias	Capas de seguridad	Acción
Tanque	Alto Nivel	Falla del BPCS	Alta Presión	Operador	
	Alta Presión	1.Alto Nivel, 2.Fuego Externo	Liberación a la atmósfera	1.Alarma, Operador, PRV 2.Sistema de aspersores	Evaluar condiciones para liberación a la atmósfera
	Flujo bajo/no hay flujo	1.Falla del BPCS	No hay consecuencias de interés		
	Flujo Reverso		No hay consecuencias de interés		

Figura 1.12.3: *Ejemplo de HazOp [21]*

1.13 Determinación del SIL

1.13.1 Definiciones

1. **Probabilidad de Falla a la Demanda (*Probability of Failure on Demand*, PFD).-** Es un valor que indica la probabilidad de que un sistema falle al responder a una demanda.

2. **Disponibilidad de Seguridad.-** Indica la probabilidad de disponibilidad del sistema ante un evento. Este dato se puede obtener de la operación 1-PFD.

3. **Factor de Reducción de Riesgo (*Risk Reduction Factor*, RRF).-** Es un valor que revela la cantidad en la que se puede reducir un riesgo ante un evento. Este dato se puede obtener de la operación 1/PFD.

4. **Fracción de Falla Segura (*Safe Failure Fraction*, SFF).-** Se obtiene del total de fallas de los instrumentos. Se estima a partir de tasa de fallas seguras detectadas y no detectadas, así como de la tasa de fallas peligrosas detectadas ($SFF = (\lambda_{SD} + \lambda_{SU} + \lambda_{DD}/Total)$ (Ver sección 1.13.3).

Tanto la PFD como la disponibilidad de seguridad y el RRF dependen del nivel de SIL deseado como lo muestra la tabla 1.2.

SIL	Probabilidad de falla a la demanda (PFD)	Disponibilidad Segura (1-PFD)	Factor de Reducción de Riesgo (1/PFD)
4	0.0001-0.00001	99.99-99.999%	10.000-100.000
3	0.001-0.0001	99.9-99.99%	1.000-10.000
2	0.01-0.001	99-99.9%	100-1.000
1	0.1-0.01	90-99%	10-100

Cuadro 1.2: *Factores de desempeño del SIS [21]*

1.13.2 Evaluación de riesgos

El riesgo está presente en todas partes, una planta, un proceso químico obviamente conlleva un riesgo que debe ser minimizado y controlado. El objetivo de cualquier compañía u organización es conseguir el riesgo cero, aunque es importante reconocer que

el riesgo cero no existe. Una actividad involucra más riesgo que otra, pero hay una medida de riesgo para toda actividad realizada [22, 10].

1.13.2.1 Niveles tolerables de riesgo

El concepto de niveles tolerables de riesgo no es solamente un asunto técnico, también involucra temas morales y legales. Decidir qué tan seguro es lo suficientemente seguro no puede ser determinado por ecuaciones algebraicas y evaluaciones probabilísticas [10].

1.13.2.2 Riesgo tolerable en la industria de procesos

El propósito de un plan de seguridad, incluido el SIS, es garantizar que el riesgo en todo momento sea tolerable. El riesgo tolerable lo marca el propietario/operador de la planta en cada momento. La norma IEC 61511 describe el riesgo tolerable como: “el riesgo que se acepta en un determinado contexto de acuerdo con los valores actuales de la sociedad”. Como se puede apreciar, es una definición muy abierta.

1.13.3 Modos de Falla

La principal preocupación para un sistema de seguridad no debería ser cómo opera el sistema sino como podría fallar. Esta es la razón principal porque los SIS difieren de los sistemas activos de control.

Las fallas no solo pueden ser categorizadas en seguras y peligrosas sino también como detectadas y no detectadas (Figura 1.13.1). Las fallas seguras son mostradas en la parte superior y las fallas peligrosas en la parte inferior, así también, las fallas detectadas son mostradas en la parte izquierda y las fallas no detectadas en la parte derecha.

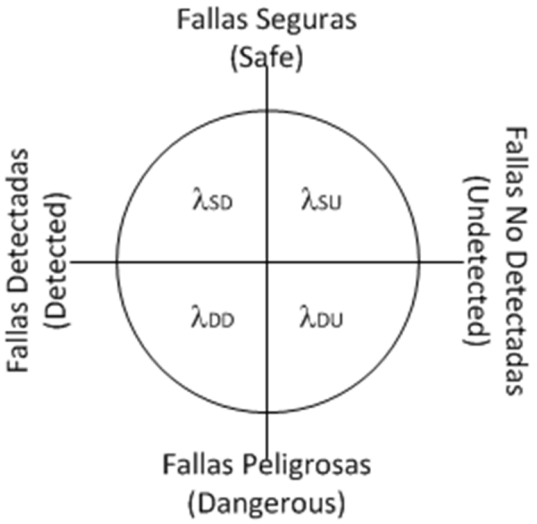


Figura 1.13.1: *Modos de Falla [10]*

1.13.3.1 Fallas Seguras/Peligrosas

Los sistemas pueden sufrir fallas esporádicas que podrían ocasionar el apagado de algún proceso cuando no hay una situación real de emergencia. Este tipo de fallas reciben muchos nombres, por ejemplo, fallas reveladas, fallas descubiertas y fallas de inicio. El término utilizado en los estándares es “falla segura”. Las fallas seguras tienden a ser muy costosas en términos de paros innecesarias en la producción. Cuando un sistema tiene demasiadas fallas seguras provoca que el personal desconfíe de ellos, como resultado se crean bypass para anular dichas fallas. Algunos accidentes fatales han tenido lugar debido al bypass de sensores o partes del SIS mientras el proceso seguía ejecutándose. Otro tipo de fallas son aquellas en las que el sistema no responde ante una demanda real, dichas fallas pueden denominarse fallas ocultas, fallas cubiertas o fallas inhibidoras. Los estándares se refieren a este tipo de fallas como “fallas peligrosas”. Si un sistema falla de esta manera podría ser potencialmente peligroso. La única manera de revelar estas fallas es realizando pruebas en el sistema antes de que entre en operación [10, 35].

1.13.3.2 Fallas Detectadas/No detectadas

Las fallas peligrosas son clasificadas como fallas peligrosas no detectadas (*Dangerous Undetected*, DU) y fallas peligrosas detectadas (*Dangerous Detected*, DD). Las fallas detectadas están relacionadas con diagnósticos automáticos (el sistema detecta por sí solo cuando se da una falla). Las fallas seguras reciben la misma clasificación [10].

1.13.3.3 Falla sin efecto

Se define como la falla de un componente que es parte de la función de seguridad pero que no tiene efecto en la misma. Dichas fallas son clasificadas como fallas seguras no detectadas de acuerdo a la norma IEC 61508. Se debe notar que estas fallas no afectan la confiabilidad o seguridad del sistema y no son incluidas en cálculos de activaciones esporádicas [28].

1.13.4 Modelado y confiabilidad de SIS

1.13.4.1 Medidas usuales en SIS

1. λ = Número de fallas por unidad de tiempo.
2. MTTF = Tiempo Medio para Fallas (*Mean Time To Fail*)
3. $MTTF_{SP}$ = (sp = *Sporious*, falla segura)
4. PFD
5. RRF
6. SFF

1.13.4.2 Fórmulas para el modelado de SIS

Las siguientes fórmulas se muestran en su forma aproximada y completa para sistemas con arquitectura 1oo1, 1oo2, 2oo2 y 2oo3[1].

[1] Tipos de arquitecturas:
1oo2 = 1 out of 2, es decir, de un arreglo de dos sensores, uno presenta falla.
2oo2 = 2 out of 2, es decir, de un arreglo de dos sensores, los dos presentan falla.

Fórmulas Aproximadas

Configuración	$MTTF_{SP}$
1oo1	$\frac{1}{\lambda_S}$
1oo2	$\frac{1}{(2 * \lambda_S)}$
2oo2	$\frac{1}{\left((2 * \lambda_S^2 * MTTR) + (\beta * \lambda_S)\right)}$
2oo3	$\frac{1}{\left((6 * \lambda_S^2 * MTTR) + (\beta * \lambda_S)\right)}$

En donde:

MTTR = Tiempo medio para reparación (*Mean Time To Repair*, MTTR).
λ_S = Tasa de fallas seguras.
β = Factor de falla común[2].

[2] Fracción de fallas que impacta en uno o más canales de los sistemas redundantes.

Fórmulas Completas [31, 13]

Configuración	PFD_{avg}
1oo1	$\left[\lambda_{DD} * \left(MTTR + {}^{TI_A}/_{2}\right)\right] + \left[\lambda_{DU} * {}^{TI_M}/_{2}\right] + \left[\lambda_{DN} * {}^{Life}/_{2}\right] + \left[{}^{TD}/_{TI_M}\right]$
1oo2	$\left[2 * (\lambda_{DD})^2 * \left(MTTR + {}^{TI_A}/_{2}\right)^2\right] + \left[{}^{((\lambda_{DU}) * (TI_M)^2)}/_{3}\right] + \left[{}^{((\lambda_{DN})^2 * Life^2)}/_{3}\right] + \left[2 * TD * \lambda_{DU} * \left({}^{\left({}^{TI_M}/_{2}\right) + MTTR}/_{TI_M}\right)\right] + \left[\lambda_{DU} * \beta * {}^{TI_M}/_{2}\right]$
2oo2	$\left[2 * \lambda_{DD} * \left(MTTR + {}^{TI_A}/_{2}\right)\right] + [\lambda_{DU} * TI_M] + [\lambda_{DN} * Life] + \left[2 * {}^{TD}/_{TI_M}\right] + \left[\lambda_{DU} * \beta * {}^{TI_M}/_{2}\right]$
2oo3	$\left[6 * (\lambda_{DD})^2 * \left(MTTR + {}^{TI_A}/_{2}\right)\right] + [(\lambda_{DU})^2 * (TI_M)^2] + [(\lambda_{DN})^2 * Life^2] + \left[6 * TD * \lambda_{DU} * \left({}^{\left({}^{TI_M}/_{2}\right) + MTTR}/_{TI_M}\right)\right] + \left[\lambda_{DU} * \beta * {}^{TI_M}/_{2}\right]$

En donde:

TI_A = Intervalo de prueba automático (*Automatic Test Interval*)
TI_M =Intervalo de prueba manual (Manual Test Interval)

β = Factor de falla común
TD = Duración de la prueba (*Test Duration*)
DD= Falla peligrosa detectada (*Dangerous Detected*)
DU= Falla peligrosa no detectada (*Dangerous Undetected*)
DN= Falla peligrosa nunca detectada (*Dangerous No Detected*)

Estas fórmulas son válidas mientras $\lambda \ll$ TI o MTTF $\gg$TI.

Las ecuaciones antes mostradas constan de las siguientes partes:

La porción peligrosa detectada (Tabla 1.3): Usualmente insignificante. Excepto en el caso de bloqueo parcial de válvulas (Porque el intervalo automático de prueba es importante en este caso).

Configuración	$\boldsymbol{MMTF_{SP}}$
1oo1	$\left[\lambda_{DD} * \left(MTTR + {TI_A}/{2}\right)\right]$
1oo2	$\left[2 * (\lambda_{DD})^2 * \left(MTTR + {TI_A}/{2}\right)^2\right]$
2oo2	$\left[2 * \lambda_{DD} * \left(MTTR + {TI_A}/{2}\right)\right]$
2oo3	$\left[6 * (\lambda_{DD})^2 * \left(MTTR + {TI_A}/{2}\right)\right]$

Tabla 1.3*: Porción peligrosa detectada.*

La porción peligrosa no detectada (Tabla 1.4).

Configuración	$\boldsymbol{MMTF_{SP}}$
1oo1	$\left[\lambda_{DU} * {TI_M}/{2}\right]$
1oo2	$\left[\left((\lambda_{DU}) * (TI_M)^2\right)/3\right]$
2oo2	$[\lambda_{DU} * TI_M]$
2oo3	$[(\lambda_{DU})^2 * (TI_M)^2]$

Tabla 1.4: *Porción peligrosa no detectada.*

La porción peligrosa nunca detectada (Tabla 1.5): Es incluida cuando se asumen pruebas manuales imperfectas.
Su impacto puede ser significativo, sin embargo, a menudo se ignora.

Configuración	$\boldsymbol{MMTF_{SP}}$
1oo1	$\left[\lambda_{DN} * {Life}/{2}\right]$
1oo2	$\left[((\lambda_{DN})^2 * Life^2)/{3}\right]$
2oo2	$[\lambda_{DN} * Life]$
2oo3	$[(\lambda_{DU})^2 * (TI_M)^2]$

Tabla 1.5: *Porción peligrosa nunca detectada.*

La porción debida a bypass (Tabla 1.6): Puede ser significativo para configuraciones 1oo1 y 2oo2, sin embargo este factor es a menudo ignorado.

Configuración	$\boldsymbol{MMTF_{SP}}$
1oo1	$\left[{TD}/{TI_M}\right]$
1oo2	$\left[2 * TD * \lambda_{DU} * \left(\left(\left({TI_M}/{2}\right) + MTTR\right)\Big/{TI_M}\right)\right]$
2oo2	$\left[2 * {TD}/{TI_M}\right]$
2oo3	$\left[6 * TD * \lambda_{DU} * \left(\left(\left({TI_M}/{2}\right) + MTTR\right)\Big/{TI_M}\right)\right]$

Tabla 1.6: *Porción debida a bypass.*

La porción de causa común (Tabla 1.7): Este factor es dominante para configuraciones 1oo2 y 2oo3. No se aplica para 1oo1.

Configuración	$\boldsymbol{MMTF_{SP}}$
1oo1	0
1oo2	$\left[\lambda_{DU} * \beta * {}^{TI_M}/_{2}\right]$
2oo2	$\left[\lambda_{DU} * \beta * {}^{TI_M}/_{2}\right]$
2oo3	$\left[\lambda_{DU} * \beta * {}^{TI_M}/_{2}\right]$

Tabla 1.7: *Porción de causa común.*

1.13.5 Métodos de determinación del SIL

Una vez determinada la PFD actual y la PFD objetivo, se decide implementar un SIS. Dicho SIS reduce la frecuencia de ocurrencia y con eso el riesgo asociado (Figura 1.13.2) [10].

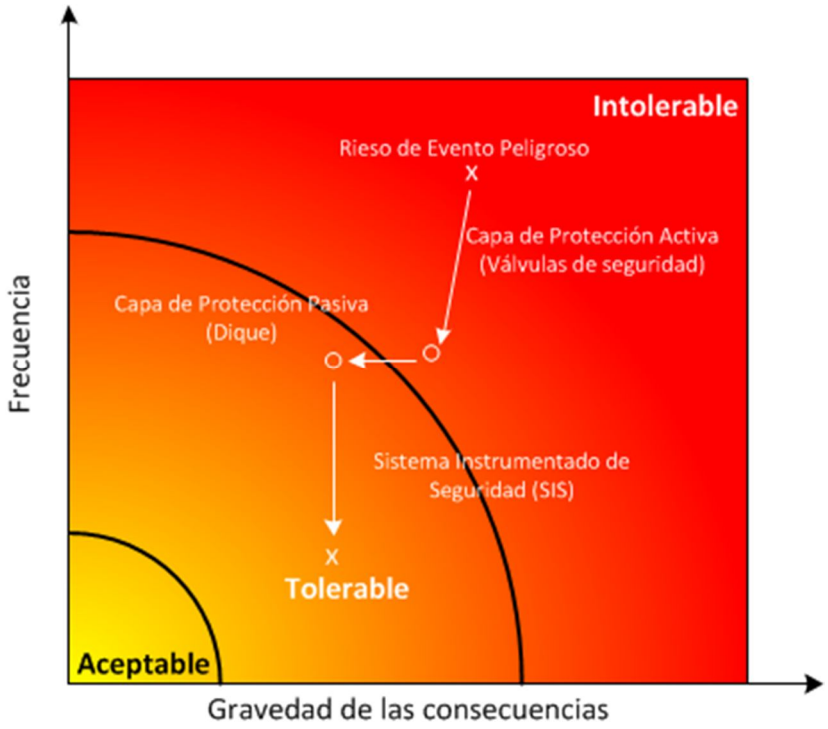


Figura 1.13.2: *Frecuencia vs. Gravedad de consecuencias*

1.13.5.1 ALARP (*As Low As Reasonably Practical*)

El principio ALARP (Tan bajo como sea razonablemente factible) normalmente se sitúa entre estos dos límites y ALARP comprende tres regiones que van asociadas a una clase de riesgo (figura 1.13.3):

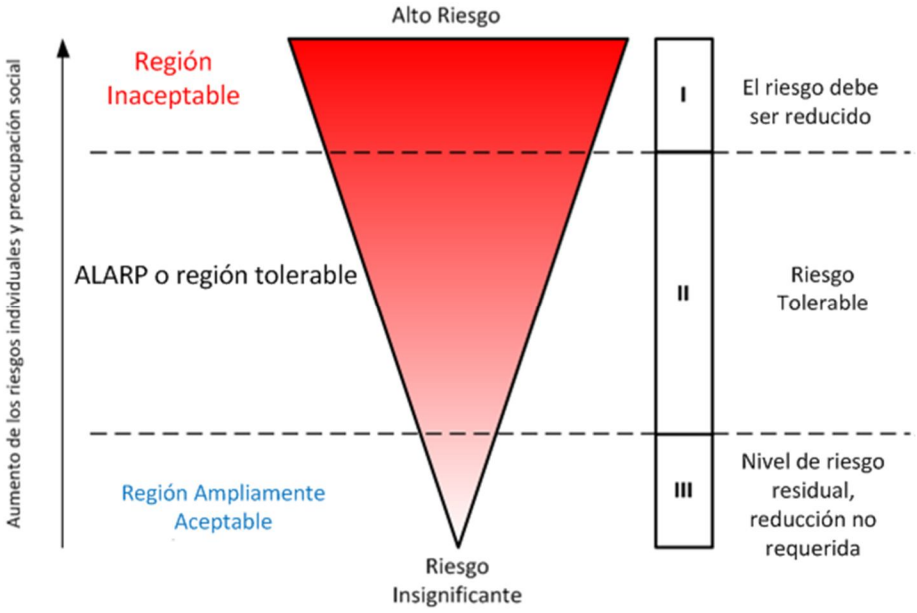


Figura 1.13.3: *Modelo ALARP [10]*

1.13.5.2 Matriz de Riesgos

La matriz de riesgos (Figura 1.13.4) es uno de los métodos más utilizados en la asignación del SIL en industrias de proceso químicas y petroquímicas. La aplicación de esta metodología consiste en la valoración de la probabilidad de ocurrencia de un accidente y la severidad de sus consecuencias. Esta metodología se encuentra en muchos estándares, recomendaciones prácticas y procedimientos internos de compañías, por ejemplo la IEC 61511-3 [4].

	Consecuencias				
Probabilidad	Insignificante (1)	Menor (2)	Moderada (3)	Mayor (4)	Catastrófica (5)
Raro (1)	**Bajo**	**Bajo**	**Moderado**	**Alto**	**Alto**
Improbable (2)	**Bajo**	**Bajo**	**Moderado**	**Alto**	**Extremo**
Posible (3)	**Bajo**	**Moderado**	**Alto**	**Extremo**	**Extremo**
Probable (4)	**Moderado**	**Alto**	**Alto**	**Extremo**	**Extremo**
Casi seguro (5)	**Alto**	**Alto**	**Extremo**	**Extremo**	**Extremo**

Figura 1.13.4: *Matriz de Riesgos [10]*

1.13.5.3 Matriz Tridimensional

Un nuevo eje está diseñado para considerar las capas adicionales de seguridad que se encuentran comúnmente en los procesos industriales. Dicho eje es llamado "cantidad y/o efectividad de capas adicionales" y se refiere a capas fuera del SIS mostrado en el "modelo de la cebolla" (Figura 1.9.1).

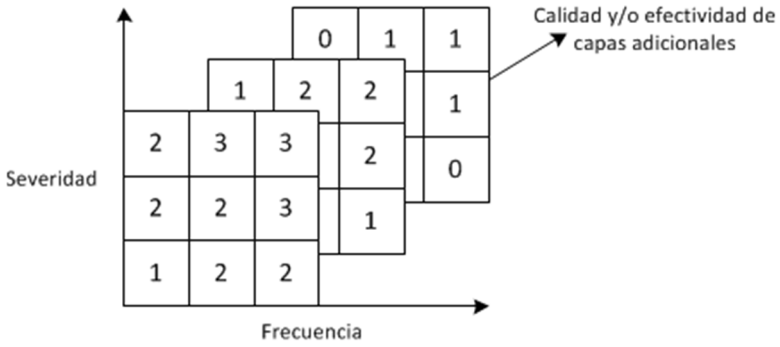


Figura 1.13.5: *Matriz Tridimensional de Riesgo para selección del SIL [10]*

Los números mostrados en los cuadros de la figura 1.13.5 representan diferentes SIL, los mismos que disminuyen con la colocación de una nueva capa de seguridad. Una dificultad asociada, es que la frecuencia de ocurrencia debería ser elegida asumiendo que las capas de seguridad no están instaladas.

Una preocupación al utilizar este método tiene que ver con los juicios cualitativos involucrados debido a que cada compañía puede tener la libertad de definir los niveles y rangos de seguridad un poco diferentes, además la industria simplemente no ha alcanzado y tal vez nunca alcance un consenso sobre todas las decisiones subjetivas y rangos involucrados [15].

1.13.5.4 Análisis de la capa de protección (*Layers Of Protection Analysis*, LOPA)

LOPA utiliza el concepto de capas de protección. Una salvaguarda puede ser considerada como capa de protección cuando cumple cuatro características [10]:

1. **Especificidad.-** Está diseñada únicamente para prevenir o mitigar las consecuencias de un evento peligroso potencial. Causas Múltiples pueden llevar al mismo evento peligroso.

2. **Independencia.-** Es independiente de otras capas de protección asociadas con identificar el peligro. La falla de una capa no impedirá que otra realice su trabajo.

3. **Confiabilidad.-** Se puede contar con ella para hacer aquello para lo que fue diseñada para hacer. Fallas aleatorias y sistemáticas son abordados en el diseño.

4. **Auditabilidad.-** Está diseñada para facilitar la validación periódica de las funciones de protección. Pruebas y/o mantenimiento son necesarios.

1.14 Dispositivos de Campo

Los dispositivos de campo incluyen sensores, elementos finales de control, cableado de campo y otros dispositivos conectados a las terminales de entrada/salida del sistema lógico. Estos dispositivos son a menudo los elementos más críticos y aplicados en los sistemas de seguridad. El énfasis prestado a los dispositivos de campo en el diseño y aplicación de sistemas de seguridad es bastante bajo en comparación con el impacto potencial que estos dispositivos pueden tener en el rendimiento general del sistema [10].

1.14.1 Porcentaje de fallos en el sistema

La figura 1.14.1 muestra el porcentaje de las fallas entre los principales elementos del sistema analizado.

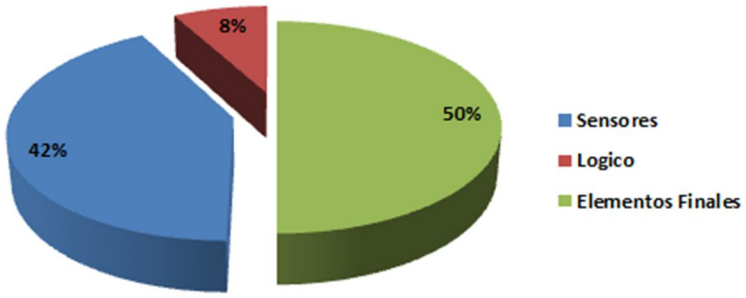


Figura 1.14.1: *Datos de confiabilidad y desempeño [10]*

Como regla general, los dispositivos de campo pueden representar aproximadamente el 90% de fallas del sistema, mientras que el sistema lógico solamente el 10%. Las fallas sistemáticas como especificaciones inadecuadas, pobres procedimientos de mantenimiento y errores de calibración. También tienen un impacto significativo en el desempeño del sistema. Las fallas sistemáticas de los dispositivos de campo pueden ser más elevadas que para el equipo lógico ya que más actividades son centradas en ellos.

1.14.2 Sensores

Los sensores son usados para medir diversas variables como temperatura, presión, flujo y nivel. Al igual que cualquier otro dispositivo pueden fallar de diferentes maneras, pueden fallar de forma segura (activarse de manera errónea) o de forma peligrosa (no activarse en un caso de emergencia). Muchos sistemas de seguridad son diseñados para dar fallas seguras, es decir, cuando se retira la alimentación eléctrica el sistema de seguridad lleva el proceso a un estado seguro. Algunas mediciones pueden ser inferidas de otras variables, por ejemplo, si un sistema está diseñado para realizar el apagado del proceso debido a una alarma de alta presión, podría también ser efectivo monitorear la temperatura ya que debido al proceso, una elevada temperatura podría implicar una alta presión [10].

1.14.3 Elementos finales

Son utilizados para ejecutar el apagado de un proceso. Los más comunes son válvulas. Estos elementos tienen la tasa más elevada de fallas que cualquier otro componente dentro de un sistema ya que al ser elementos mecánicos están sujetos a condiciones extremas del proceso.

Algunos sistemas utilizan las válvulas de control como válvulas de apagado debido a que la válvula de control está normalmente moviéndose todo el tiempo, esto se considera como una "auto-prueba". Compartir elementos finales de control así como sensores no es recomendable [10].

1.14.4 Redundancia

La redundancia es la técnica usada para conseguir un sistema tolerante a fallas. El sistema más común de redundancia de hardware es la votación por mayoría. Es adecuada para fallas imprevistas que afectan a las acciones del sistema y se compensan con funciones redundantes en el sistema. La redundancia del sistema vendrá definida por la arquitectura seleccionada, dicha selección es una actividad que sebe ser definida durante el paso del diseño conceptual. La arquitectura tiene un fuerte impacto sobre la integridad de la seguridad del sistema. Se debe determinar qué nivel de redundancia se requiere para lograr el SIL objetivo y la disponibilidad para todos los elementos que conforman el SIS.

La redundancia es un término que se utiliza en automatización para conseguir esencialmente la disponibilidad de los elementos deseados [10].

En este capítulo se analizó las normas y los conceptos básicos para el diseño y desarrollo de un SIS. Se citó algunos eventos ocurridos que estuvieron relacionados con la seguridad funcional, los cuales, son un claro ejemplo de las consecuencias catastróficas que pueden resultar de un evento inesperado.

Se estudió los métodos y técnicas utilizados en la determinación del SIL, realizando un enfoque detallado en el método del HazOp.

Se examinó cada una de las etapas del ciclo de vida del SIS y también se analizó ejemplos de fallas que tuvieron lugar en cada una de dichas etapas.

Capítulo 2

ESTADO DEL ARTE

2.1 Avances en el Desarrollo de SIS

2.1.1 Fallas de causa común (*Common Cause Failure*, CCF)

Las fallas de causa común son una seria amenaza para la confiabilidad de los SIS y podrían provocar fallas simultáneas de componentes redundantes y barreras de seguridad [29, 32]. La norma IEC 61508 define a las CCF como "una falla que resulta en uno o más eventos, causando fallas de dos o más canales separados en un sistema multicanal, dando lugar a una falla en el sistema". Un canal es una trayectoria redundante simple dentro de una
SIF [18].

Potenciales CFF pueden ser introducidas en la fase de diseño (comprensión inadecuada de mecanismos de falla y respuesta) así como en la fase operacional (pruebas inapropiadas, errores humanos durante la operación y mantenimiento). Algunos autores encuentran útil dividir las causas de CCF en causas raíz[3] y factores de acoplamiento[4] [25, 26].

2.1.1.1 Un nuevo enfoque de defensa contra CFF

Un nuevo enfoque se concentra en seguir los siguientes aspectos:

1. Evitar introducir CCF durante las pruebas de funcionamiento e inspección.

2. Identificar CCF's y sus causas basadas en reportes de fallas.

3. Utilizar el conocimiento de causas de falla para seleccionar medios eficientes para evitar futuras CCF's.

El enfoque de defensa contra CCF sigue las principales tareas de funcionamiento e inspección que se muestran en la figura 2.1.1.

[3] Una causa raíz es una causa básica de falla de un componente (Por ejemplo: corrosión)

[4] Un factor de acoplamiento explica por qué algunos componentes son afectados por la misma causa raíz.

Las seis tareas están basadas en listas de verificación y métodos analíticos como diagramas de secuencia operacional (*Operational Sequence Diagrams*, OSD), diagramas de influencia y matrices de causa-defensa [18, 25].

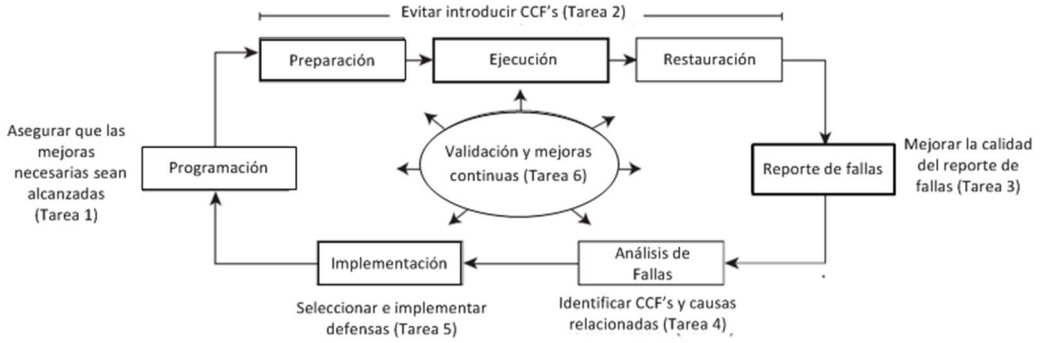


Figura 2.1.1: *Principales conceptos del enfoque de defensa contra las CCF [18].*

Las tareas principales se detallan a continuación:

1. **Asegurar que las mejoras necesarias son alcanzadas.-** La programación de procedimientos de prueba funcional e inspección se realiza generalmente de forma automática y con intervalos predefinidos por el sistema de gestión de mantenimiento. Durante el proceso de planificación, se crea un paquete de trabajo que especifica el tipo de recursos, un estimado de horas necesarias para realizar el trabajo y el procedimiento de prueba que se utiliza. Una defensa importante contra las CCF es asegurar que las correcciones y mejoras en el procedimiento de prueba se capturan cuando se crean nuevos paquetes de trabajo de prueba funcional o inspección.

2. **Evitar introducir CCF durante la preparación, ejecución y restauración.-** La experiencia ha demostrado que las CCF son introducidas a menudo durante el mantenimiento debido a errores humanos (acciones deliberadas, omisión accidental o ejecución inadecuada), procedimientos erróneos (mala calibración de equipos y ajustes inapropiados) y deficientes procesos de trabajo (inadecuada coordinación entre disciplinas de mantenimiento). Resulta favorable utilizar listas de verificación independientes las tres tareas: la preparación, la ejecución y la restauración. A menudo, los componentes similares (transmisores de presión) dentro de la misma zona se prueban simultáneamente.

En este caso, la lista de verificación de preparación se puede aplicar una vez, mientras que las listas de ejecución y restauración se deben repetir para cada componente probado o inspeccionado.

3. **Mejorar la calidad del reporte de fallas.-** En la actualidad los sistemas de gestión de mantenimiento no tienen registro directo de las CCF, éstas tienen que ser identificadas a partir de eventos de falla registrados, pero la clasificación de fallas puede ser interpretada de diferentes maneras. Las bases de datos correspondientes a fallas requieren acceso a descripciones más profundas de causas y efectos. Cualquier información deficiente puede ser difícil de reunir en una etapa posterior, ya que el personal involucrado puede estar ausente.

4. **Identificar las CCF a través de un análisis de fallas.-** El Análisis de fallas de fallas registradas es usualmente realizado por el sistema o por un equipo de ingenieros, dicho análisis servirá para identificar las CCF. El principal objetivo es la identificación de los CCF con el fin de seleccionar las defensas específicas adecuadas, puede ser necesario también para desarrollar procedimientos y sistemas para la recopilación e intercambio de datos sobre las CCF. Los principales resultados del análisis son las causas y los factores de acoplamiento que se pueden enumerar en una matriz causa-defensa simplificada, como se ilustra en la figura 2.1.2.

CCF	Causa Raíz	Factor de Acoplamiento	Defensas alternativas	R	C	Impacto (A/M/B)	Costo (A/M/B)
Falla de las válvulas de apagado	Solenoide atascado debido a polución en la fuente hidráulica	Mismo diseño	Implementar control periódico de la calidad de la hidráulica	√	√	M	B
		Conectada a la misma fuente hidráulica	Instalar filtros en la fuente hidráulica	√		A	M
			Reemplazar solenoides existentes por nuevos y robustos				

R = Causa Raíz (Root)
C = Factor de acoplamiento (Coupling Factor)
A = Alto
M = Medio
B = Bajo

Figura 2.1.2: *Matriz causa-defensa simplificada.*

5. **Implementar medidas de defensa.-** Implementar defensas es importante para prevenir futuras ocurrencias de fallas similares. En las matrices causa-defensa, un conjunto de defensas predefinidas son consideradas para cada causa raíz y factor de acoplamiento. Algunos tipos de defensas son cubiertas, como mejoras relacionadas con el diseño, procedimientos relacionados y barreras físicas. El impacto esperado para todas las defensas alternativas es evaluado y utilizado para medir su eficiencia. Para el enfoque de defensa es recomendable aplicar matriz de causa-defensa simplificada, es decir, que el análisis de impacto esté limitado a una pequeña selección de opciones de defensa.

6. **Validación y mejoras continuas.-** Las fallas sistemáticas que pueden llevar a CCF, no siempre son capturadas a través de la ejecución y seguimiento de pruebas funcionales e inspección. Validar todas las tareas de trabajo en intervalos regulares con respecto a la forma en que cumplen con el nuevo enfoque puede capturar debilidades y conducir a la mejora continua. También puede ser relevante para evaluar el efecto de las defensas aplicadas, ya sea cualitativamente o cuantitativamente.

Una limitación principal de la versión actual del enfoque de defensa contra CCF es la falta de medios cuantitativos para indicar las tendencias en el estado de las defensas contra CCF en la fase operacional. Por lo tanto, esta es una importante área para la investigación futura. Hay algunas otras ideas para trabajo a futuro. Una cuestión obvia es poner a prueba las listas de verificación y herramientas de la industria de petróleo y gas, y analizar información para futuras mejoras de la metodología. Otra área es considerar otras técnicas analíticas, por ejemplo, para el análisis de las causas y los factores de acoplamiento.

Una última cuestión es analizar nuevos conceptos operativos y la tecnología y cómo se pueden introducir nuevas causas de CCF. En el futuro, se puede esperar un amplio uso de las pruebas de funcionamiento automatizadas y nuevas formas de interacción humana que pueden introducir nuevas molestias a la tecnología, así como a los seres humanos y las organizaciones [26].

2.1.2 Activaciones Esporádicas

Las activaciones esporádicas del SIS pueden resultar en un apagado parcial o total del proceso. Podrían ser la consecuencia de una falsa demanda del proceso o fallas en un elemento del SIS.

En la industria de procesos es muy importante reducir la cantidad de activaciones esporádicas para evitar pérdidas de producción innecesarias, reducir el riesgo relacionado a dichas activaciones y evitar peligros durante la restauración y reinicio no programado del sistema. El enfoque principal del estándar IEC 61511 es asegurar que el SIS esté disponible para actuar bajo demanda, por ello requiere que una tasa máxima de activaciones esporádicas (*Spurious Trip Rate*, STR) sea especificada, pero el estándar no provee una guía para estimar la STR [20].

2.1.2.1 Causas de activaciones esporádicas

- **Operación esporádica (*Spurious Operation*, SO).-** Una SO es la activación de un elemento del SIS sin la demanda del proceso especificado. Por ejemplo, una lectura errónea de nivel debido a una falla del transmisor. Se deben a dos causas principales:

  - Una falla interna del elemento o de su equipo de apoyo.
  - El elemento de entrada responde a una demanda falsa.

  Fallas por SO debidas a fallas internas son a menudo consideradas fallas seguras ya que no impiden que el SIS se desempeñe bajo demanda. Sin embargo, todas las fallas seguras no conducen a SO, por ello es necesario estudiar los modos de falla segura para cada elemento y así determinar cuáles son relevantes para la SO. Los estándares IEC 61508 e IEC 61511 distinguen dos clases de fallas seguras, fallas seguras aleatorias de hardware[5] y fallas seguras sistemáticas[6] [20, 4, 3].

- **Activación esporádica (*Spurious Trip*, ST).-** Una ST es la activación de uno o más elementos del SIS, provocando que el SIS ejecute una SIF sin la presencia de una demanda del proceso especificado.

[5] Fallas debidas principalmente a la degradación normal.

[6] Fallas debidas a errores de diseño o exposición excesiva al ambiente.

Por ejemplo, dos detectores de llama en una configuración 2oo3 dan una falsa señal provocando que el sistema contra incendios se active. Hay algunas causas para activaciones esporádicas, por ejemplo:

- Pérdida de características neumáticas, hidráulicas o energía del sistema.
- Fallas peligrosas detectadas: En algunos casos, el SIS puede ser diseñado para activar esporádicamente una SIF si las fallas peligrosas detectadas constituyen un obstáculo para que la SIF funcione bajo demanda.

Una SIF también podría activarse debido a errores humanos, por ejemplo, pruebas de funcionamiento [20].

- **Apagado esporádico (*Spurious Shutdown*, SS).-** Un apagado esporádico es un apagado parcial o total del proceso sin la demanda del proceso especificado. Una activación esporádica usualmente pero no siempre llevará al proceso a un apagado esporádico. Si la SIF no interactúa directamente con el proceso entonces el proceso no será perturbado. Un apagado esporádico también podría ser ocasionado por el cierre o paro de equipo que no pertenece al SIS pero interactúa con el proceso (bombas y válvulas de control) [20].

2.1.2.2 Nuevas técnicas para determinar la STR

- **Operación esporádica:**

La STR debida a fallas internas de una configuración 1oon de elementos de tipo j[7] es:

$$STR_{1,j} = n\lambda_{SO,j} \qquad (2.1.1)$$

Si los elementos son expuestos a CCF, eso puede ser modelado por un modelo de factor $\beta_j^{SO}\lambda_{SO,j}$[8] obteniendo así una STR:

$$STR_{1,j} = n\left(1-\beta_j^{SO}\right)\lambda_{SO,j} + \beta_j^{SO}\lambda_{SO,j} = n\lambda_{SO,j} - (n-1)\beta_j^{SO}\lambda_{SO,j} \qquad (2.1.2)$$

La STR para una configuración de *k*oo*n* de elementos tipo j debido a fallas internas es:

$$SRT_{1,j}^{koon} = n\left(1-\beta_j^{SO}\right)\lambda_{SO,j}P_r(M \geq k-1) + \beta_j^{SO}\lambda_{SO,j}$$

[7] Elementos tipo j.- Son elementos tipo "a" (Sus modos de falla son conocidos) o tipo "b" (No todos sus modos de falla son conocidos).

[8] Factor de falla común para elementos tipo j debido a operaciones esporádicas.

$$\approx n\left(1-\beta_j^{SO}\right)\lambda_{SO,j}\left[\sum_{m=k-1}^{n-1}\binom{n-1}{m}p^m(1-p)^{n-1-m}\right]+\beta_j^{SO}\lambda_{SO,j} \qquad (2.1.3)$$

En donde $p = \left(1-\beta_j^{SO}\right)\lambda_{SO,j}MDT_j$, MDT = Tiempo medio de paro (*Mean Down Time*).

En el caso de falsas demandas la STR se expresa de la siguiente manera:

$$STR_{2,j} = (\lambda_F + \lambda_{SF})(1-PFD) \qquad (2.1.4)$$

En donde λ_F es la tasa de fallas y λ_{SF} es la tasa de fallas seguras. La PFD de una SIF es tan pequeña que la parte (1-PFD) puede ser omitida.

- **Fallas peligrosas detectadas:**

La STR para una configuración *koo*n de elementos de tipo j está dada por:

$$SRT_{3,j}^{koon} = n\left(1-\beta_j^{DD}\right)\lambda_{DD,j}P_r(M^* \geq n-k) + \beta_j^{DD}\lambda_{DD,j}$$

$$\approx n\left(1-\beta_j^{DD}\right)\lambda_{DD,j}\left[\sum_{m=k-1}^{n-1}\binom{n-1}{m}(P^*)^m x(1-p^*)^{n-1-m}\right]+\beta_j^{DD}\lambda_{DD,j}$$

En este caso $MDT^* = (n-1, p^*)$ ya que está distribuido binomialmente. En donde $P^* = \left(1-\beta_j^{DD}\right)\lambda_{DD,j}MDT^*$.

2.1.2.3 Fórmulas simplificadas

En la tabla 2.1 se muestran nuevas fórmulas para algunas configuraciones seleccionadas, para ello se han realizado las siguientes suposiciones [11]:

- Las contribuciones de falsas demandas, demandas no previstas y fallas sistemáticas serán despreciables en la mayoría de los casos.

- Las contribuciones de fallas independientes ocurriendo durante el MDT han sido omitidas ya que su contribución puede ser despreciable en comparación con la contribución de las CCF.

- La ISA [12] y la PSD [23] utilizan el (peligroso, *dangerous,* D) factor β "convencional", denotado como β^D.

- La ISA [12] incluye todas las fallas seguras en sus fórmulas. Para comparar las fórmulas, se asume que λ_S es igual a λ_{SO}.

Configuración	**Aproximación**		
	Nueva	**PSD [23]**	**ISA [12]**
1oo1	$\lambda_{SO} + \lambda_{DD}$	λ_{SO}	$\lambda_S + \lambda_{DD}$
1oo2	$(2 - \beta^{SO})\lambda_{SO} + \beta^{DD}\lambda_{DD}$	$2\lambda_{SO}$	$2(\lambda_S + \lambda_{DD}) + \beta^D(\lambda_S + \lambda_{DD})$
1oo3	$(3 - 2\beta^{SO})\lambda_{SO} + \beta^{DD}\lambda_{DD}$	$3\lambda_{SO}$	$3(\lambda_S + \lambda_{DD}) + \beta^D(\lambda_S + \lambda_{DD})$
2oo3	$\beta^{SO}\lambda_{SO} + \beta^{DD}\lambda_{DD}$	$2.4\beta^D\lambda_{SO}$	$\beta^D(\lambda_S + \lambda_{DD})$
2oo4	$\beta^{SO}\lambda_{SO} + \beta^{DD}\lambda_{DD}$	$4\beta^D\lambda_{SO}$	$\beta(\lambda_S + \lambda_{DD})$

Tabla 2.1: *Fórmulas aproximadas para obtener la STR [20]*

Las nuevas fórmulas se han establecido teniendo como base las nuevas definiciones de activaciones esporádicas.
Sus principales ventajas son:

- Pueden ser utilizadas para cualquier configuración *koo**n***.

- Capturan las causas más importantes de las activaciones esporádicas identificadas.

- Consideran las diferentes fallas peligrosas y fallas por activaciones esporádicas que contribuyen a la STR.

Además han sido comparadas con otras fórmulas que son frecuentemente utilizadas en la industria de petróleo y gas. Aunque a primera vista las fórmulas pueden verse un poco diferentes, los resultados obtenidos no varían demasiado.

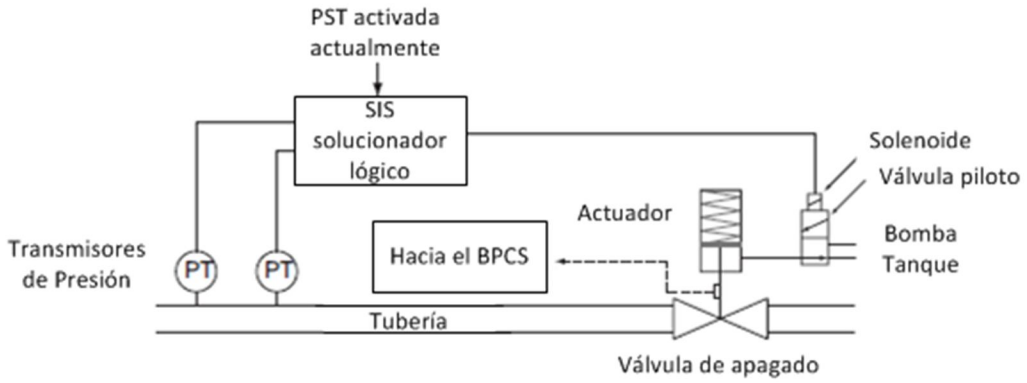
Un área importante para investigaciones futuras es la de conseguir una visión más clara de las causas de las SO y las activaciones esporádicas, y cómo se pueden equilibrar la seguridad y la disponibilidad. En muchos sectores de la industria, el estado de falla segura no está bien definido y una activación esporádica o un apagado esporádico pueden dar lugar a situaciones peligrosas.

2.1.3 Pruebas de cierre parcial (*Partial Stroke Test*, PST)

Las pruebas funcionales implican detener el proceso, esto resulta perjudicial ya que las pérdidas de producción y por tanto las económicas son considerables debido al tiempo de paro. Para evitar dichas pérdidas se ha desarrollado una técnica conocida como PST.

Esta técnica consiste en cerrar una válvula de manera parcial y regresarla a su posición inicial. Dicho cierre es tan pequeño que el impacto en el flujo o presión del proceso es despreciable, pero este movimiento puede ser suficiente para revelar algunos tipos de fallas. En procesos continuos la PST es económicamente más viable que las pruebas de funcionamiento. El incremento en la confiabilidad que se gana por introducir la PST mejora la seguridad y/o reduce costos [19] ya que los intervalos entre las pruebas periódicas funcionales no son afectados.

La PST es introducida para detectar, sin perturbar el proceso. La medida en que la PST pueda detectar fallas depende de la manera en la que esté implementada. Dos variantes de implementación se muestran en la figura
2.1.3, en la primera como parte integrada del SIS y en la segunda como una parte separada [19].



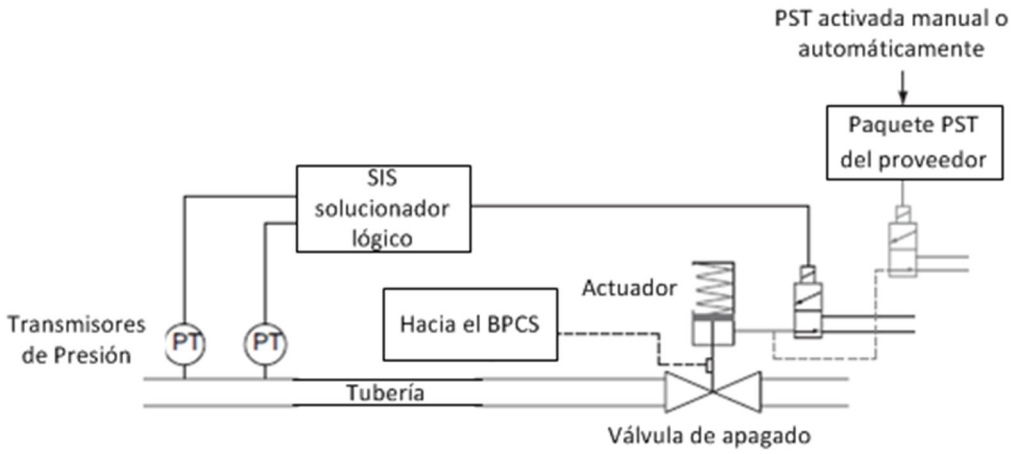


Figura 2.1.3: *Modos de implementación de PST [19]*

Los estándares [3] y [4] distinguen dos tipos principales de pruebas relacionadas con los SIS en la fase de funcionamiento, pruebas de diagnóstico[9] y pruebas funcionales[10] [19].

2.1.3.1 Efectos de confiabilidad al introducir PST

La fracción de fallas peligrosas no detectadas que son detectadas por PST entre todas las fallas DU es llamada "cobertura de la PST", y se define como:

$$\theta_{PST} = \frac{\lambda_{DU,PST}}{\lambda_{DU}} \qquad (2.1.5)$$

En donde:

$\lambda_{DU,PST}$ = Tasa de fallas DU que pueden ser detectadas por PST.
λ_{DU} = Total de fallas DU.

La cobertura de la PST también puede ser expresada como la probabilidad condicional:

[9] Identifican automáticamente y reportan ciertos tipos de fallas así como sus causas.
[10] Revelan todas las fallas peligrosas del SIS, por ello puede ser restaurado a su funcionalidad después de la prueba.

$$\theta_{PST} = P_r \text{ (Falla DU detectada por PST| Falla DU presente)} \qquad (2.1.6)$$

La cobertura de la PST para válvulas de cierre o apagado es a menudo considerado en el rango del 60-70% [30].

El valor de θ_{PST} para una aplicación específica debería ser determinada en base a condiciones específicas en la planta, como el tipo de válvula, requisitos de funcionamiento y condiciones ambientales y de operación. Cuando no está implementada la PST, la PFD promedio de la válvula de cierre es aproximadamente la suma de la PFD promedio de la prueba funcional (PFD_{FT}) y la PFD promedio de la prueba de diagnóstico (PFD_{DT}) [19].

$$PFD \approx PFD_{FT} + PFD_{DT} \approx \frac{\lambda_{DU}.\tau_{FT}}{2} + \frac{\lambda_{DU}.\tau_{DT}}{2} \qquad (2.1.7)$$

En donde:

τ_{FT} = Intervalo de prueba funcional.
τ_{DT} = Intervalo de prueba de diagnóstico.

El intervalo de la prueba de diagnóstico es generalmente muy pequeño, por lo tanto la PFD_{DT} es despreciable. Ya que la PST puede detectar solamente una fracción, θ_{PST}, de las fallas DU; entonces la PFD puede quedar expresada de la siguiente manera:

$$PFD \approx PFD_{FT} + PFD_{DT} \approx (1 - \theta_{PST}).\frac{\lambda_{DU}.\tau_{FT}}{2} + \theta_{PST}.\frac{\lambda_{DU}.\tau_{PST}}{2} \qquad (2.1.8)$$

En donde:

τ_{PST} = Es el intervalo de la PST.

La PFD es reducida cuando se introduce PST, ya que una fracción de las fallas DU es revelada y corregida dentro de un intervalo de tiempo más corto después de que ocurran, que por las pruebas de funcionamiento. Entonces, si el intervalo de prueba funcional se mantiene sin cambios, la confiabilidad de la SIF es mejorada [19, 27].

2.1.3.2 Procedimientos para determinar la cobertura de PST

El procedimiento está configurado para la fase inicial de diseño, pero también se puede utilizar para actualizar la estimación de la cobertura de PST en la fase operativa. Una importante suposición es que la cobertura de la PST es una característica de los componentes individuales del SIS en lugar de un grupo de componentes, y debería ser determinado en este nivel [19].

$$\theta_{PST} = \frac{Pr(Falla\ DU\ detectada\ por\ PST \cap Falla\ DU\ presente)}{Pr(Falla\ DU\ presente)} \qquad (2.1.9)$$

Definiendo como $FM_1, FM_2, \dots, FM_n$ a los modos relevantes de falla DU, la ecuación antes mostrada se puede escribir de la forma:

$$\theta_{PST} = \sum_{i=1}^{n} \frac{\Pr(FM_i\ Detectadas|FM_i\ presente).\Pr(FM_i\ presente)}{\Pr(Falla\ DU\ presente)} \qquad (2.1.10)$$

Haciendo una analogía con la ecuación 2.1.5 se define:

$$\theta_{FM,i} = \Pr(FM_i\ Detectadas|FM_i\ presente) \qquad (2.1.11)$$

Como la cobertura de la PST del modo FM_i de la falla DU para i = 1, 2, …, n.

La fracción

$$w_i = \frac{\Pr(FM_i\ presente)}{\Pr(Falla\ DU\ presente)} \qquad (2.1.12)$$

Es la fracción de fallas FM_i entre todas las fallas DU para i = 1, 2, …, n.

La cobertura de la PST puede sin embargo ser expresada como:

$$\theta_{PST} = \sum_{i=1}^{n} \theta_{FM,i}.w_i \qquad (2.1.13)$$

Se sugiere que la cobertura de la PST por modo de falla está determinada en dos sub-pasos, ya que la detección exitosa de un modo de falla yace en dos factores:

- El modo de falla debería ser revelable durante una operación de cierre parcial (revelavibilidad por modo de falla).

- Es importante que los resultados sean confiables, tal que los resultados anunciados reflejen la condición de la válvula (confiabilidad de la PST por modo de falla).

Esto significa que:

$$\theta_{FM,i} = PST_{Rev,i}.PST_{Rel,i} \qquad (2.1.14)$$

En donde:

$PST_{Rev,i}$ = Revelabilidad por PST del modo "i" de falla.
$PST_{Rel,i}$ = Es la confiabilidad de la PST del modo "i" de falla.

La revelabilidad podría ser determinada por juicio experto, mientras se sugiere que la confiabilidad de la PST está basada en una lista de verificación. El procedimiento comprende seis pasos.

- Paso 1: Familiarizarse con la PST y su implementación.- Recolectar información relevante en la implementación de PST y la aplicación de condiciones específicas como:

  Qué componentes del SIS son operados durante una PST.

  - Cómo la PST es iniciada y controlada por software y hardware especializados.
  - La interfaz de la PST con el SIS y otros sistemas.

- Paso 2: Analizar el hardware y el software de la PST.- Identificar y analizar como las fallas del hardware y software de la PST afectan la ejecución de la misma y del SIS.

- Paso 3: Determinar la confiabilidad de la PST.- Es una medida de la capacidad del hardware y software de la PST para proveer resultados muy útiles y confiables. Se propone una lista de verificación para calcular la confiabilidad de la PST.

- Paso 4: Determinar la revelabilidad (por modo de falla).

- Paso 5: Determinar los pesos de los modos de falla.- Los pesos de la ecuación 2.1.12 puede determinarse por juicio experto o análisis histórico de datos de falla.

- Paso 6: Determinar la cobertura de la PST.- Puede ser determinada utilizando la ecuación 2.1.13.

Las principales desventajas del nuevo procedimiento podrían estar relacionadas a la implementación práctica. Primero, las preguntas de la lista de verificación podrían ser utilizadas para hacer mejoras erróneas a la cobertura de la PST, particularmente si la implementación de las preguntas de la lista de verificación no corresponden a como se ejecuta la PST en la fase operacional. Segundo, el procedimiento también requiere que el usuario final pase más tiempo en comprender el hardware y software que el empleado normalmente.

Nuevas investigaciones pueden ser necesarias para elaborar una lista de verificación genérica y ampliamente aceptada por la confiabilidad de la PST, similar a lo que se ha hecho en la lista de verificación en la determinación de los factores beta en el estándar IEC 61508. También los efectos secundarios de la PST deben ser analizados y apoyados por la recolección de datos. Sin este tipo de clasificación, puede ser difícil de utilizar datos históricos para confirmar en qué medida PST es capaz de revelar fallas DU [19].

2.2 Tecnología aplicada a los SIS

En la década de 1960 se introducen los primeros interruptores de estado sólido (basados en transistores) y unidades lógicas. La introducción de la tecnología de estado sólido fue punto de partida para el desarrollo de aplicaciones de control lógico; debido a que estos elementos tienen un modo de falla predecible (Transistores, diodos y triacs principalmente) se estableció que debían ser configurados en forma redundante para ser utilizados en sistemas de protección. La invención del circuito integrado en 1958 prepara el camino para la aparición de microprocesadores y microcomputadores. En los años 80 se empiezan a utilizar los PLC's, pero al igual que los sistemas de estado sólido tenían un modo de fallo predecible, por lo que también debieron adoptar un esquema redundante para alcanzar los requisitos de seguridad ante fallos.

Las configuraciones de PLC's redundantes durante un período fueron especificados para aplicaciones de seguridad funcional. Aunque era una solución fiable, daba problemas de disponibilidad.

No es hasta la aparición de los microprocesadores de 32 bits (finales de los años 80), con una alta velocidad de procesamiento, cuando se empieza a desarrollar equipos de seguridad mediante PLC's redundantes, debido entonces, a un precio ya razonable para la industria y además cumplían dos premisas básicas en sistemas de seguridad, disponibilidad y fiabilidad. A continuación se muestra un resumen de la evolución en sistemas instrumentados de seguridad [9].

Años 60: Lógica cableada con relés e interruptores e instalación en donde se identificaba la necesidad de seguridad.

Años 70: Lógica cableada con relés e interruptores, lógica de estado sólido e instalación en donde se identifica la necesidad de seguridad.

Años 80: Comienzo de uso de PLC's. Primera generación de sistemas instrumentados de seguridad, TMR (Triple Modular Redundancy, Ej. Tricon de TRICONEX). Se desarrolla el procedimiento HAZOP.

Años 90:

- Surgen los PLC's de seguridad.
- Segunda generación de sistemas instrumentados de seguridad. Emplean un alto nivel de diagnóstico acoplado a técnicas de votación[11] (1oo2, 2oo3) para proveer seguridad y disponibilidad con más tolerancia a fallos y menos costo que los sistemas de primera generación. Ej. H41q/H51q de HIMA, FSC de Honeywell, evolución de Tricon de TRICONEX. Sistemas certificados por TÜV[12] (Technischer Überwachungs-Verein) según el estándar IEC 61508 a finales de la década de los 90.
- Se desarrollan estándares para los PLC's de seguridad.
- Aparecen las arquitecturas con diagnóstico.
- Se desarrollan metodologías para el análisis cuantitativo de riesgos.
- Se introducen metodologías para la identificación sistemática de riesgos.

[11] Método de diseño en el cual se consideran los casos de falla de m de n elementos en un sistema.

[12] Son organizaciones certificadoras alemanas que tratan de prevenir a los seres humanos y al medio ambiente frente a los peligros que provienen de fábricas y de mecanismos de cualquier tipo.

Años 2000:

- Equipos certificados para aplicaciones de seguridad (Válvulas y transmisores) según IEC 61508.

- Aparece la tercera generación de sistemas instrumentados de seguridad de Redundancia Modular Flexible
(*Flexible Modular Redundancy*, FMR), certificados por TÜV según IEC 61508. Ej. Delta V SIS de EMERSON, SIMATIC S7-F/FH de SIEMENS.

- Ofrecen un alto nivel de diagnósticos.

- Alta integración con el Sistema de Control Distribuido (*Distributed Control System*, DCS).

- Son sistemas altamente modulares y escalables.

- Ofrecen herramientas avanzadas de programación.

- Se implantan los procesos basados en el ciclo de vida de seguridad.

- Aplicación de IEC 61511.

Se debe considerar que ninguna tecnología es mejor que las otras, cada una de ellas tiene sus ventajas y desventajas. No se trata sobre cuál es la mejor sino de cuál es la más apropiada, considerando factores como el nivel de riesgo, complejidad, flexibilidad, mantenimiento y seguridad. Algunas de las tecnologías utilizadas en SIS se detallan a continuación:

2.2.1 Sistemas Neumáticos

Son relativamente simples y seguros a fallas, en caso de suscitarse una falla usualmente resulta en la despresurización del sistema iniciando así el apagado. Necesitan obligatoriamente de un gas limpio y seco. Es necesaria la operación y/o pruebas frecuentes para evitar situaciones de riesgo. Son muy utilizados en aplicaciones pequeñas en donde se busca simplicidad, seguridad intrínseca y en donde la energía eléctrica no está disponible.

2.2.2 Sistemas Basados en Relés

Son relativamente simples, además son económicos e inmunes a interferencias electromagnéticas (*ElectroMagnetic Interference*, EMI) o interferencias por radio frecuencia (*Radio Frecuency Interference*, RFI). Son propensos a sufrir activaciones esporádicas y pueden llegar a ser difíciles de manejar cuando el sistema es complejo. En ocasiones se requiere realizar cambio en la lógica del sistema, por ello el cableado se debe cambiar y los diagramas de conexión deben ser actualizados. Los sistemas basados en relés utilizan señales lógicas discretas (encendido/apagado, on/off). Los relés son muy utilizados en sistemas pequeños en los cuales no tienen más de 15 entradas y salidas (IN/OUT, I / O) aproximadamente.

2.2.3 Sistemas de Estado Sólido

Fueron desarrollados para reemplazar a los relés por circuitos pequeños y de baja potencia. Estos sistemas son muy especializados, relativamente costosos con respecto a otras tecnologías, además tienen aplicaciones limitadas y no son muy comunes.

Sus principales ventajas son:

- Incluyen características de prueba como luces y pueden ejecutar tareas de bypass.
- Ofrecen la capacidad de comunicarse de manera serial con sistemas computarizados externos.
- Pueden responder más rápido que otros sistemas basados en software.

Sus desventajas son:

- Necesitan cables al igual que los relés, esto implica que al realizar cambios en sus conexiones los planos deben ser actualizados.
- Desempeñan la misma clase de lógica digital al igual que los relés. En la actualidad algunos sistemas ya disponen de entradas de señales analógicas.
- Pueden ser muy costosos, pero ofrecen mayor funcionalidad que los relés y no necesitan software como un PLC.

- Son utilizados en configuraciones no redundantes ya que si uno falla podría provocar falsas alarmas en el proceso.

2.2.4 Sistemas Basados en Software (Microprocesador/PLC)

Son utilizados en un gran porcentaje de aplicaciones. Los PLC fueron desarrollados para reemplazar a los relés pero su incursión en el campo de la seguridad ha sido inevitable.

Sus principales ventajas son:

- Costo razonable
- Facilidad para realizar cambios, es decir, no es necesario realizar cambios en el cableado sino que estos pueden realizarse en el programa principal. Aunque esto es una ventaja muy favorable también es una ruta abierta a cambios indebidos o erróneos que pueden provocar fallas en el sistema.
- Comunicación serial ya que puede transferir información a otros sistemas.
- Interfaces de operador.
- Auto documentación.
- Tamaño reducido.

Los sistemas basados en software van desde PLC's de propósito general hasta PLC's orientados a seguridad. Sin embargo algunos de estos sistemas no están orientados específicamente a la seguridad por lo que no ofrecen altos niveles de diagnóstico y redundancia efectiva que pudieran ser requeridos.

2.3 SIS en el Mercado Internacional

Son muchos los fabricantes de SIS que se encuentran en el mercado, todos ellos están en constante desarrollo de nuevos equipos que ofrezcan mayores prestaciones en las aplicaciones en las que están involucrados. Al igual que en otros campos, algunos de estos fabricantes poseen gran parte del mercado en el que se desarrollan. Los sistemas instrumentados de seguridad no escapan a esto, algunas de las principales marcas comerciales de SIS se detallan a continuación:

- TRICONEX
- ICS Triplex
- Hima
- Allen Bradley
- Siemens
- Modicon

Pero el desarrollo de nuevas tecnologías ha dado lugar a nuevos fabricantes que buscan un lugar en el mercado desarrollando nuevos sistemas para aplicaciones en la industria de procesos, algunos ejemplos de estos fabricantes son:

- Babbitt Steam Specialty Co.- Fabricantes de válvulas para operaciones en ambientes muy extremos.
- Pilz GmbH & Co. KG.- Es una empresa innovadora en tecnología de automatización.
- Tapeswitch Corporation.- Proveedores de elementos de seguridad interlocks magnéticos y electrónicos.
- Innominate Security Technologies AG.- Líder en tecnología de dispositivos de seguridad embebidos en aplicaciones industriales.
- Interroll.- Fabricante de productos para logística interna y automatización.

- GreCon Inc.- Detección de chispas, sistemas de prevención de fuego y explosiones de polvo en silos y equipos del almacenamiento.

- SEL.- Fabrican productos para protección, monitoreo y control de sistemas de líneas eléctricas.

- Pepperl+Fuchs GmbH.- Desarrolla y manufactura de sensores y componentes electrónicos para automatización de sistemas.

- Yokogawa.- Fabrica productos para medida, instrumentación de campo, información y procesos de control.

2.4 Nuevas Técnicas Utilizadas

El SIS no podrá cumplir su función si todos sus componentes no están trabajando adecuadamente, esto se debe a que el rendimiento de esos componentes eventualmente se degradará con el paso del tiempo. Se puede mejorar las posibilidades de que el SIS esté funcionando correctamente parando el proceso para ejecutar pruebas funcionales y mantenimiento preventivo, pero la producción perdida y los mayores costos de mano de obra hacen que esa sea una solución costosa.

Nuevas técnicas se han desarrollado para obtener diagnósticos en línea, un ejemplo de esto es el SIS inteligente. Este puede dar una mejor vista de lo que está sucediendo en el proceso, también proporciona más que una luz informativa para indicar que se ha producido una falla. En lugar de eso, entrega una clara imagen de cuál es el problema y en donde está.

2.4.1 Sistema Instrumentado de Seguridad Inteligente

Un sistema instrumentado de seguridad inteligente incluye los componentes primarios de cualquier sistema instrumentado de seguridad (sensores, solucionador lógico y elementos finales de control) pero aprovecha el flujo de información en todo el lazo de seguridad. Este flujo incluye no solo datos de medición y control tradicionales, sino información adicional sobre la condición operativa del equipo y del proceso.

Para ello dispone de los siguientes recursos:

2.4.1.1 Dispositivos de campo inteligentes

Estos dispositivos usan microprocesadores incorporados para reunir, manejar y comunicar no sólo variables de proceso y señales de control, sino también información acerca del estado de los dispositivos mismos, del equipo relacionado e incluso del proceso analizado. Esta información permite que los diagnósticos detecten, identifiquen e incluso predigan problemas que podrían conducir a seguridad deficiente o reducir la fiabilidad del SIS, por ejemplo, un transmisor de temperatura inteligente puede avisar cuando detecta una sonda de temperatura está defectuosa. De manera similar, un controlador de válvula digital puede indicar cuando hay una pérdida de presión en el suministro de aire, o incremento en la fricción del vástago que podría impedir que la válvula se mueva adecuadamente cuando se necesita.

2.4.1.2 Comunicaciones digitales

Las comunicaciones HART llevan información agregada proveniente de los dispositivos de campo inteligentes a todo el lazo, en forma de datos digitales superpuestos en el señal normal de 4-20 mA. La información digital puede fluir en ambas direcciones. Un transmisor inteligente no sólo puede enviar su variable de proceso e información de estado al solucionador lógico y aplicación de gestión de activos, sino también puede recibir datos para configuración o calibración.

Aunque los datos HART se pueden usar para predecir e identificar problemas potenciales, no están certificados para usarse como la única fuente de información para decisiones relacionadas con la seguridad.

2.4.1.3 Solucionadores lógicos inteligentes

Los solucionadores lógicos de un SIS inteligente han sido diseñados específicamente para aprovechar la información agregada disponible de los sensores y controladores de válvula inteligentes del sistema. Por ejemplo, un SIS inteligente reconoce cuando una entrada es mala o incluso cuando es dudosa. El solucionador lógico evalúa la información y, dependiendo de cómo se configure para cada conjunto de circunstancias, su respuesta puede ser:

- Enviar una alarma al personal de operación o de mantenimiento.
- Desviar la medición incorrecta y usar datos de otro dispositivo en un conjunto redundante hasta que se pueda revisar el primero, o
- Disparar la función de seguridad

2.4.1.4 Software de gestión de activos

El software de gestión de activos documenta, archiva y procesa datos acerca de los dispositivos de campo de un
SIS inteligente.

Mientras que el solucionador lógico usa información de estado de los dispositivos, el software de gestión de activos proporciona una base de datos central y permite ver la condición de la información acerca de los sensores y elementos finales de control, incluyendo las configuraciones y cambios en los instrumentos, la condición de la información y las alarmas. También analiza el equipo y los datos de diagnóstico para identificar problemas y proporcionar una guía para corregirlos.

Se puede tener acceso a la información del software donde se necesite, desde las estaciones de operador hasta las oficinas de ingeniería. Sin embargo, generalmente se usa en el taller de mantenimiento, donde sus herramientas de análisis e informes proporcionan una sola aplicación para diagnósticos predictivos, documentación, gestión de calibración y configuración de dispositivos.

2.4.1.5 Solución de lazo completo

La posibilidad de reunir, interpretar y usar información acerca de la condición de todo el lazo también permite una vista más amplia del estado y confiabilidad del SIS de lo que se puede lograr con las soluciones tradicionales.

El solucionador lógico del SIS inteligente no sólo sabe si está funcionando correctamente, sino también sabe si los dispositivos de campo están haciendo lo mismo, es decir, que sabe si puede usar la información de los sensores para tomar decisiones de seguridad, y si los elementos finales de control responderán si se necesita.

Eso es especialmente importante considerando que el 90% de los problemas que afectan a la operación de un SIS se relacionan con los dispositivos de campo. En otras palabras, con un SIS inteligente se sabe qué está pasando en el enlace más débil del lazo de seguridad (generalmente con suficiente advertencia para que tome una acción correctiva antes de que la fiabilidad del sistema sea afectada). Y eso nos lleva a una mayor disponibilidad del SIS.

2.5 Tendencias de los SIS

Debido a que los fabricantes adquieren mayores conocimientos sobre los temas de seguridad, se están realizando análisis de peligros y riesgos más exhaustivos para determinar sus necesidades con más precisión. Ellos buscan la reducción del riesgo, aumentando su enfoque en la seguridad global haciendo que su SIS satisfaga sus necesidades de una manera más rentable mediante una mayor integración de la seguridad con los sistemas de control. También buscan una arquitectura flexible con más escalabilidad; una mayor funcionalidad para modificar alarmas basadas en condiciones del proceso y ordenados procedimientos de apagado en caso de emergencia.

2.5.1 Integración con el sistema de control

Muchas empresas de manufactura tienen controladores orientados para seguridad independientemente separados de aquellos utilizados para control y optimización. Los controladores utilizados para SIS vienen de fabricantes especializados quienes aportan amplios diagnósticos y reciben certificación de seguridad. En el pasado no hubo más remedio que utilizar diferentes sistemas para control y seguridad, algunos usuarios incluso implementaban dichos sistemas considerando diferentes fabricantes.

Hay muchas otras razones para separar las funciones de seguridad y las de control, por ejemplo:

- **Fallas independientes.-** Minimizar el riesgo de fallas simultáneas de un sistema de control conjuntamente con el SIS.

- **Seguridad.-** Prevenir cambios en el sistema de control causando algún otro cambio en el SIS asociado.

- **Diferentes requerimientos para controladores de seguridad.-** Un sistema de seguridad está normalmente diseñado para fallar en una forma segura, mientras que un BPCS usualmente maximizará la disponibilidad. Un SIS también tiene características especiales como diagnóstico extendido, software especial para la revisión de errores, almacenamiento de datos y tolerancia a fallas.

La norma de seguridad IEC 61508 es algo ambigua en este asunto; recomienda estrictamente la separación de los sistemas pero no lo demanda. Hoy, un gran número de usuarios están buscando razones lógicas para utilizar sistemas similares para control y seguridad, como esto reducirá problemas asociados con diferentes procedimientos de programación, lenguajes, requerimientos de instalación y mantenimiento. Siempre existe el riesgo asociado con diferentes procedimientos, contribuyendo al error humano y posibles problemas de seguridad. Los beneficios económicos de utilizar sistemas similares también son claros, los costos de hardware reducido, configuración y entrenamiento son el resultado de reducir el equipo requerido. Además se elimina el problema de diferentes servicios y soporte de ayuda asociado al retiro de sistemas independientes.

Algunos proveedores de sistemas de control y SIS ahora ofrecen sistemas similares para cualquiera de las funciones que incorporan interfaces humano-máquina (*Human Machine Interface*, HMI), procedimientos de configuración, lenguajes de programación y procedimientos de mantenimiento semejantes. Se debe asegurar que a pesar de que los dos sistemas están separados, con hardware y software diferentes, tienen una configuración, operaciones e interfaz de mantenimiento comunes. Esto permite a los usuarios alcanzar los beneficios operacionales de integración mientras satisfacen los requisitos de seguridad por separado. Los sistemas de control y seguridad se comunican de forma transparente entre sí, pero tienen una protección adecuada contra la corrupción del uno debido al otro.

Algunos beneficios de integrar el sistema de seguridad y el sistema de control son:

- Asignación de datos comunes
- Mayor seguridad
- Herramientas de ingeniería similares
- Diferencia visual entre los entornos de control y seguridad a nivel de estación de trabajo

- Protección de acceso adecuada
- Reducción significativa en esfuerzos de integración.

Las fallas de causa común son responsables de muchos paros en la producción debido a que, una falla originada en un sensor defectuoso puede afectar a otro en buen estado, esto genera molestias en el proceso. Otro tipo de fallas que también afectan a la producción son las causadas por activaciones esporádicas, esto se debe principalmente a la falta de mantenimientos de los sensores y elementos finales presentes en el sistema.

Las pruebas de cierre parcial de válvulas son una herramienta muy importante para el diagnóstico del correcto funcionamiento de dichos elementos. Al realizar PST se puede determinar si el elemento analizado está en buenas condiciones, lo que asegura su funcionamiento bajo demanda, de no ser así, esto puede resultar en situaciones de alto riesgo.

La tecnología de la que disponen los SIS hoy en día es muy variada, es decir, dichos sistemas constan de elementos eléctricos, neumáticos e hidráulicos, lo que proporciona una gran variedad de dispositivos que se pueden utilizar. Esto ha impulsado el crecimiento de nuevas técnicas e instrumentos en el desarrollo de SIS.

Capítulo 3

NECESIDAD DE SIS EN LA INDUSTRIA DE PROCESOS DE CUENCA.

3.1 Diagnóstico de la aplicación de la seguridad funcional en la industria de procesos.

Para recopilar información sobre la seguridad funcional que se maneja en algunas industrias, se aplicó una encuesta en diferentes áreas (operaciones, jefaturas, supervisión, técnica y gerencia) en algunas de las industrias más importantes de la ciudad debido a su volumen de producción, procesos industriales, infraestructura y ubicación geográfica para evidenciar mediante cifras accidentes relacionados con la seguridad funcional que no son registrados o considerados.

El universo de análisis estuvo conformado por diez empresas (46 empleados encuestados) dentro de las cuales se pudo observar los procesos llevados a cabo en cada una de ellas. Cabe recalcar que en todas estas industrias la seguridad ocupacional es una de sus prioridades fundamentales debido a que, proporcionar un ambiente seguro de trabajo al personal, es parte de su política.

Los resultados obtenidos del estudio realizado se muestran a continuación:

1. Cargo desempeñado en la organización.

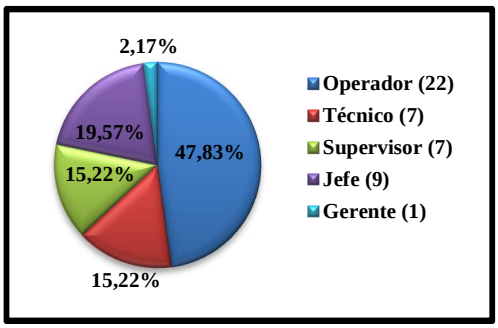


Figura 3.1.1: *Personal encuestado.*

Del personal laboral encuestado se logró tener acceso a personal de planta, técnico, jefes de mantenimiento, supervisores y en especial al gerente de una de las empresas. Se consideró recopilar información de empleados de diferentes áreas para constatar las diversas reacciones referentes a la seguridad funcional, no se obtuvo mucha aceptación a la encuesta por parte del personal de las áreas administrativas, por ello se consideró realizar la mayor cantidad de entrevistas al personal de planta.

2. Áreas de trabajo.

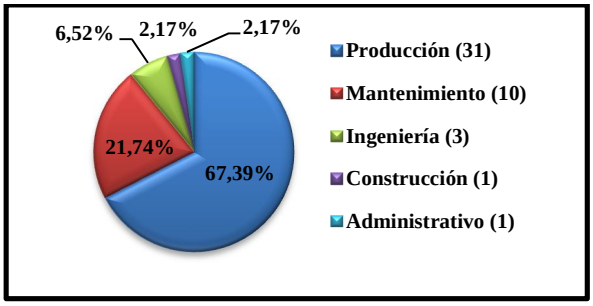


Figura 3.1.2: *Áreas de trabajo.*

La información más relevante fue obtenida de las áreas más dinámicas al interior de una planta, tal es el caso de mantenimiento y producción. Estas son dos de las áreas más involucradas con la seguridad funcional debido a su interacción directa con la maquinaria.

3. Cantidad de líneas de producción.

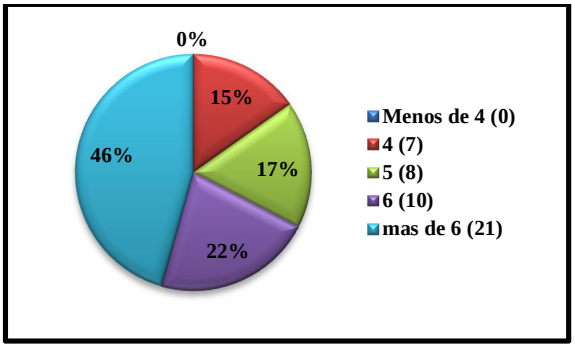


Figura 3.1.3: *Líneas de producción.*

Las empresas de las que se obtuvo la información recopilada tienen en promedio seis líneas de producción. Cabe recalcar que aunque unas tienen más líneas de producción que otras, los procesos llevados a cabo son más riesgosos que otros debido al uso de ciertos químicos o materiales inflamables.

4. Cantidad total de líneas de producción automatizadas en las industrias analizadas.

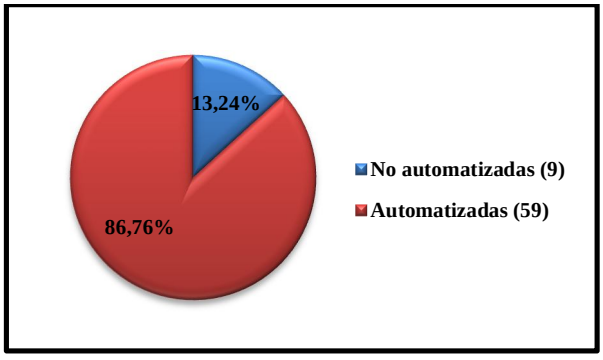


Figura 3.1.4: *Líneas de producción automatizadas.*

A pesar de haber recopilado información de diez empresas, sumando en total 68 líneas de producción, fue muy interesante observar que 59 de las mismas estaban automatizadas. Esto permite demostrar que la automatización de procesos en la industria de Cuenca es un área en la que aún hay muchos avances que hacer, ya que esto implica que algunos procesos todavía se tengan que seguir realizando manualmente, lo que eleva el riesgo en el trabajo para el personal de planta.

5. Procesos de mayor riesgo para la maquinaria y el personal dentro de las instalaciones.

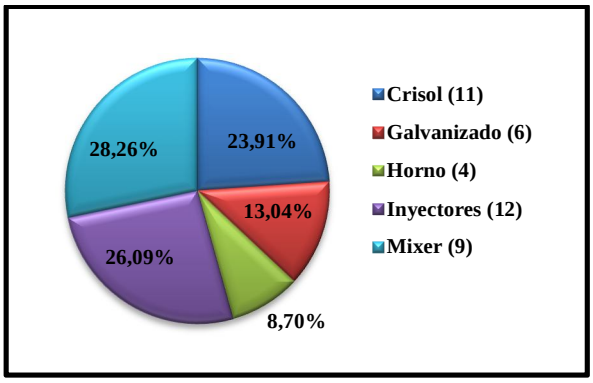


Figura 3.1.5: *Líneas de mayor riesgo.*

Ya que las industrias de análisis están relacionadas con la producción de cerámica, material metálico y químico, las áreas de mayor riesgo para el personal son aquellas en las que se procesa la materia prima principalmente por las elevadas temperaturas que en esas áreas se maneja.

6. Presencia de sistemas de seguridad en las industrias analizadas.

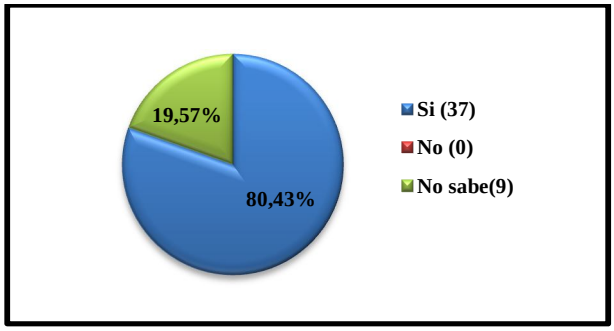


Figura 3.1.6: *Presencia de sistemas de seguridad.*

El personal encuestado tenía conocimientos de la utilización de aspersores en caso de incendios y algunas señales luminosas para alertar al personal de la ocurrencia de algún evento, mientras que un reducido grupo del mismo no tenía conocimiento de la existencia de dichos sistemas o de ciertos recursos para el caso de emergencias.

7. Cantidad de sistemas de seguridad automatizados.

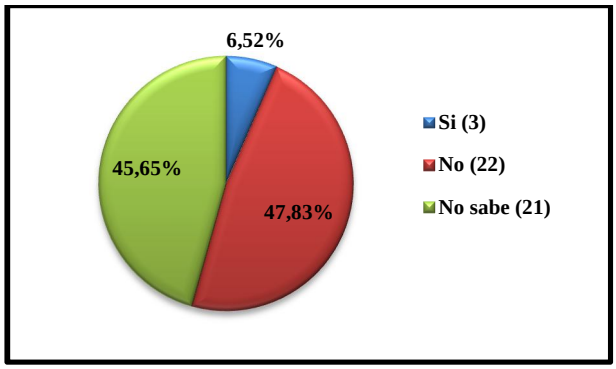


Figura 3.1.7: *Sistemas automatizados.*

El nivel de automatización de una empresa con respecto a otra difiere en algunos aspectos, entre ellos la forma de activación del sistema de seguridad, mientras en unas pocas se utiliza sensores, en la mayoría de ellas un pulsante de pánico tiene que ser accionado.

El hecho de utilizar un pulsante hace que el sistema dependa del factor humano para su desempeño. Esto afecta significativamente al sistema cuando ocurra un evento peligroso.

8. Tipos de accionamiento utilizado para sistemas de seguridad.

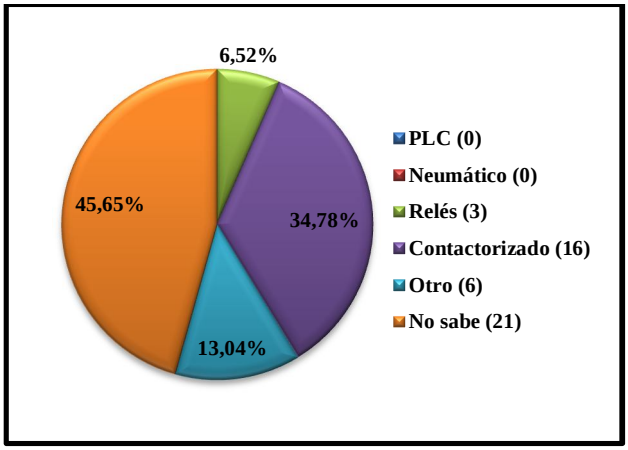


Figura 3.1.8: *Tipos de sistemas de seguridad.*

El sistema más utilizado es el basado en lógica de contactores, debido a su robustez y su amplio uso en procesos industriales. Otro grupo también muy utilizado es el basado en relés, aunque no en igual proporción que los sistemas contactorizados. Esto demuestra que la preferencia por los sistemas eléctricos es considerable sobre otro tipo de sistemas como el neumático.

9. Tipos de sensores utilizados en el sistema de seguridad.

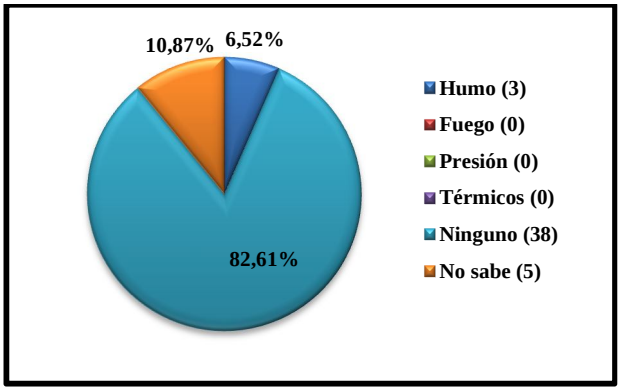


Figura 3.1.9: *Tipos de sensores utilizados.*

En muchas de las empresas analizadas no se utilizan sensores para detectar eventos peligrosos, en su lugar, el factor humano es el principal dispositivo para dicha tarea.

10. Cantidad de personas que conocen de PLC's orientados a seguridad.

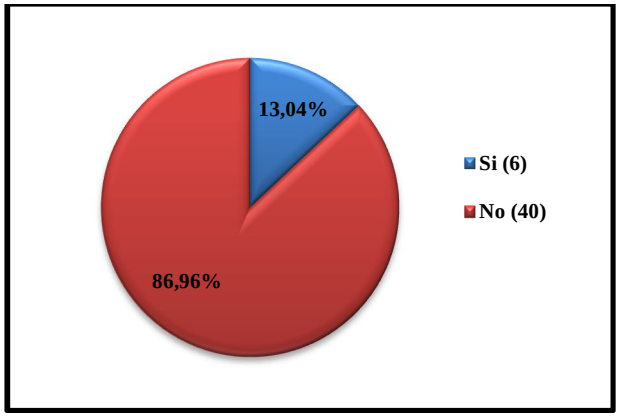


Figura 3.1.10: *PLC's orientados a seguridad.*

Como se muestra en la gráfica anterior, un elevado porcentaje del personal encuestado no tiene conocimiento acerca de los PLC's de seguridad. Esto fue común en todas las plantas ya que el PLC ha sido utilizado ampliamente con fines de automatización de procesos pero no ha sido considerado para proveer seguridad a dichos procesos.

11. Conocimiento sobre la realización de análisis de riesgos de los procesos industriales.

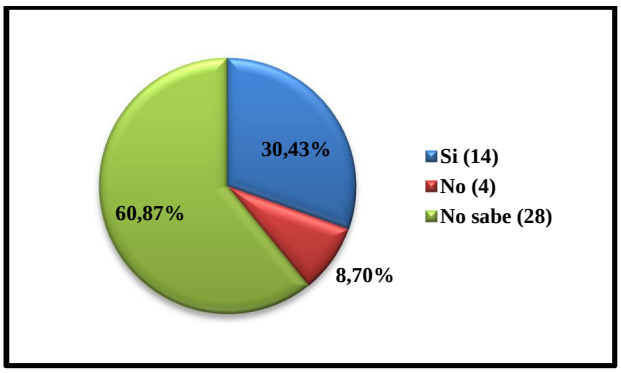


Figura 3.1.11: *Realización de análisis de riesgo.*

La mayoría del personal encuestado no sabía si se ha realizado un análisis de riesgo en los procesos desarrollados. Algunos de estos procesos llevan años de ejecución con la misma maquinaria con la que iniciaron hace años y hasta la actualidad no han sido analizados.

12. Realización de análisis de identificación de peligros de seguridad y operativos.

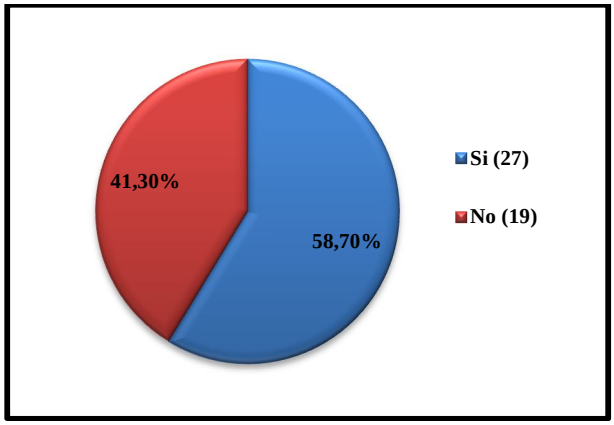


Figura 3.1.12: *Realización de análisis cuantitativo.*

La identificación de peligros ha contribuido a determinar las zonas de mayor riesgo dentro de las industrias, por medio de dicho análisis las empresas han podido desarrollar procedimientos de respuesta ante eventos inesperados, así mismo ha impulsado al personal encargado de la seguridad a realizar constantes mejoras en sus sistemas para garantizar un ambiente seguro de trabajo.

13. Monto anual gastado en mantenimiento de sistemas de seguridad.

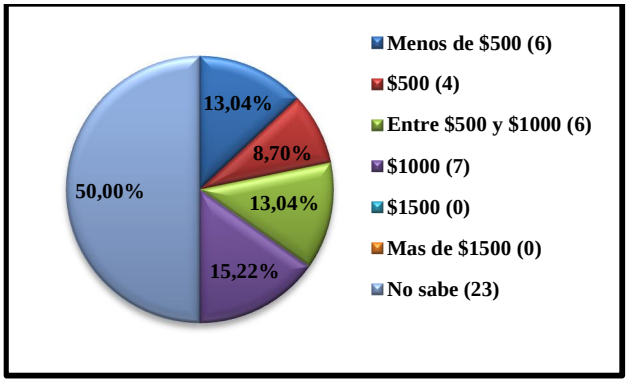


Figura 3.1.13: *Gastos en mantenimiento anual de sistema de seguridad.*

Ya que la minoría de las encuestas corresponde a personal administrativo, no se obtuvo un dato concreto acerca del gasto realizado anualmente por cada empresa en sus sistemas de seguridad. El valor promedio está comprendido entre los $500 y $1000, pero dichas cantidades son gastadas principalmente en el reemplazo de partes y componentes pero no en su mejora.

14. Conocimientos sobre la ocurrencia de accidentes que involucraron la vida del personal.

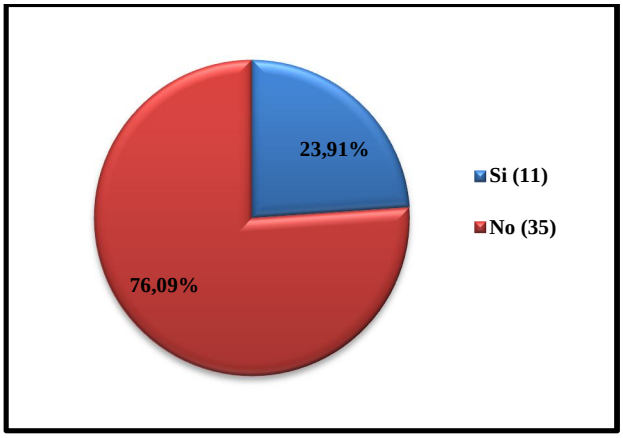


Figura 3.1.14: *Accidentes graves que involucraron la vida de operadores.*

Este fue un tema muy delicado de tratar dentro de cada empresa ya que en ninguna de ellas se dio mucha apertura hacia el tema. Un reducido porcentaje afirmó que en algunos accidentes cobraron la vida de empleados, principalmente operadores.

15. Cantidad de accidentes graves ocurridos en un período de un año.

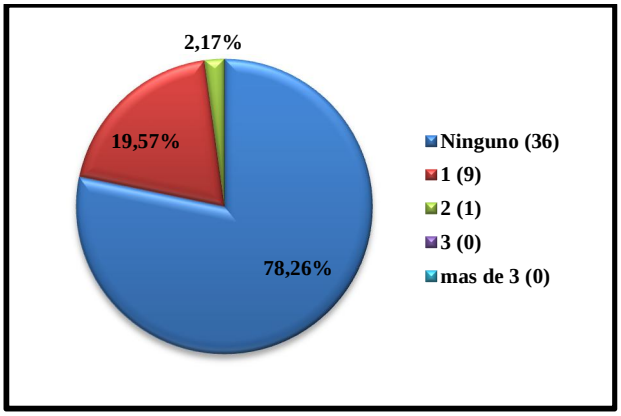


Figura 3.1.15: *Accidentes suscitados durante un año.*

En promedio se ha registrado al menos un accidente grave dentro de cada planta principalmente por errores humanos, ya sea por descuido o por mala operación de la maquinaria. La mayoría de accidentes graves han tenido lugar durante el turno vespertino en donde el personal fácilmente experimenta un estado de somnolencia.

16. Cantidad de personas que tienen conocimientos sobre seguridad funcional.

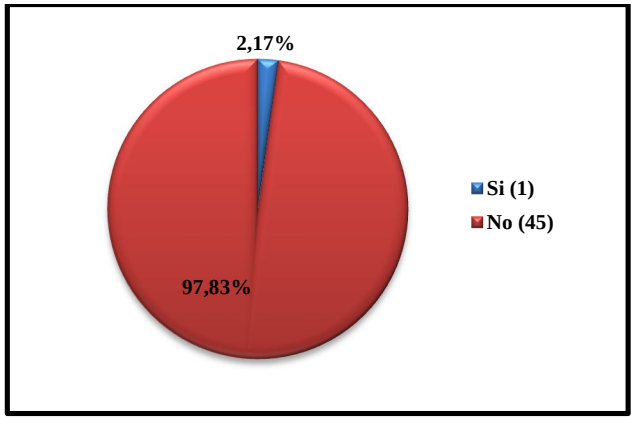


Figura 3.1.16: *Conocimientos sobre seguridad funcional.*

La respuesta afirmativa a esta pregunta únicamente la dio una persona del área de seguridad, todas las demás personas no han escuchado acerca de la seguridad funcional aplicada a procesos. Esto evidencia que la seguridad funcional es un tema totalmente nuevo en el área de la industria de procesos.

17. Cantidad de personas que tienen conocimientos sobre SIS.

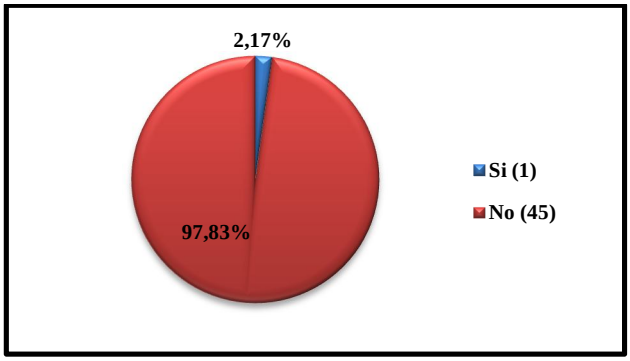


Figura 3.1.17: *Conocimientos sobre SIS.*

Así como la seguridad funcional, los SIS también son desconocidos para el personal encuestado, por ello es un área que puede ser explotada en la industria de procesos por los beneficios que traería a la misma.

18. Dispositivos disponibles para seguridad funcional.

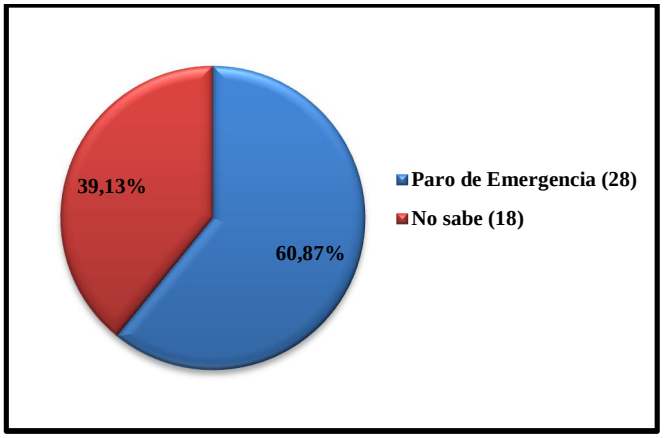


Figura 3.1.18: *Dispositivos de seguridad funcional.*

En muchas de las empresas, el personal que tiene más conocimiento de la maquinaria está familiarizado con los recursos que dispone de la misma, por ello el pulsante de paro/emergencia fue el más destacado entre el personal. Dicho dispositivo no puede ser considerado como uno de seguridad ya que no es un sensor y no es útil para desempeñar acciones automáticas.

19. Normativas de seguridad funcional utilizadas por las empresas.

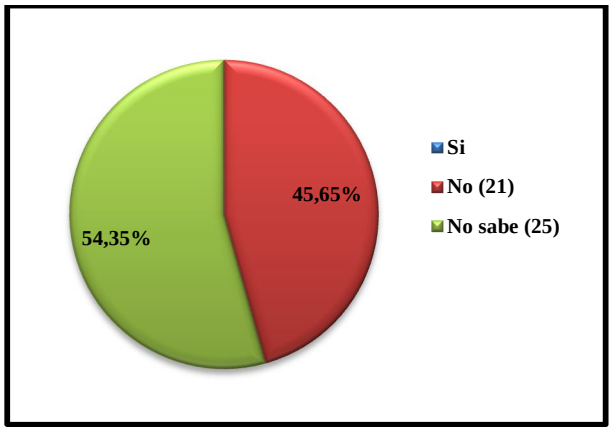


Figura 3.1.19: *Manejo de normativas de seguridad.*

En ninguna de las empresas analizadas se manejan normativas de seguridad funcional, sin embargo, algunas personas respondieron que la normativa que utilizaban era la OHSAS 18001 (Sistemas de Gestión de Salud y Seguridad Laboral), pero dicha norma no hace referencia a seguridad funcional sino a seguridad ocupacional.

20. Interés en la aplicación de SIS en las instalaciones.

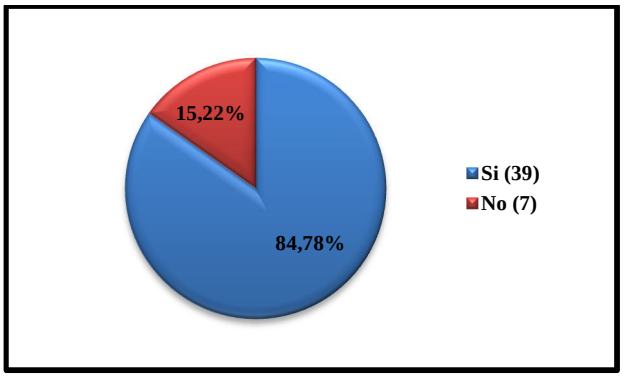


Figura 3.1.20: *Interés en la aplicación de SIS en las instalaciones.*

Se apreció gran apertura a la aplicación de SIS en las instalaciones por parte del personal de planta, por otro lado, el personal administrativo se mostró negativo. La principal razón para no disponer del SIS fue “hasta el momento no hemos necesitado de un SIS y sería muy costoso”, esto demuestra que al tratarse de un nuevo tema no se analizan primero sus beneficios sino su costo.

21. Aceptación del personal a la aplicación de SIS en las instalaciones.

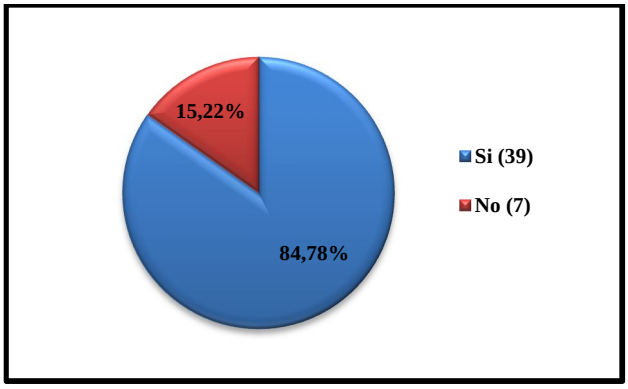


Figura 3.1.21: *Incremento de seguridad en entorno laboral.*

El personal que labora en planta mostró estar de acuerdo en disponer de un entorno de trabajo seguro, principalmente en aquellos procesos que conllevan peligros constantes tanto para ellos como para el resto del personal. Como en preguntas anteriores, hubo un grupo reducido de personas que consideran que el ambiente de trabajo del que disponen actualmente es lo suficientemente seguro y que la aplicación de un SIS no sería necesaria.

22. Consideración de la seguridad funcional para la realización de automatizaciones.

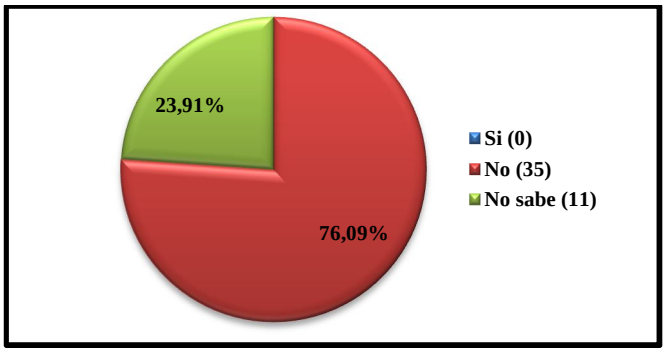


Figura 3.1.22: *Consideración de seguridad funcional.*

Se puede notar que en la mayoría de las plantas analizadas, realizaron automatizaciones a sus líneas de producción considerando únicamente factores de producción y seguridad ocupacional, mas no de seguridad funcional.

23. Combustibles utilizados por las industrias.

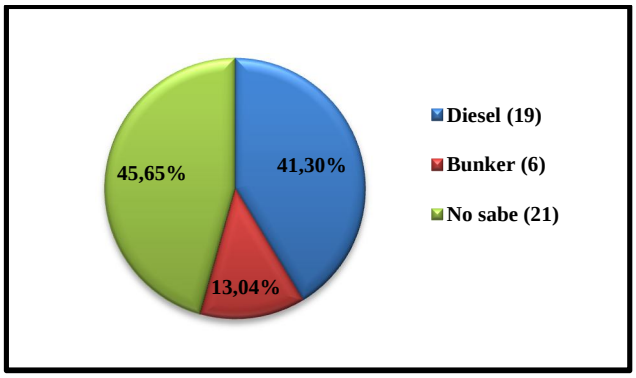


Figura 3.1.23: *Combustibles o solventes utilizados.*

La utilización de diésel y de bunker (en menor cantidad) en la mayoría de las empresas analizadas, demuestra que están expuestas a eventos inesperados como incendios, derrame de combustible e incluso la explosión de un tanque de almacenamiento.

24. Capas de seguridad aplicadas al área de almacenamiento de combustibles.

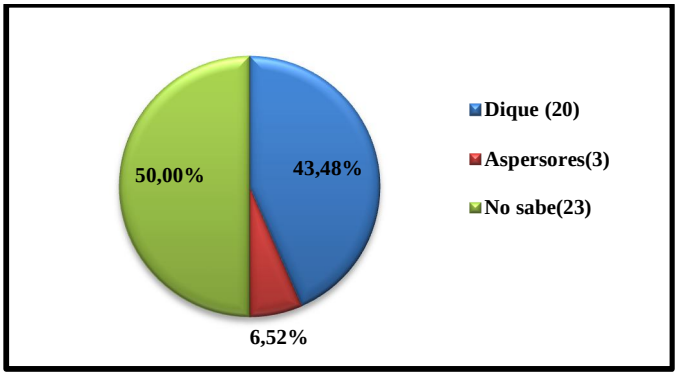


Figura 3.1.24: *Seguridad en área de almacenamiento de combustibles.*

El dispositivo de seguridad más común es el dique de contención, ya que se han presentado algunos derrames de combustibles o químicos en algunas industrias y este medio de mitigación ha cumplido satisfactoriamente su cometido. En menor cantidad se encuentran los aspersores como recurso inmediato en el caso de presencia de fuego en el área de almacenamiento de combustibles.

Los resultados de las encuestas realizadas pueden ser analizados de manera más detallada, es decir, se puede obtener la desviación estándar y la moda de las respuestas obtenidas para determinar cuál es la respuesta esperada del personal al tratar el tema de la seguridad funcional. Mediante un gráfico de barras se puede apreciar de una mejor manera, para ello se han considerado únicamente las respuestas afirmativas (figuras 3.1.25 y 3.1.26).

ANALISIS DE UNIFORMIDAD DE LAS REPUESTAS	A. SI	B. NO	C. NO SABE	TOTAL	MODA	% DE DESVIACION
1. ¿DISPONE DE ALGÚN SISTEMA DE SEGURIDAD EN SUS INSTALACIONES?	37	0	9	46	SI	3,97%
	0,80	0,00	0,20	%		
2. ¿SU SISTEMA DE SEGURIDAD ESTÁ AUTOMATIZADO?	3	22	21	46	NO	2,47%
	0,07	0,48	0,46	%		
3. ¿CONOCE O HA ESCUCHADO UD. ACERCA DE PLC's ORIENTADOS A SEGURIDAD?	6	40	0	46	NO	3,37%
	0,13	0,87	0,00	%		
4. ¿EN SUS INSTALACIONES SE HA REALIZADO UN ANÁLISIS DE RIESGO CON RESPECTO A LOS PROCESOS INDUSTRIALES LLEVADOS A CABO?	14	4	28	46	SI	4,60%
	0,30	0,09	0,61	%		
5. ¿HA REALIZADO UN ANÁLISIS CUANTITATIVO O DE IDENTIFICACIÓN DE PELIGROS DE SEGURIDAD Y OPERATIVOS?	27	19	0	46	SI	4,92%
	0,59	0,41	0,00	%		
6. ¿SE HAN PRODUCIDO ACCIDENTES GRAVES QUE HAYAN INVOLUCRADO LA VIDA DE OPERADORES DE LA PLANTA?	11	35	0	46	NO	4,27%
	0,24	0,76	0,00	%		
7. ¿HA ESCUCHADO O TIENE CONOCIMIENTOS ACERCA DE SEGURIDAD FUNCIONAL?	1	45	0	46	NO	1,46%
	0,02	0,98	0,00	%		
8. ¿HA ESCUCHADO SOBRE SISTEMAS INSTRUMENTADOS DE SEGURIDAD (SIS)?	1	45	0	46	NO	1,46%
	0,02	0,98	0,00	%		
9. ¿EN SUS INSTALACIONES SE MANEJAN NORMATIVAS DE SEGURIDAD FUNCIONAL?	0	21	25	46	NO SABE	0,00%
	0,00	0,46	0,54	%		
10. ¿ESTARÍA INTERESADO EN LA APLICACIÓN DE UN SIS EN SUS INSTALACIONES?	39	7	0	46	SI	3,59%
	0,85	0,15	0,00	%		
11. ¿PIENSA UD. QUE LA APLICACIÓN DE UN SIS EN LAS INSTALACIONES ASEGURARÍA UN ENTORNO DE TRABAJO MAS CONFIABLE PARA EL PERSONAL?	39	7	0	46	SI	3,59%
	0,85	0,15	0,00	%		
12. ¿EN LAS AUTOMATIZACIONES REALIZADAS EN LAS INSTALACIONES SE CONSIDERÓ LA SEGURIDAD FUNCIONAL PARA CADA UNA DE ELLAS?	0	35	11	46	NO	0,00%
	0,00	0,76	0,24	%		
					% PROMEDIO	2,81%

Figura 3.1.25: *Desviación estándar de datos obtenidos.*

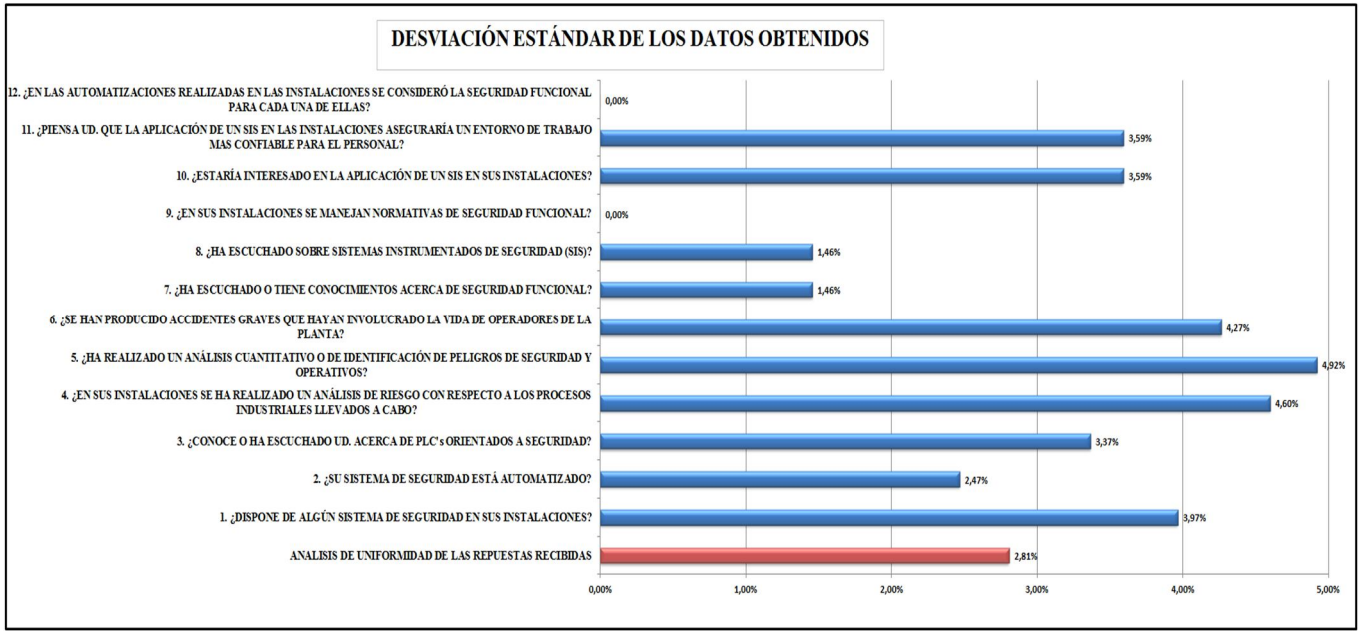


Figura 3.1.26: *Certeza de los datos obtenidos.*

De los resultados obtenidos se observa que pocas o ninguna de las personas encuestadas han escuchado o tienen conocimiento sobre seguridad funcional o de sus normativas, principalmente en las áreas de seguridad y de mantenimiento, siendo esta última la que constantemente monitorea el estado de la maquinaria para su correcto funcionamiento.

A pesar de que la mayoría de líneas de producción están automatizadas, la seguridad funcional en dichas líneas no ha sido considerada, dejando abierta la posibilidad de que pueda producirse un evento peligroso evitando alcanzar el desarrollo sostenible.

Al informar sobre los SIS al personal de planta, se obtuvieron diversas reacciones, mientras unos se mostraron interesados otros se mantuvieron escépticos ya que consideraban innecesaria la implementación de un sistema de este tipo alegando que hasta el momento no ha sido necesario dicho sistema para cumplir con la producción y proporcionar seguridad al personal.

En muchas de las industrias analizadas, consideran como un dispositivo de seguridad funcional al pulsante de paro general o de apagado; en casos de emergencia es el único instrumento del que dispone el personal para detener la maquinaria y evitar cualquier situación de riesgo, esto evidencia la falta de conocimiento sobre modernos dispositivos orientados a seguridad de los que se dispone en el mercado.

Un factor común en las empresas de análisis es la utilización de combustibles como diésel y búnker para la maquinaria, los mismos que son almacenados en tanques de gran capacidad. La capa de mitigación comúnmente utilizada para estos tanques son los diques, algunos de los cuales ya han cumplido su función exitosamente debido a derrames producidos en ciertos casos por fallas en el sistema de control de bombas de llenado o por factores humanos.

3.2 Accidentes graves registrados en las industrias de análisis en la ciudad de Cuenca.

De la mayoría de accidentes registrados en las industrias de procesos, son pocos los que están relacionados con la seguridad funcional, es decir, no son considerados o simplemente no son registrados. Esto evidencia que la seguridad ocupacional es una prioridad para todas las empresas pero no de igual manera la seguridad funcional.

La información recopilada para este análisis fue tomada de un universo de estudio correspondiente a las cuatro fábricas más significativas de la ciudad de Cuenca y en las cuales se registra la mayor tasa de accidentes laborales anuales.

- **Empresa A:** Es una empresa que se dedica a la fabricación de tubería, perfiles y paneles metálicos. Dispone de un área de almacenamiento de combustibles de 100.000 galones de diésel y 50.000 galones de bunker. Todas sus líneas de producción están automatizadas y en ellas laboran 94 personas en dos turnos de seis horas durante seis días a la semana.

- **Empresa B:** Empresa dedicada a la fabricación de cerámica y porcelanato, dispone de 540 empleados que trabajan en tres turnos de ocho horas los siete días de la semana. La temperatura que alcanzan los hornos de cocción alcanza los 1200 °C, el combustible utilizado en el horno es bombeado desde el área de combustibles de la empresa A y almacenado en un tanque secundario de 1000 galones.

- **Empresa C:** Está dedicada a la fabricación de piezas y partes metálicas, el quemador aquí instalado alcanza 900 °C de temperatura. Su personal consta de 87 personas que trabajan en dos turnos de seis horas durante seis días a la semana. Al igual que la empresa B, el combustible necesario para el quemador es bombeado desde el área de combustibles de la empresa A hacia un tanque de almacenamiento secundario de 1000 galones.

Las empresas A, B y C se encuentran ocupando un área común de 11 hectáreas y totalizan 721 empleados puesto que pertenecen al mismo grupo empresarial.

- **Empresa D:** Se dedica a la fabricación de pinturas, adhesivos y solventes. Comprende una extensión de 39690 metros cuadrados, aquí están alojados tres tanques de almacenamiento de 500 galones de químicos como rubber, mek y tolueno. Las líneas de producción están parcialmente automatizadas ya que aún es necesaria la intervención del operador en algunos procesos. El personal laboral consta de 47 personas que trabajan en dos turnos de 12 horas los 7 días de la semana.

Durante el período del 2007 hasta el 2012 se registraron en promedio 24 accidentes laborales por año, uno o dos estaban relacionados con seguridad funcional; los demás comprendían casos de quemaduras, cortes y caídas.

Los datos obtenidos se muestran en las figuras a continuación:

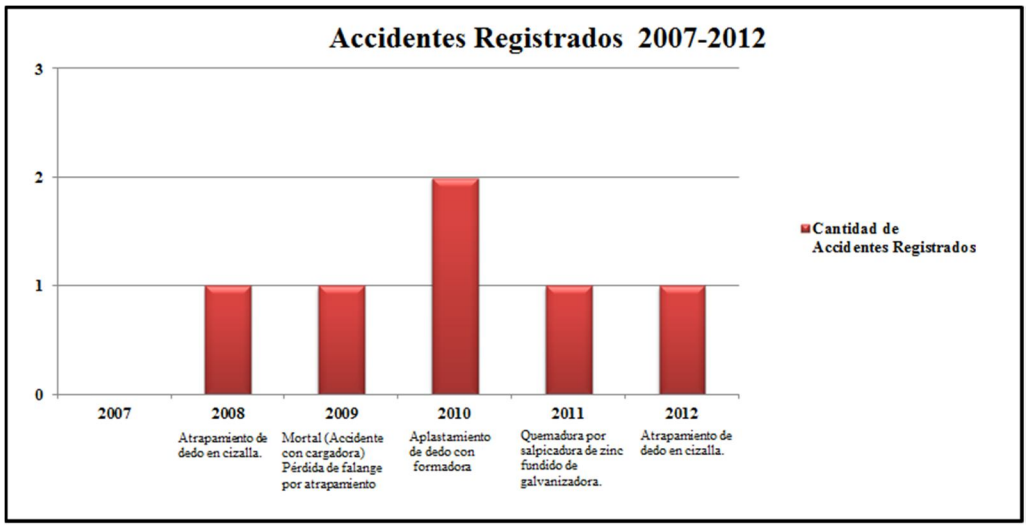


Figura 3.2.1: *Empresa A*

Figura 3.2.2: *Empresa B*

Figura 3.2.3: *Empresa C*

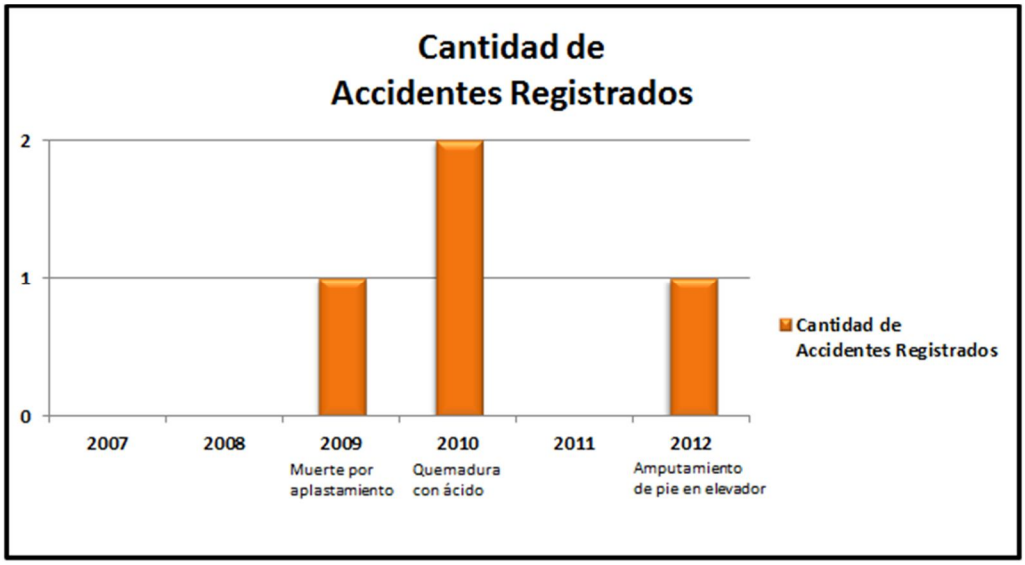


Figura 3.2.4: *Empresa D*

Como se observa, la cantidad de accidentes funcionales registrados es muy baja comparada con los accidentes ocupacionales. Incluso si consideramos el área física de las instalaciones, es fácil notar que muchos de los accidentes que se suscitan no son considerados dentro de los registros. Es por ello que es necesario implementar la seguridad funcional en las industrias para poder garantizar el bienestar y seguridad tanto de personal como de la maquinaria involucrada, de esta manera se podrá alcanzar el desarrollo sustentable deseado.

Si bien el personal que labora en las instalaciones ha sido capacitado en procedimientos de evacuación y de acción ante eventos inesperados, no saben cómo proceder ante eventos que relacionan el estado de la maquinaria, como por ejemplo, el derrame de un químico, exceso de presión en un tanque de almacenamiento o temperatura excesiva en un caldero. Esto da oportunidad a que un pequeño evento pueda convertirse en una catástrofe de proporciones considerables, más aún cuando el evento implica combustibles.

El operador humano representa también el elemento más vulnerable del sistema y el que más fácilmente se pasa por alto. Conocer y optimizar el funcionamiento global de los sistemas de control de los procesos industriales depende de un planteamiento sistemático, que se ocupe tanto del rápido desarrollo de la tecnología como del papel esencial del operador humano.

La seguridad funcional debería formar parte de la cultura industrial ya que disponer de sistemas que se encarguen de llevar el proceso a un estado seguro en situaciones de riesgo contribuiría significativamente a reducir la tasa de accidentes.

De todas las industrias analizadas, ninguna dispone de un SIS en sus instalaciones. Se han enfocado en la implementación de sistemas contra incendios en los sectores de almacenamiento de combustibles, pero en las líneas de proceso no hay sistema alguno de seguridad siendo aquí en donde se presenta la mayor cantidad de accidentes.

La muerte de un empleado es algo con lo que las industrias no quieren lidiar, es por ello que este estudio busca demostrar el beneficio que representa la implementación de SIS en sus procesos. La implementación de un SIS puede considerarse costosa, pero en muchos casos es más costoso prescindir de él que disponer de él.

3.3 Tasa de Accidentabilidad.

Es necesario obtener una referencia sobre la cantidad de accidentes anuales acontecidos en las instalaciones. Para ello, se debe recopilar y analizar la información de dichos accidentes para, de esta manera, poder determinar en cifras la cantidad de eventos registrados que están relacionados con la seguridad funcional. Se deben determinar tres parámetros muy importantes con la información obtenida, la tasa de riesgo, el índice de frecuencia y el índice de gravedad.

La tasa de accidentabilidad o tasa de riesgo (TR) representa el índice de ocurrencia de accidentes laborales. Por ejemplo, en una fábrica la tasa de accidentabilidad fue de 3% en el mes de junio, considerando que existen 100 trabajadores en dicha fábrica, esto se interpretaría de la siguiente manera: De 100 empleados 3 se accidentaron en ese mes. De esta manera se puede obtener dicha información para cada mes siguiente y así poder comprobar si este indicador subió o bajó para tomar las medidas pertinentes o mantener las ya existentes. Otros indicadores importantes son el índice de frecuencia (IF) y el índice de gravedad (IG).

- Índice de Frecuencia:

$$IF = \frac{\#\ lesiones\ x\ 100000}{\#\ horas\ hombre} \qquad (3.3.1)$$

  Representa el número de accidentes acaecidos durante la jornada de trabajo por cada millón de horas trabajadas por los trabajadores expuestos al riesgo.

- Índice de Gravedad:

$$IG = \frac{\#\ días\ perdidos\ x\ 100000}{\#\ horas\ hombre} \qquad (3.3.2)$$

  Relaciona la gravedad de las lesiones con el tiempo de trabajo perdido. Además de los días perdidos ya descritos en la fórmula, también deben considerarse los días de cargo correspondientes al tipo de lesión. Esto se muestra en la figura 3.3.1.

NATURALEZA DE LA LESION	JORNADAS DE TRABAJO PERDIDAS
Muerte	6000
Incapacidad permanente absoluta	6000
Incapacidad permanente total	4500
Pérdida del brazo por encima del codo	4500
Pérdida del brazo por el codo o debajo	3600
Pérdida de la mano	3000
Pérdida o invalidez permanente del pulgar	600
Pérdida o invalidez permanente de un dedo cualquiera	300
Pérdida o invalidez permanente de 2 dedos	750
Pérdida o invalidez permanente de 3 dedos	1200
Pérdida o invalidez permanente de 4 dedos	1800
Pérdida o invalidez permanente pulgar y un dedo	1200
Pérdida o invalidez permanente pulgar y dos dedos	1500
Pérdida o invalidez permanente pulgar y tres dedos	2000
Pérdida o invalidez permanente pulgar y cuatro dedos	2400
Pérdida de una pierna por encima de la rodilla	4500
Pérdida de una pierna por la rodilla o debajo	3000
Pérdida del pié	2400
Pérdida o invalidez permanente de dedo gordo o de 2 o más dedos del pié	300
Pérdida de la vista (un ojo)	1800
Ceguera total	6000
Pérdida de un oído (uno sólo)	600
Sordera total	3000

Figura 3.3.1: *Jornadas perdidas por tipo de lesión.*

- Tasa de Accidentabilidad:

$$TR = \frac{\#\ lesiones\ x\ 100}{\#\ de\ empleados} \qquad (3.3.3)$$

Es el porcentaje de accidentes ocurridos en relación al número de trabajadores de la empresa.

A continuación se calculará la tasa de accidentabilidad para cada empresa de análisis respecto a los accidentes de seguridad tanto ocupacional como funcional dentro del período comprendido desde el año 2007 al 2012, como se muestra a continuación:

EMPRESA A (Seguridad Ocupacional):

Al tratarse de seguridad ocupacional, todos los accidentes aquí registrados son los que se han acontecido en la planta de producción durante un año. Lo primero es determinar la cantidad total de horas hombre trabajadas (HHT) durante un año:

$$HTT = 8 * \#\ de\ turnos * días\ de\ la\ semana\ trabajaos * 50 * \#\ de\ empleados$$

Para la empresa A, se tiene:

$$HHT = 8 * 2 * 6 * 50 * 94 = 451200 \text{ horas al año.}$$

Tanto los días de para como en número de accidentes registrados fueron proporcionados por el personal del área de seguridad de la planta.

	2007	**2008**	**2009**	**2010**	**2011**	**2012**
HHT	451200	451200	451200	451200	451200	451200
Días de para	488	431	165	54	34	45
# de Accidentes	8	4	6	4	3	4

Tabla 3.1: *Datos proporcionados por la empresa A.*

	2007	**2008**	**2009**	**2010**	**2011**	**2012**	**Descripción**
IF	17.73	8.87	13.3	8.87	6.64	8.87	# de accidentes por cada 1000000 horas de trabajo
IG	1081.6	955.2	365.7	119.7	75.4	99.7	# de días de para por cada 1000000 horas de trabajo
TR	8.5%	4.25%	6.38%	4.25%	3.19%	4.25%	% de ocurrencia de accidentes

Tabla 3.2: *Índices de Frecuencia, Gravedad y Accidentabilidad.*

EMPRESA A (Seguridad Funcional):

Son pocos los accidentes registrados relacionados a seguridad funcional, pero se desarrollará el mismo proceso realizado anteriormente. Ya que se trata de la misma fábrica, la cantidad de HHT es la misma.

	2007	2008	2009	2010	2011	2012
HHT	451200	451200	451200	451200	451200	451200
Días de para	0	150	6120	300	205	150
# de Accidentes	0	1	1	2	1	1

Tabla 3.3: *Datos proporcionados por la empresa A.*

	2007	2008	2009	2010	2011	2012	Descripción
IF	17.73	8.87	13.3	8.87	6.64	8.87	# de accidentes por cada 1000000 horas de trabajo
IG	1081.6	955.2	365.7	119.7	75.4	99.7	# de días de para por cada 1000000 horas de trabajo
TR	8.5%	4.25%	6.38%	4.25%	3.19%	4.25%	% de ocurrencia de accidentes

Tabla 3.4: *Índices de Frecuencia, Gravedad y Accidentabilidad.*

EMPRESA B (Seguridad Ocupacional):

Para la empresa B, se tiene:

$$HHT = 8 * 3 * 7 * 50 * 540 = 4536000 \text{ horas al año.}$$

Tanto los días de para como en número de accidentes registrados fueron proporcionados por el personal del área de seguridad de la planta.

	2007	2008	2009	2010	2011	2012
HHT	4536000	4536000	4536000	4536000	4536000	4536000
Días de para	1004	341	388	179	568	111
# de Accidentes	22	12	19	10	12	10

Tabla 3.5: *Datos proporcionados por la empresa B.*

	2007	2008	2009	2010	2011	2012	Descripción
IF	4.85	2.65	4.19	2.20	2.65	2.20	# de accidentes por cada 1000000 horas de trabajo
IG	221.3	75.2	85.5	39.5	125.2	24.5	# de días de para por cada 1000000 horas de trabajo
TR	4.07%	2.22%	3.5%	1.85%	2.22%	1.85%	% de ocurrencia de accidentes

Tabla 3.6: *Índices de Frecuencia, Gravedad y Accidentabilidad.*

EMPRESA B (Seguridad Funcional):

Son pocos los accidentes registrados relacionados a seguridad funcional, pero se desarrollará el mismo proceso realizado anteriormente. Ya que se trata de la misma fábrica, la cantidad de HHT es la misma.

	2007	2008	2009	2010	2011	2012
HHT	4536000	4536000	4536000	4536000	4536000	4536000
Días de para	0	155	0	225	155	0
# de Accidentes	0	1	0	1	1	0

Tabla 3.7: *Datos proporcionados por la empresa B.*

	2007	2008	2009	2010	2011	2012	Descripción
IF	0	0.22	0	0.22	0.22	0	# de accidentes por cada 1000000 horas de trabajo
IG	0	34.2	0	49.6	34.2	0	# de días de para por cada 1000000 horas de trabajo
TR	0	0.18%	0	0.18%	0.18%	0	% de ocurrencia de accidentes

Tabla 3.8: *Índices de Frecuencia, Gravedad y Accidentabilidad.*

EMPRESA C (Seguridad Ocupacional):

Para la empresa C, se tiene:

$$HHT = 8 * 2 * 6 * 50 * 87 = 417600 \text{ horas al año.}$$

Tanto los días de para como en número de accidentes registrados fueron proporcionados por el personal del área de seguridad de la planta.

	2007	**2008**	**2009**	**2010**	**2011**	**2012**
HHT	417600	417600	417600	417600	417600	417600
Días de para	644	94	60	580	48	19
# de Accidentes	8	2	1	4	1	1

Tabla 3.9: *Datos proporcionados por la empresa C.*

	2007	**2008**	**2009**	**2010**	**2011**	**2012**	**Descripción**
IF	19.15	4.8	2.39	9.57	2.39	2.39	# de accidentes por cada 1000000 horas de trabajo
IG	1542.1	225.1	143.7	1388.8	114.9	45.5	# de días de para por cada 1000000 horas de trabajo
TR	9.19%	2.3%	1.15%	4.6%	1.15%	1.15%	% de ocurrencia de accidentes

Tabla 3.10: *Índices de Frecuencia, Gravedad y Accidentabilidad.*

EMPRESA C (Seguridad Funcional):

Son pocos los accidentes registrados relacionados a seguridad funcional, pero se desarrollará el mismo proceso realizado anteriormente. Ya que se trata de la misma fábrica, la cantidad de HHT es la misma.

	2007	2008	2009	2010	2011	2012
HHT	417600	417600	417600	417600	417600	417600
Días de para	155	300	0	205	0	155
# de Accidentes	1	2	0	1	0	1

Tabla 3.11: *Datos proporcionados por la empresa C.*

	2007	2008	2009	2010	2011	2012	Descripción
IF	2.39	4.79	0	2.39	0	2.39	# de accidentes por cada 1000000 horas de trabajo
IG	371.2	718.4	0	490.9	0	371.2	# de días de para por cada 1000000 horas de trabajo
TR	1.14%	2.3%	0	1.14%	0	1.14%	% de ocurrencia de accidentes

Tabla 3.12: *Índices de Frecuencia, Gravedad y Accidentabilidad.*

EMPRESA D (Seguridad Ocupacional):

Para la empresa D, se tiene:

$$HHT = 12 * 2 * 7 * 50 * 66 = 554400 \text{ horas al año.}$$

Tanto los días de para como en número de accidentes registrados fueron proporcionados por el personal del área de seguridad de la planta.

	2007	2008	2009	2010	2011	2012
HHT	554400	554400	554400	554400	554400	554400
Días de para	51	185	36	90	23	74
# de Accidentes	5	8	2	2	1	3

Tabla 3.13: *Datos proporcionados por la empresa D.*

	2007	2008	2009	2010	2011	2012	Descripción
IF	9.02	14.43	3.6	3.6	1.8	5.4	# de accidentes por cada 1000000 horas de trabajo
IG	91.9	333.7	64.9	162.3	41.5	133.5	# de días de para por cada 1000000 horas de trabajo
TR	7.6%	12.12%	3%	3%	1.51%	4.5%	% de ocurrencia de accidentes

Tabla 3.14: *Índices de Frecuencia, Gravedad y Accidentabilidad.*

EMPRESA D (Seguridad Funcional):

Son pocos los accidentes registrados relacionados a seguridad funcional, pero se desarrollará el mismo proceso realizado anteriormente. Ya que se trata de la misma fábrica, la cantidad de HHT es la misma.

	2007	2008	2009	2010	2011	2012
HHT	554400	554400	554400	554400	554400	554400
Días de para	0	0	6120	450	0	155
# de Accidentes	0	0	1	2	0	1

Tabla 3.15: *Datos proporcionados por la empresa D.*

	2007	2008	2009	2010	2011	2012	Descripción
IF	0	0	1.8	3.6	0	1.8	# de accidentes por cada 1000000 horas de trabajo
IG	0	0	11038.9	811.7	0	279.6	# de días de para por cada 1000000 horas de trabajo
TR	0	0	1.51%	3.03%	0	1.51%	% de ocurrencia de accidentes

Tabla 3.16: *Índices de Frecuencia, Gravedad y Accidentabilidad.*

Los datos de las empresas analizadas demuestran que los accidentes registrados en su mayoría están relacionados con seguridad ocupacional, mientras que en menor cantidad se encuentran los relacionados con seguridad funcional. Resulta interesante ver que la tasa de riesgo, el índice de gravedad y el índice de frecuencia correspondiente a la seguridad funcional son nulos en algunos años. Esto hace suponer que no ocurrieron accidentes durante dichos períodos, sin embargo, la realidad es que no fueron registrados debido a que el personal de seguridad que lleva el registro de dichos acontecimientos no los ha clasificado como tales.

Los accidentes laborales registrados en su mayoría están relacionados con la seguridad ocupacional. Esto se debe principalmente a que los organismos reguladores tales como el Ministerio de Salud Pública (MSP) y el Instituto Ecuatoriano de Seguridad Social (IESS) realizan inspecciones periódicas a las instalaciones para conocer el estado de la seguridad ocupacional que se maneja en el interior de las mismas. De esta manera se constata que se cumplan las normas de seguridad requeridas para el personal, dejando a un lado la seguridad funcional.

De la información recopilada mediante encuestas, se determinó que la aplicación de SIS en la industria de procesos de la ciudad es nula. Esto generalmente ha llevado a paro en la producción y en ocasiones a la muerte de personal de planta al presentarse situaciones inesperadas.

Uno de los principales motivos por los que las empresas no disponen de sistemas de seguridad se debe a su costo. En algunas empresas no se tiene claro o no quieren asimilar el criterio de que “es más costoso prescindir de él, que disponer de él.”.

El concepto de desarrollo sostenible manejado por algunas empresas está enfocado en los factores económicos, materiales y humanos, pero no contempla el factor ambiental.

En algunas empresas la maquinaria utilizada en sus procesos ya ha excedido su tiempo de vida útil. Para algunas máquinas ya ni siquiera es posible conseguir partes de reemplazo, por ello, muchas de estas partes son fabricadas localmente. Esto no garantiza el buen funcionamiento de la maquinaria lo que da lugar a situaciones de riesgo.

Capítulo 4

DISEÑO DE UN SIS PARA EL AREA DE ALMACENAMIENTO DE COMBUSTIBLES DE TUGALT.

Una de las empresas más grandes de la ciudad, tanto a nivel geográfico como a nivel productivo es Tugalt. Dicha empresa está orientada a la fabricación de toda clase de perfiles, paneles y tubos metálicos, pero también se encarga de almacenar combustible que es enviado a otras industrias como Industrias Químicas del Austro (IQA), Vanderbilt, y Graiman. El combustible almacenado consta principalmente de diésel y bunker, los mismos que son fundamentales para la realización de todos los procesos llevados a cabo en las industrias antes indicadas.

Se ha considerado el área de almacenamiento de combustible para desarrollar el diseño del SIS debido a que en la actualidad no dispone de ningún dispositivo o sistema para prevenir o mitigar eventos inesperados o de alto riesgo en dicha zona. Algunos eventos como derrames de combustible, obstrucción de líneas de bombeo o pérdida de presión en las mismas ya han tenido lugar, pero no se han resultado en situaciones graves.

Este capítulo está orientado al diseño de un SIS que se encargue de monitorear el proceso de distribución de combustible desde los tanques de almacenamiento primario (100 000 glns. de diésel y 50 000 glns. de bunker) hacia los procesos involucrados. Los tanques de almacenamiento primario son cargados mediante la utilización de bombas que vacían el contenido de tanqueros que visitan las instalaciones dos veces por semana (búnker) y cinco veces por semana (diésel). El combustible es transmitido a tanques de almacenamiento secundario y de aquí es enviado hacia los quemadores, hornos y crisol respectivamente. En el tramo comprendido entre los tanques de almacenamiento primario y secundario, el SIS debe conocer constantemente el estado del flujo de combustible, el nivel del mismo dentro de los tanques primarios y la temperatura presente en la niquelina que calienta el búnker.

4.1 Desarrollo del HazOp

Para desarrollar el HazOp (Anexo 2) es fundamental disponer del diagrama P&ID del sistema (Anexo 1). Con base en dicho diagrama se definen los peligros que podrían suscitarse y que elementos del sistema están involucrados.

4.2 Desarrollo del LOPA.

Con el hazOp realizado previamente se desarrolla el análisis de las capas de protección (LOPA). En él se analizan las situaciones que pudieran presentarse, sus respectivas causas de inicio y su frecuencia de ocurrencia.

En primer lugar, se analizó el sistema en su estado actual y posteriormente se realizó un nuevo análisis considerando las capas de protección a implementar según el SIL requerido por cada una de las SIF (Anexo 3) para reducir el riesgo a niveles tolerables. Se pudo observar que la integridad de seguridad de la SIF varió drásticamente al agregar capas adicionales de protección.

4.3 Desarrollo de la SRS

Luego de haber establecido las capas de seguridad necesarias en el sistema se procede al desarrollo de la ingeniería en detalle del SIS, para ello se desarrollaron las especificaciones de requerimientos de seguridad (SRS), las mismas que se detallan a continuación:

1. **DEFINICION DEL PROCESO**

   El proceso analizado hace referencia al almacenamiento y transferencia de combustible desde los tanques primarios hacia los secundarios. En dicho proceso están involucradas bombas eléctricas para realizar el llenado de los tanques, que son operadas de forma manual ya que el proceso no se encuentra automatizado.

   Ya se han presentado situaciones de emergencia debido a la falta de control sobre el proceso, un ejemplo de ello es el derrame de combustible de los tanques primarios debido a un sobrellenado de los mismos.

Al momento el personal de planta tiene que realizar inspecciones periódicas para conocer el nivel de combustible en los tanques de almacenamiento secundario. Si se requiere rellenar uno de ellos se abre una válvula manual para permitir el paso del combustible.

2. REQUERIMIENTOS GENERALES

Ya que el sistema carece de un BPCS, todo el proceso de monitoreo lo realiza personal de la planta tomando como referencia las lecturas arrojadas por instrumentos de medición localizados en campo.

El sistema instrumentado de seguridad debe controlar el flujo combustible (diésel y bunker) en las tuberías de transferencia y los niveles del mismo en los tanques de almacenamiento primario y secundario, así también, debe monitorear la temperatura en calefactor del bunker para evitar la obstrucción de tuberías de combustible.

3. REQUERIMIENTOS DEL SOFTWARE

Muchas técnicas y métodos son utilizados para desarrollar el software de aplicación, por lo general estos métodos siguen una secuencia de pasos con el fin de lograrlo. El método más común y a la vez el más peligroso es el “codificar y reparar”, es decir, el programador escribe el código y pregunta al cliente si es lo que desea. Esto se vuelve repetitivo ya que se realizan muchas modificaciones provocando que el software desarrollado esté basado en lineamientos que no van acordes con los requerimientos de seguridad.

Para que el software desarrollado cumpla con los requerimientos de seguridad, se ha desarrollado diferentes modelos para su desarrollo. Un ejemplo de ellos es el modelo en V (Figura 4.3.1), el mismo que describe una aproximación de diseño y pruebas.

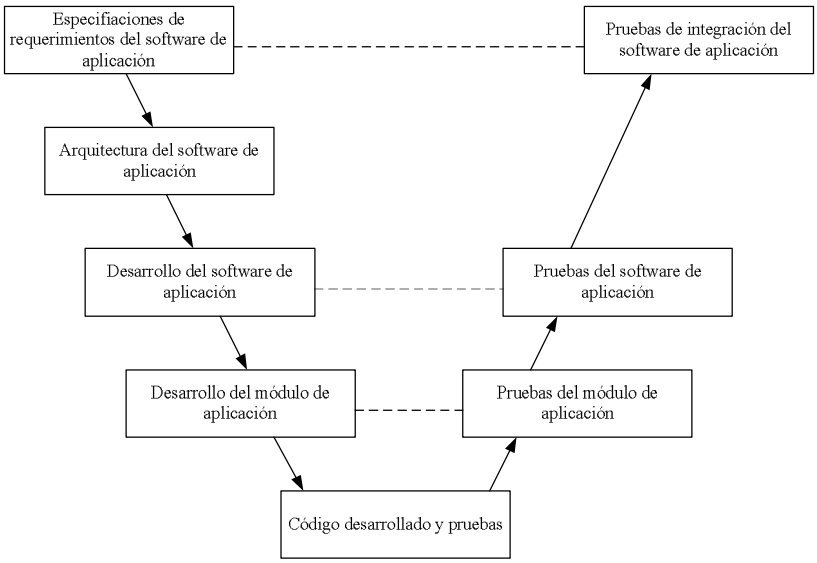


Figura 4.3.1 *Modelo en V.*

Los requerimientos del software de seguridad para el SIS a diseñar son los siguientes:

1. **Requerimientos del Software.-** El software a desarrollar debe encargarse de apagar todos los elementos finales que se encuentren energizados cuando se produzca un evento peligroso, al mismo tiempo activará las correspondientes alarmas para notificar que tipo de evento a ocurrido. El software es del tipo *orientado a utilidad*[13] debido a que será utilizado en el desarrollo y verificación del programa de aplicación. Será operado por personal capacitado, técnicos y administradores del sistema por lo que debe disponer de contraseñas según el grado de acceso que se le permita al usuario. La edición o actualización del programa deberá ser realizado únicamente por el personal técnico capacitado para dicha tarea.

2. **Arquitectura del Software.-** El software consta de una rutina principal y de subrutinas que se encargarán respectivamente de activar el lazo de seguridad necesario.

[13] El software orientado a utilidad se utiliza para desarrollar y verificar el programa de aplicación.

Será elaborado en lenguaje de variabilidad limitada (*Limited Variability Language,* LVL) debido a que será restringido a la aplicación de librerías de función predeterminadas.

3. **Programación.-** El lenguaje de programación a utilizar será Lógica de escalera (*Ladder Logic*) debido a que es simple y fácil de comprender cuando se revisa el programa. Además es considerado apto para aplicaciones con un SIL de 1 a 3 y es el lenguaje de programación por defecto para el controlador ControlLogix a utilizar.

4. **Integración.-** La integración del sistema de seguridad no presentará interferencias debido a que en las instalaciones no hay sistema de control de procesos. Por ello, la ejecución del programa de seguridad no se verá afectado por ningún elemento ajeno al SIS.

5. **Pruebas.-** Se deberán realizar pruebas en las cuales se compruebe el desempeño del programa de seguridad, es decir, evaluar cada una de las SIF y corroborar si desempeñan la acción esperada, en caso de no cumplirla se deberá revisar la conexión de todo el hardware involucrado para determinar la causa del mal funcionamiento de la SIF en cuestión.

4. REQUERIMIENTOS FUNCIONALES

Fuente de demanda.- Falla bomba B1.
Descripción Funcional.- La SIF debe proteger al sistema cuando el flujo en la tubería de transferencia L1 sea reducido. Debe sensar la cantidad de fluido en la tubería, si la cantidad es menor a un valor de referencia o nulo, debe de activar una alarma para indicar que el flujo ha disminuido.
Estado seguro del proceso.- Al reducirse el flujo en L1, la SIF debe apagar la bomba B1.
Tasa de demanda de la SIF.- 0.71.
SIL determinado para la SIF.- SIL 1.

Fuente de demanda.- Falla en el calentador de bunker.
Descripción Funcional.- La SIF debe proteger al sistema cuando el nivel en el tanque TA_1 sobrepase el límite superior permitido. Debe sensar el nivel de fluido almacenado en el tanque, si la cantidad de combustible supera el límite superior, se debe de activar una alarma para indicar que el nivel es muy elevado y debe cerrar la electroválvula V-16 colocada al ingreso del tanque para evitar que se produzca un derrame de combustible.
Estado seguro del proceso.- Cuando el nivel de combustible en el tanque sea muy elevado, la SIF debe cerrar V-16.
Tasa de demanda de la SIF.- 0.0317.
SIL determinado para la SIF.- SIL 1.

Fuente de demanda.- Falla control de temperatura.
Descripción Funcional.- La SIF debe proteger al sistema cuando la temperatura del calentador del bunker cambie bruscamente. Debe sensar la temperatura del calentador, si la temperatura excede los límites inferior o superior debe activar una alarma indicando que un evento ha tenido lugar. Así también, activará la electroválvula V-14 que bloqueará el ingreso de bunker al calentador para evitar que este se bloquee.
Estado seguro del proceso.- Al reducirse la temperatura en el calentador H1, la SIF debe bloquear el paso de bunker al mismo.
Tasa de demanda de la SIF.- 0.030.
SIL determinado para la SIF.- SIL 1.

Fuente de demanda.- Falla bomba B2.
Descripción Funcional.- La SIF debe proteger al sistema cuando el nivel en el tanque TA_2 alcance el límite superior, así también, activará la electroválvula V-15 que bloqueará el ingreso de combustible al tanque.
Estado seguro del proceso.- Alto nivel de combustible en el tanque cierra V-15.
Tasa de demanda de la SIF.- 0.030.
SIL determinado para la SIF.- SIL 1.

Fuente de demanda.- Bajo flujo en L4.
Descripción Funcional.- La SIF debe proteger al sistema cuando la cantidad de flujo en la tubería de transferencia L4 sea reducido. Debe sensar la cantidad de fluido en la tubería, si la cantidad es menor a un valor de referencia o nulo, debe de activar una alarma para indicar que el flujo ha disminuido.
Estado seguro del proceso.- Alto nivel de combustible en el tanque cierra V-15.
Tasa de demanda de la SIF.- 0.0317.
SIL determinado para la SIF.- SIL 1.

Fuente de demanda.- PLC de llenado.
Descripción Funcional.- La SIF debe proteger al sistema cuando el nivel en el tanque TA_3 alcance el límite superior, así también, activará la electroválvula V-16 que bloqueará el ingreso de combustible al tanque.
Estado seguro del proceso.- Al activar V-16 se evita que ingrese más combustible al tanque y se produzca un derrame del mismo.
Tasa de demanda de la SIF.- 0.00948.
SIL determinado para la SIF.- SIL 2.

4.4 Cálculo de SIL de los lazos de seguridad.

4.4.1 CALCULO DE PFD ELEMENTOS DE SEGURIDAD:

Los principales parámetros involucrados en los cálculos para determinar la Probabilidad de Falla a la Demanda (PFD) son:

λ_T = Tasa de fallas
λ_S = Tasa de fallas seguras = λ_T x 50%
λ_d = Tasa de fallas peligrosas = λ_T x 50%
λ_{dd} = Tasa de fallas peligrosas detectadas = $\lambda_T / 2xDC$
λ_{du} = Tasa de fallas peligrosas no detectadas = $\lambda_T / 2x(1 - DC)$
Fracción de Falla Segura (SFF) = $(\lambda_S + \lambda_{dd})/\lambda_T$
Cobertura de diagnóstico (DC)
β = Factor de causa común para fallas no detectadas.
β_D = Factor de causa común para fallas detectadas.

Para los siguientes elementos de seguridad, los datos antes mencionados fueron tomados del libro "Offshore Reliability Data" (OREDA, 2002). Así mismo, el porcentaje de cobertura de diagnóstico se establece en un 70% ya que se considera que la frecuencia de la prueba de diagnóstico es baja:

- <60% = ninguna
- 60% to <90% = baja
- 90% to <99% = media
- 99%+ = alta

Sensor de flujo (1oo1)

MTTR= 8 hrs.
CD = 70%
T_1 = 1 $año$ (8760 $hrs.$)
λ_T = $2.54x10^{-5}/hora.$
λ_S = $\lambda_T x0.5$ = $1.27x10^{-5}/hora.$
λ_D = $\lambda_T x0.5$ = $1.27x10^{-5}/hora.$
λ_{dd} = $\lambda_T/2xDC$ = $2.54x10^{-5}/2x0.7$ = $8.89x10^{-6}$
λ_{du} = $\lambda_T/2x(1-DC)$ = $2.54x10^{-5}/2x(1-0.7)$ = $3.81x10^{-6}$

Tasa de fallas peligrosas:

$$\lambda_D = \lambda_{dd} + \lambda_{du} = 8.89x10^{-6} + 3.81x10^{-6} = 1.27x10^{-5}$$

Fracción de Falla Segura:

$$SFF = \frac{\lambda_S + \lambda_{dd}}{\lambda_T}$$

$$SFF = \frac{1.27x10^{-5} + 8.89x10^{-6}}{2.54x10^{-5}} = 0.85$$

$$SFF = 85\%$$

Tiempo medio de para en el subsistema:

$$t_{CE} = \frac{\lambda_{du}}{\lambda_D}\left(\frac{T_1}{2} + MTTR\right) + \frac{\lambda_{dd}}{\lambda_D} MTTR$$

$$t_{CE} = \frac{3.81x10^{-6}}{1.27x10^{-5}}\left(\frac{8760}{2} + 8\right) + \frac{8.89x10^{-6}}{1.27x10^{-5}} * 8 = 1322$$

$$t_{CE} = 1322$$

Probabilidad de falla a la demanda:

$$PFD_{AV} = (\lambda_{dd} + \lambda_{du})t_{CE}$$

$$PFD_{AV} = (8.89x10^{-6} + 3.81x10^{-6}) * 1322$$
$$\boldsymbol{PFD_{AV} = 0.0168}$$

Sensor de nivel (1oo1)

MTTR= 8 hrs.
$CD = 70\%$
$T_1 = 1\ año\ (8760\ hrs.)$
$\lambda_T = 2.28x10^{-6}/hora.$
$\lambda_S = \lambda_T x0.5 = 1.14x10^{-6}/hora.$
$\lambda_D = \lambda_T x0.5 = 1.14x10^{-6}/hora.$
$\lambda_{dd} = \lambda_T/2xDC = 2.28x10^{-6}/2x0.7 = 7.98x10^{-7}$
$\lambda_{du} = \lambda_T/2x(1-DC) = 2.28x10^{-6}/2x(1-0.7) = 3.42x10^{-7}$

Tasa de fallas peligrosas:

$$\lambda_D = \lambda_{dd} + \lambda_{du} = 7.98x10^{-7} + 3.42x10^{-7} = 1.14x10^{-6}$$

Fracción de Falla Segura:

$$SFF = \frac{\lambda_S + \lambda_{dd}}{\lambda_T}$$
$$SFF = \frac{1.14x10^{-6} + 7.98x10^{-7}}{2.28x10^{-6}} = 0.85$$

$$SFF = 85\%$$

Tiempo medio de para en el subsistema:

$$t_{CE} = \frac{\lambda_{du}}{\lambda_D}\left(\frac{T_1}{2} + MTTR\right) + \frac{\lambda_{dd}}{\lambda_D} MTTR$$

$$t_{CE} = \frac{3.42x10^{-7}}{1.14x10^{-6}}\left(\frac{8760}{2} + 8\right) + \frac{7.98x10^{-7}}{1.14x10^{-6}} * 8 = 1322$$

$$t_{CE} = 1322$$

Probabilidad de falla a la demanda:

$$PFD_{AV} = (\lambda_{dd} + \lambda_{du})t_{CE}$$

$$PFD_{AV} = (7.98x10^{-6} + 3.42x10^{-7}) * 1322$$
$$\boldsymbol{PFD_{AV} = 0.0151}$$

Sensor de nivel (1oo2)

MTTR= 8 hrs.
$CD = 70\%$
$\beta = 10\%$
$\beta_D = 10\%$
$T_1 = 1\ año\ (8760\ hrs.)$
$\lambda_T = 2.28x10^{-6}/hora.$
$\lambda_S = \lambda_T x0.5 = 1.14x10^{-6}/hora.$
$\lambda_D = \lambda_T x0.5 = 1.14x10^{-6}/hora.$
$\lambda_{dd} = \lambda_T/2xDC = 2.28x10^{-6}/2x0.7 = 7.98x10^{-7}$
$\lambda_{du} = \lambda_T/2x(1-DC) = 2.28x10^{-6}/2x(1-0.7) = 3.42x10^{-7}$

Tasa de fallas peligrosas:

$$\lambda_D = \lambda_{dd} + \lambda_{du} = 7.98x10^{-7} + 3.42x10^{-7} = 1.14x10^{-6}$$

Fracción de Falla Segura:

$$SFF = \frac{\lambda_S + \lambda_{dd}}{\lambda_T}$$

$$SFF = \frac{1.14x10^{-6} + 7.98x10^{-7}}{2.28x10^{-6}} = 0.85$$

$$SFF = 85\%$$

Tiempo medio de para en el subsistema:

$$t_{CE} = \frac{\lambda_{du}}{\lambda_D}\left(\frac{T_1}{2} + MTTR\right) + \frac{\lambda_{dd}}{\lambda_D} MTTR$$

$$t_{CE} = \frac{3.42x10^{-7}}{1.14x10^{-6}}\left(\frac{8760}{2} + 8\right) + \frac{7.98x10^{-7}}{1.14x10^{-6}} * 8 = 1322$$

$$t_{CE} = 1322$$

$$t_{GE} = \frac{\lambda_{du}}{\lambda_D}\left(\frac{T_1}{3} + MTTR\right) + \frac{\lambda_{dd}}{\lambda_D} MTTR$$

$$t_{GE} = \frac{3.42x10^{-7}}{1.14x10^{-6}}\left(\frac{8760}{3} + 8\right) + \frac{7.98x10^{-7}}{1.14x10^{-6}} * 8 = 884$$

$$t_{GE} = 884$$

Probabilidad de falla a la demanda:

$$PFD_{AV} = 2 * [(1 - \beta_D) * \lambda_{DD} + (1 - \beta) * \lambda_{DU}]^2 * t_{CE} * t_{GE} + (\beta_D * \lambda_{DD} * MTTR) + \beta * \lambda_{DU} * \left({}^{T_1}/_{2} + MTTR\right)$$

$$PFD_{AV} = 2 * [(1 - 0.1) * 7.98x10^{-7} + (1 - 0.1) * 3.42x10^{-7}]^2 * 1322 * 884 + (0.1 * 7.98x10^{-7} * 8) + 0.1 * 3.42x10^{-7} * \left({}^{8760}/_{2} + 8\right)$$

$$\boldsymbol{PFD_{AV} = 0.0015}$$

Sensor de Temperatura (1oo1)

MTTR= 8 hrs.
CD = 70%
T_1 = 1 $año$ (8760 $hrs.$)
$\lambda_T = 1.705x10^{-5}/hora.$
$\lambda_S = \lambda_T x0.5 = 8.525x10^{-6}/hora.$
$\lambda_D = \lambda_T x0.5 = 8.525x10^{-6}/hora.$

$\lambda_{dd} = \lambda_T / 2xDC = 1.705x10^{-5} / 2x0.7 = 5.967x10^{-6}$
$\lambda_{du} = \lambda_T / 2x(1 - DC) = 7.28x10^{-6} / 2x(1 - 0.7) = 2.557x10^{-6}$

Tasa de fallas peligrosas:

$$\lambda_D = \lambda_{dd} + \lambda_{du} = 5.967x10^{-6} + 2.557x10^{-6} = 8.525x10^{-6}$$

Fracción de Falla Segura:

$$SFF = \frac{\lambda_S + \lambda_{dd}}{\lambda_T}$$

$$SFF = \frac{8.525x10^{-6} + 5.967x10^{-6}}{1.705x10^{-5}} = 0.85$$

$$SFF = 85\%$$

Tiempo medio de para en el subsistema:

$$t_{CE} = \frac{\lambda_{du}}{\lambda_D}\left(\frac{T_1}{2} + MTTR\right) + \frac{\lambda_{dd}}{\lambda_D} MTTR$$

$$t_{CE} = \frac{2.557x10^{-6}}{8.525x10^{-6}}\left(\frac{8760}{2} + 8\right) + \frac{5.967x10^{-6}}{8.525x10^{-6}} * 8 = 1322$$

$$t_{CE} = 1322$$

Probabilidad de falla a la demanda:

$$PFD_{AV} = (\lambda_{dd} + \lambda_{du}) t_{CE}$$

$$PFD_{AV} = (5.967x10^{-6} + 2.557x10^{-6}) * 1322$$
$$\boldsymbol{PFD_{AV} = 0.0112}$$

Válvula operada remotamente (1oo1)

MTTR= 8 hrs.
T_1 = 1 $año$ (8760 $hrs.$)
CD = 70%
λ_T = $8.02x10^{-5}/hora.$
λ_S = $\lambda_T x0.5$ = $4.01x10^{-5}/hora.$
λ_D = $\lambda_T x0.5$ = $4.01x10^{-5}/hora.$
λ_{dd} = $\lambda_T/2xDC$ = $8.02x10^{-5}/2x0.7$ = $2.807x10^{-6}$
λ_{du} = $\lambda_T/2x(1-DC)$ = $8.02x10^{-6}/2x(1-0.7)$ = $1.203x10^{-6}$

Tasa de fallas peligrosas:

$$\lambda_D = \lambda_{dd} + \lambda_{du} = 2.807x10^{-6} + 1.203x10^{-6} = 4.01x10^{-6}$$

Fracción de Falla Segura:

$$SFF = \frac{\lambda_S + \lambda_{dd}}{\lambda_T}$$

$$SFF = \frac{4.01x10^{-6} + 2.807x10^{-6}}{8.02x10^{-6}} = 0.85$$

$$SFF = 85\%$$

Tiempo medio de para en el subsistema:

$$t_{CE} = \frac{\lambda_{du}}{\lambda_D}\left(\frac{T_1}{2} + MTTR\right) + \frac{\lambda_{dd}}{\lambda_D} MTTR$$

$$t_{CE} = \frac{1.203x10^{-6}}{4.01x10^{-6}}\left(\frac{8760}{2} + 8\right) + \frac{2.807x10^{-6}}{4.01x10^{-6}} * 8 = 1322$$

$$t_{CE} = 1322$$

Probabilidad de falla a la demanda:

$$PFD_{AV} = (\lambda_{dd} + \lambda_{du})t_{CE}$$

$$PFD_{AV} = (2.807x10^{-6} + 1.203x10^{-6}) * 1322$$
$$\boldsymbol{PFD_{AV} = 0.0053}$$

PLC de Seguridad (1oo1)

El PLC escogido es un Controlador 1756 ControlLogix, el mismo tiene las siguientes características:

MTTR= 8 hrs.
$T_1 = 1\ año\ (8760\ hrs.)$
$\lambda_T = 9.47x10^{-7}/hora.$
$\lambda_S = 4.74x10^{-7}/hora.$
$\lambda_D = 4.74x10^{-7}/hora.$
$\lambda_{dd} = 4.26x10^{-7}$
$\lambda_{du} = 4.74x10^{-8}$

Tasa de fallas peligrosas:

$$\lambda_D = \lambda_{dd} + \lambda_{du} = 4.26x10^{-7} + 4.74x10^{-8} = 4.74x10^{-7}$$

Fracción de Falla Segura:

$$SFF = \frac{\lambda_S + \lambda_{dd}}{\lambda_T}$$

$$SFF = \frac{4.74x10^{-7} + 4.26x10^{-7}}{9.47x10^{-7}} = 0.95$$

$$SFF = 95\%$$

Tiempo medio de para en el subsistema:

$$t_{CE} = \frac{\lambda_{du}}{\lambda_D}\left(\frac{T_1}{2} + MTTR\right) + \frac{\lambda_{dd}}{\lambda_D} MTTR$$

$$t_{CE} = \frac{4.74x10^{-8}}{4.74x10^{-7}}\left(\frac{8760}{2} + 8\right) + \frac{4.26x10^{-7}}{4.74x10^{-7}} * 8 = 445.99$$

$$t_{CE} = 445.99$$

Probabilidad de falla a la demanda:

$$PFD_{AV} = (\lambda_{dd} + \lambda_{du}) t_{CE}$$

$$PFD_{AV} = (4.26x10^{-7} + 4.74x10^{-8}) * 445.99$$

$$\boldsymbol{PFD_{AV} = 0.000211}$$

PLC de Seguridad (1oo2)

El PLC escogido es un Controlador 1756 ControlLogix, el mismo tiene las siguientes características:

MTTR= 8 hrs.
β = 10%
β_D = 10%
T_1 = 1 *año* (8760 *hrs.*)
$\lambda_T = 9.47x10^{-7}/hora.$
$\lambda_S = 4.74x10^{-7}/hora.$
$\lambda_D = 4.74x10^{-7}/hora.$
$\lambda_{dd} = 4.26x10^{-7}$
$\lambda_{du} = 4.74x10^{-8}$

Tasa de fallas peligrosas:

$$\lambda_D = \lambda_{dd} + \lambda_{du} = 4.26x10^{-7} + 4.74x10^{-8} = 4.74x10^{-7}$$

Fracción de Falla Segura:

$$SFF = \frac{\lambda_S + \lambda_{dd}}{\lambda_T}$$

$$SFF = \frac{4.74x10^{-7} + 4.26x10^{-7}}{9.47x10^{-7}} = 0.95$$

$$SFF = 95\%$$

Tiempo medio de para en el subsistema:

$$t_{CE} = \frac{\lambda_{du}}{\lambda_D}\left(\frac{T_1}{2} + MTTR\right) + \frac{\lambda_{dd}}{\lambda_D} MTTR$$

$$t_{CE} = \frac{4.74x10^{-8}}{4.74x10^{-7}}\left(\frac{8760}{2} + 8\right) + \frac{4.26x10^{-7}}{4.74x10^{-7}} * 8 = 445.99$$

$$t_{CE} = 445.99$$

$$t_{GE} = \frac{\lambda_{du}}{\lambda_D}\left(\frac{T_1}{3} + MTTR\right) + \frac{\lambda_{dd}}{\lambda_D} MTTR$$

$$t_{GE} = \frac{4.74x10^{-8}}{4.74x10^{-7}}\left(\frac{8760}{3} + 8\right) + \frac{4.26x10^{-7}}{4.74x10^{-7}} * 8 = 299.99$$

$$t_{GE} = 299.99$$

Probabilidad de falla a la demanda:

$$PFD_{AV} = 2 * [(1 - \beta_D) * \lambda_{DD} + (1 - \beta) * \lambda_{DU}]^2 * t_{CE} * t_{GE} + (\beta_D * \lambda_{DD} * MTTR) + \beta * \lambda_{DU} * \left({}^{T_1}/_{2} + MTTR\right)$$

$$PFD_{AV} = 2 * [(1 - 0.1) * 4.26x10^{-7} + (1 - 0.1) * 4.74x10^{-8}]^2 * 445.99 * 299.99 + (0.1 * 4.26x10^{-7} * 8) + 0.1 * 4.74x10^{-8} * \left({}^{8760}/_{2} + 8\right)$$

$$\boldsymbol{PFD_{AV} = 0.000021}$$

Relé de Seguridad

El relé de seguridad elegido es un 1771 digital I/O Relay Contact Output, el mismo tiene las siguientes especificaciones:

MTTR= 8 hrs.
T_1 = 1 $año$ (8760 $hrs.$)
λ_T = $1.65x10^{-7}/hora.$
λ_S = $8.25x10^{-8}/hora.$
λ_D = $8.25x10^{-8}/hora.$
λ_{dd} = $4.95x10^{-8}$
λ_{du} = $3.30x10^{-8}$

Tasa de fallas peligrosas:

$$\lambda_D = \lambda_{dd} + \lambda_{du} = 4.95x10^{-8} + 3.30x10^{-8} = 8.25x10^{-8}$$

Fracción de Falla Segura:

$$SFF = \frac{\lambda_S + \lambda_{dd}}{\lambda_T}$$

$$SFF = \frac{8.25x10^{-8} + 4.95x10^{-8}}{1.65x10^{-7}} = 0.8$$

$$SFF = 80\%$$

Tiempo medio de para en el subsistema:

$$t_{CE} = \frac{\lambda_{du}}{\lambda_D}\left(\frac{T_1}{2} + MTTR\right) + \frac{\lambda_{dd}}{\lambda_D} MTTR$$

$$t_{CE} = \frac{3.30x10^{-8}}{8.25x10^{-8}}\left(\frac{8760}{2} + 8\right) + \frac{4.95x10^{-8}}{8.25x10^{-8}} * 8 = 1760$$

$$t_{CE} = 1760$$

Probabilidad de falla a la demanda:

$$PFD_{AV} = (\lambda_{dd} + \lambda_{du})t_{CE}$$

$$PFD_{AV} = (4.95x10^{-8} + 3.30x10^{-8}) * 1760$$

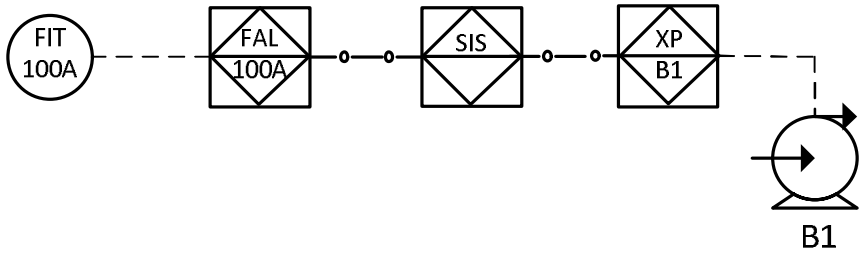
$$\boldsymbol{PFD_{AV} = 0.000145}$$

4.4.2 CÁLCULO DE PFD DE LAZOS DE SEGURIDAD:

En los lazos de seguridad que corresponden a SIL 2, se ha considerado la redundancia debido a que son lazos con un elevado índice de riesgo, es decir, se debe asegurar el funcionamiento de dichos lazo bajo demanda. Además los elementos utilizados en dichos lazos tienen una SFF comprendida entre el 60% y 90%, por lo que se recomienda utilizar redundancia.

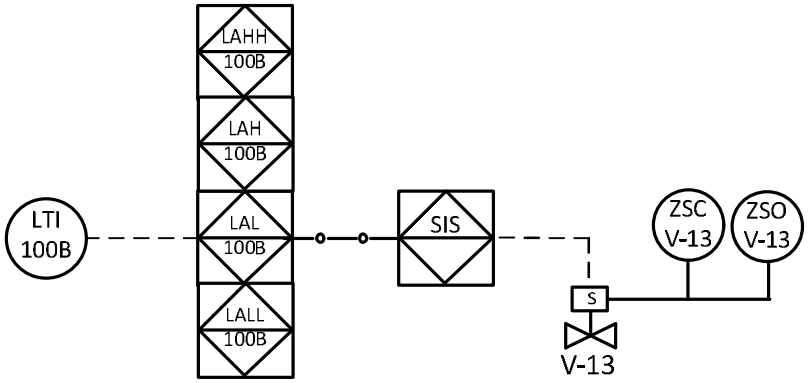
Lazo 100A

SIL	PFD	RRF	HFT
1	0.019	52.63	0



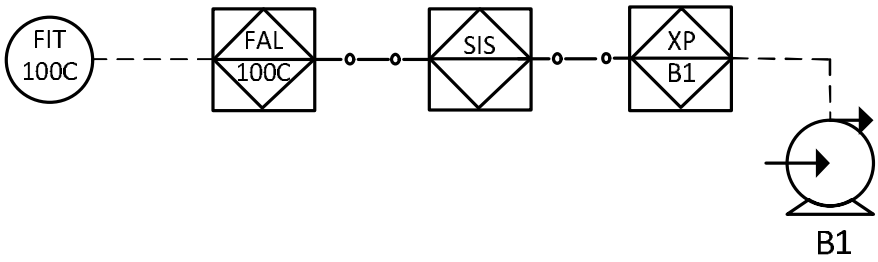
Lazo 100B

SIL	PFD	RRF	HFT
2	0.005619	177.968	1



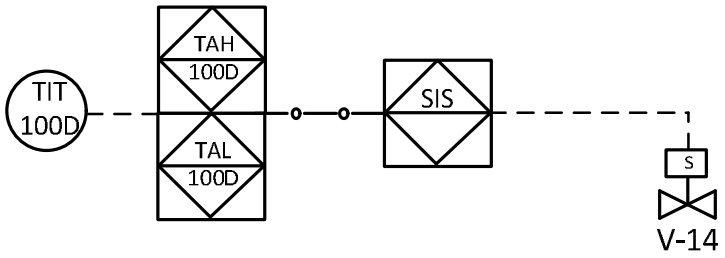
Lazo 100C

SIL	PFD	RRF	HFT
1	0.019	52.63	0



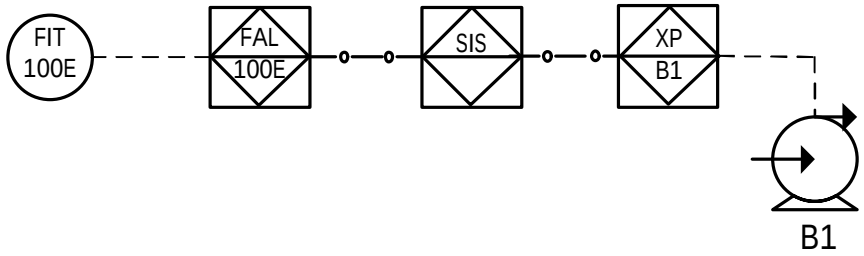
Lazo 100D

SIL	PFD	RRF	HFT
1	0.019	52.63	0



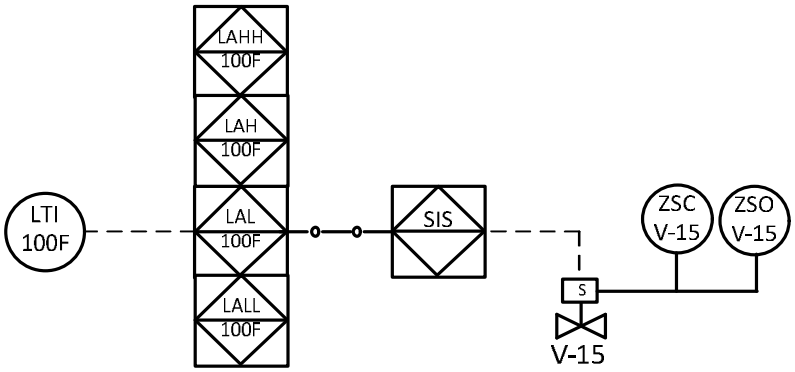
Lazo 100E

SIL	PFD	RRF	HFT
1	0.019	52.63	0



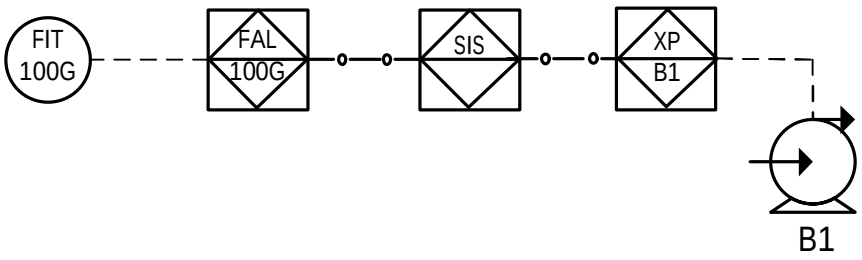
Lazo 100F

SIL	PFD	RRF	HFT
2	0.005619	177.968	1



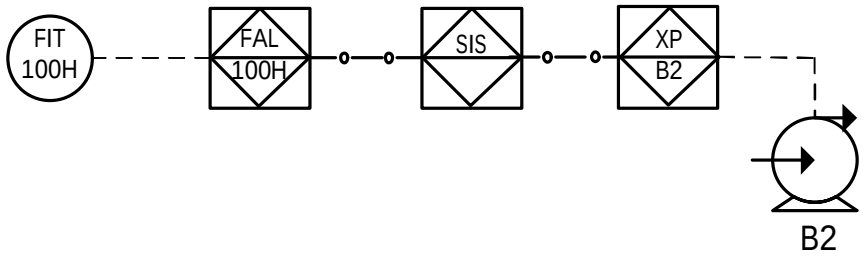
Lazo 100G

SIL	PFD	RRF	HFT
1	0.019	52.63	0



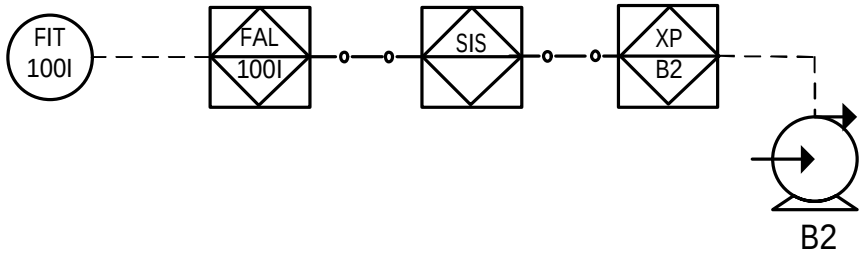
Lazo 100H

SIL	PFD	RRF	HFT
1	0.019	52.63	0



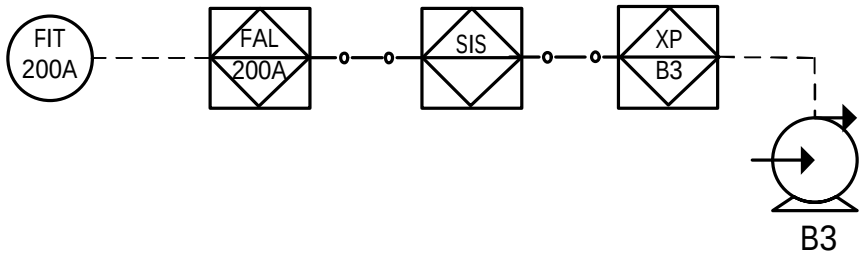
Lazo 100I

SIL	PFD	RRF	HFT
1	0.019	52.63	0



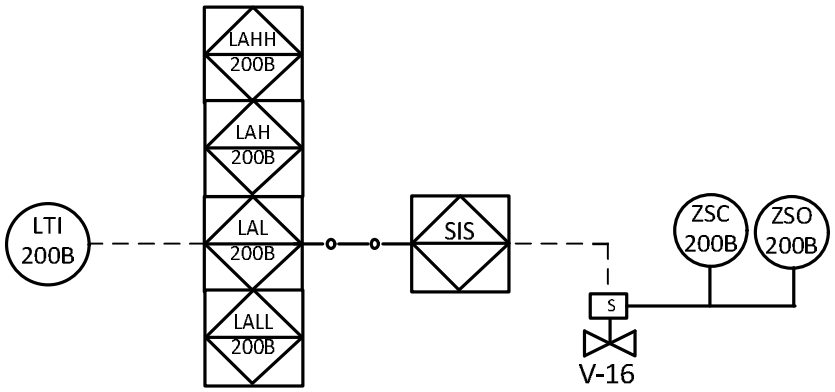
Lazo 200A

SIL	PFD	RRF	HFT
1	0.019	52.63	0



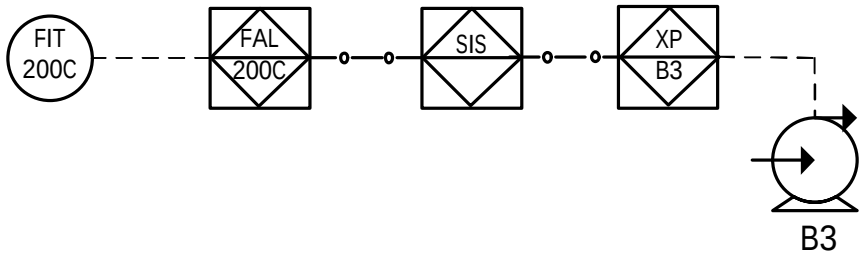
Lazo 200B

SIL	PFD	RRF	HFT
2	0.005619	177.968	1



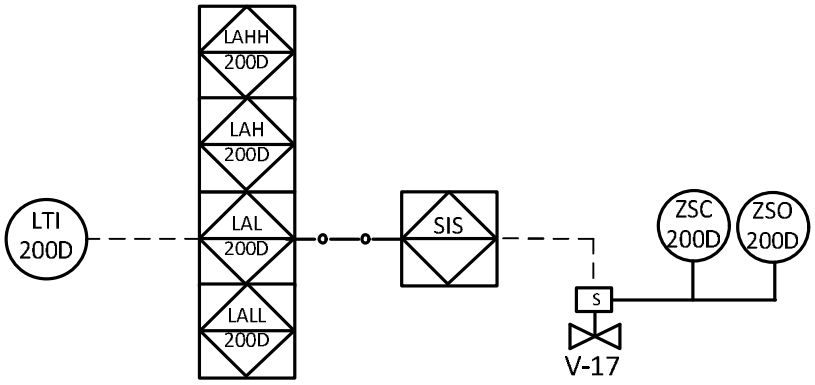
Lazo 200C

SIL	PFD	RRF	HFT
1	0.019	52.63	0



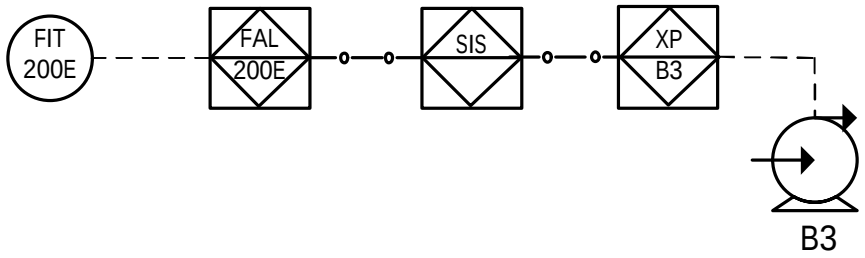
Lazo 200D

SIL	PFD	RRF	HFT
2	0.005619	177.968	1



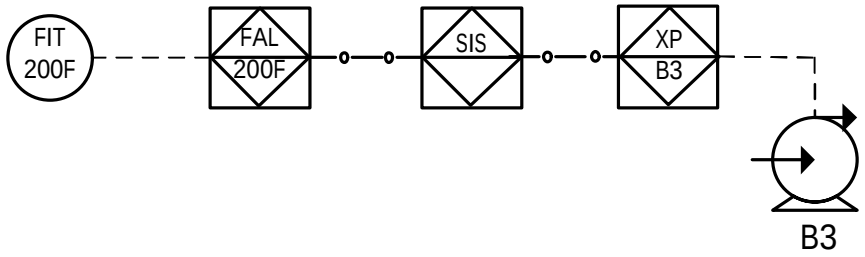
Lazo 200E

SIL	PFD	RRF	HFT
1	0.019	52.63	0



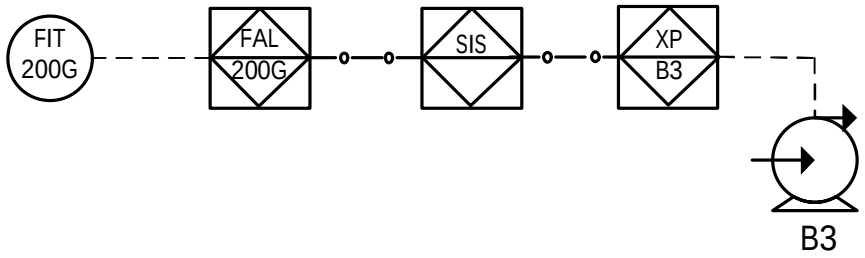
Lazo 200F

SIL	PFD	RRF	HFT
1	0.019	52.63	0



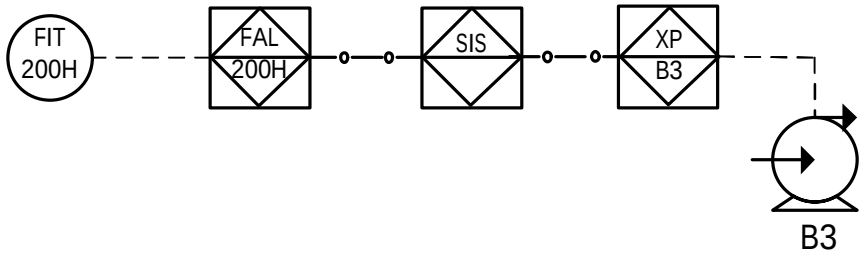
Lazo 200G

SIL	PFD	RRF	HFT
1	0.019	52.63	0



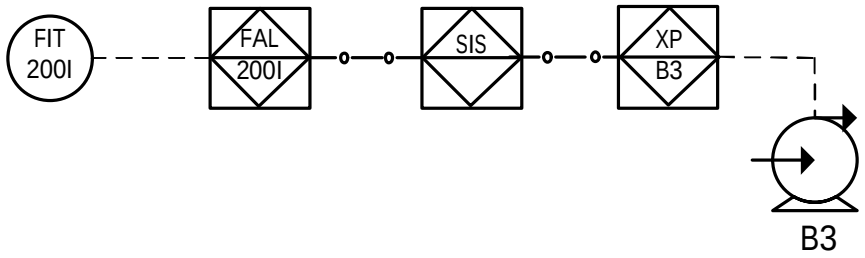
Lazo 200H

SIL	PFD	RRF	HFT
1	0.019	52.63	0



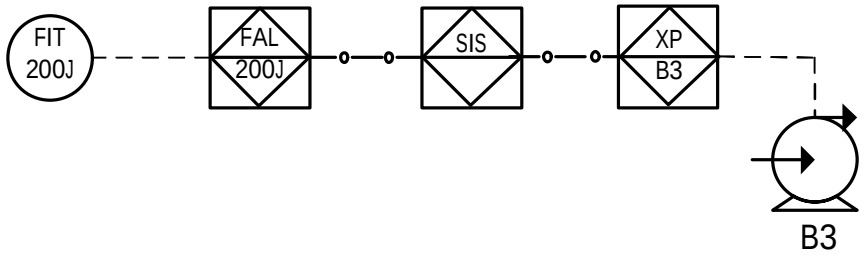
Lazo 200I

SIL	PFD	RRF	HFT
1	0.019	52.63	0



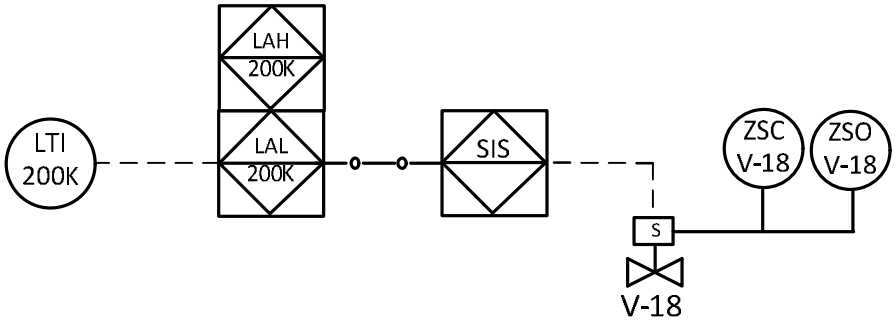
Lazo 200J

SIL	PFD	RRF	HFT
1	0.019	52.63	0



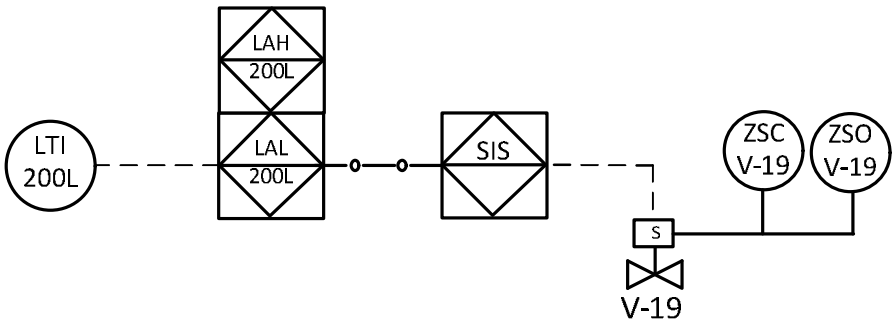
Lazo 200K

SIL	PFD	RRF	HFT
1	0.019	52.63	0



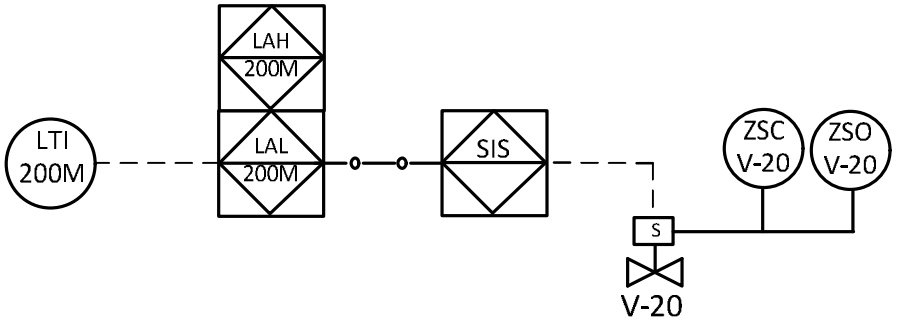
Lazo 200L

SIL	PFD	RRF	HFT
1	0.019	52.63	0



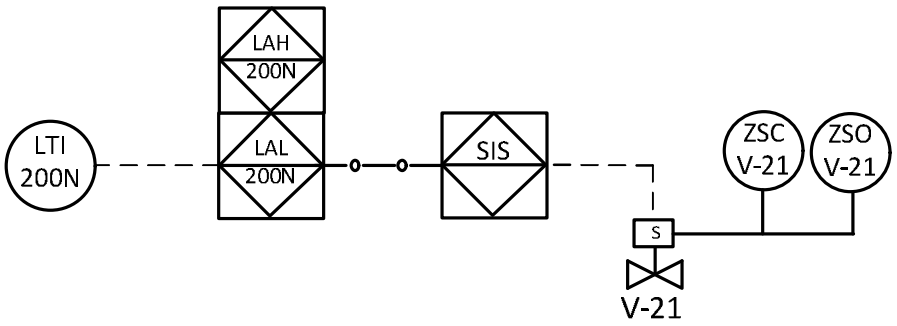
Lazo 200M

SIL	PFD	RRF	HFT
1	0.019	52.63	0



Lazo 200N

SIL	PFD	RRF	HFT
1	0.019	52.63	0



Otro factor importante que hay que determinar es la tolerancia de falla del hardware (Hardware Fault Tolerance, HFT). Según la norma IEC 61511 la tolerancia de falla se define como la capacidad para llevar a cabo la función de seguridad requerida en la presencia de uno o más fallos peligrosos, en muchos casos, se impone redundancia al hardware para compensar cualquier deficiencia con el fin de cumplir con el SIL objetivo.

La norma IEC 61511 estable ce la tolerancia a fallas del hardware tanto para el solucionador lógico (Tabla 4.4.2.1), los sensores y los elementos finales (Tabla 4.4.2.2) en función del SIL correspondiente al lazo en el cual actúan dichos elementos.

SOLUCIONADOR LÓGICO			
	Tolerancia a Fallas del Hardware		
SIL	SFF<60%	SFF 60% a 90%	SFF>90%
1	1	0	0
2	2	1	0
3	3	2	1
4	Revisar Norma IEC 61508		

Tabla 4.4.2.1 *Tolerancia a fallas para solucionador lógico.*

La tolerancia a fallas del hardware de "n" significa que "n+1" fallas va a evitar que la acción de seguridad ocurra, por ejemplo, para una aplicación SIL 2, un solucionador lógico con una SFF entre 60% y 90% requerirá una tolerancia a fallas del hardware mínimo de 1. Esto significa que por lo menos debe tener redundancia doble, es decir, tolera una falla.

SENSORES Y ELEMENTOS FINALES	
SIL	**Tolerancia a Fallas del Hardware**
1	0
2	1
3	2
4	Revisar Norma IEC 61508

Tabla 4.4.2.2 *Tolerancia a fallas para sensores y elementos finales.*

A primera vista, la tabla anterior es extremadamente restrictiva. Para una función de seguridad SIL 2 la tolerancia a fallas del hardware es de 1, lo que implica sensores o elementos finales redundantes.

Con los cálculos de los lazos de seguridad previamente realizados y con la HFT determinada, se realizó el P&ID del sistema con toda la instrumentación necesaria para que el SIS desempeñe la función deseada. (Anexo 4).

4.4.3 DIAGRAMAS DE BLOQUES DE LOS LAZOS DE SEGURIDAD.

Los lazos de seguridad con SIL 1, están representados por el siguiente diagrama de bloques que se muestra en la figura 4.3.3.1, mientras que los lazos correspondientes a SIL 2 se representan como lo indica la figuna 4.3.3.2.

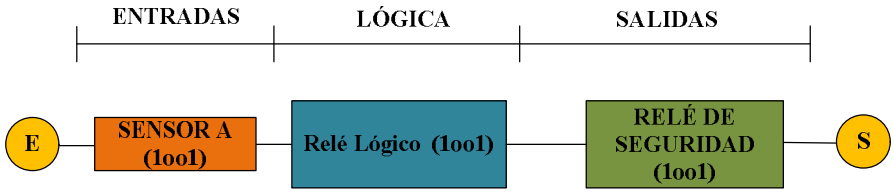


Figura 4.3.3.1 *Diagrama de bloques para configuración 1oo1 (Control de Temperatura y flujo).*

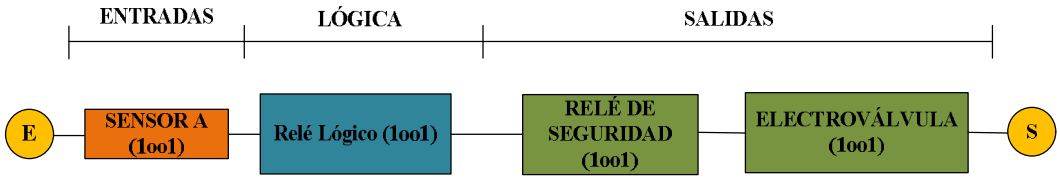


Figura 4.3.3.2 *Diagrama de bloques para configuración 1oo1 (Control de Nivel en Tanques de Almacenamiento Secundarios).*

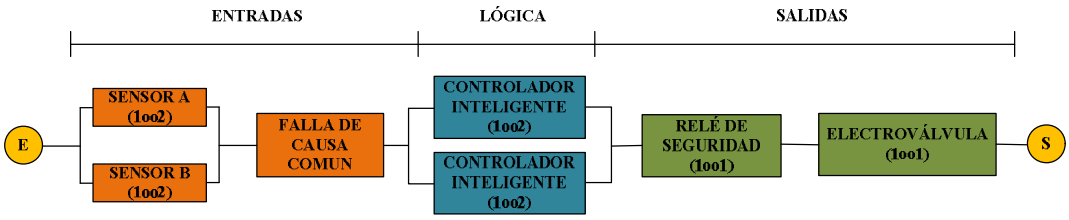


Figura 4.3.3.3 *Diagrama de bloques para configuración 1oo2 (Control de Nivel en Tanques de Almacenamiento Primario).*

La configuración 1oo2 es utilizada únicamente en los lazos de seguridad que están relacionados con el control de nivel en los tanques de almacenamiento primario (Búnker y Diésel).

4.5 Arquitectura del sistema de seguridad.

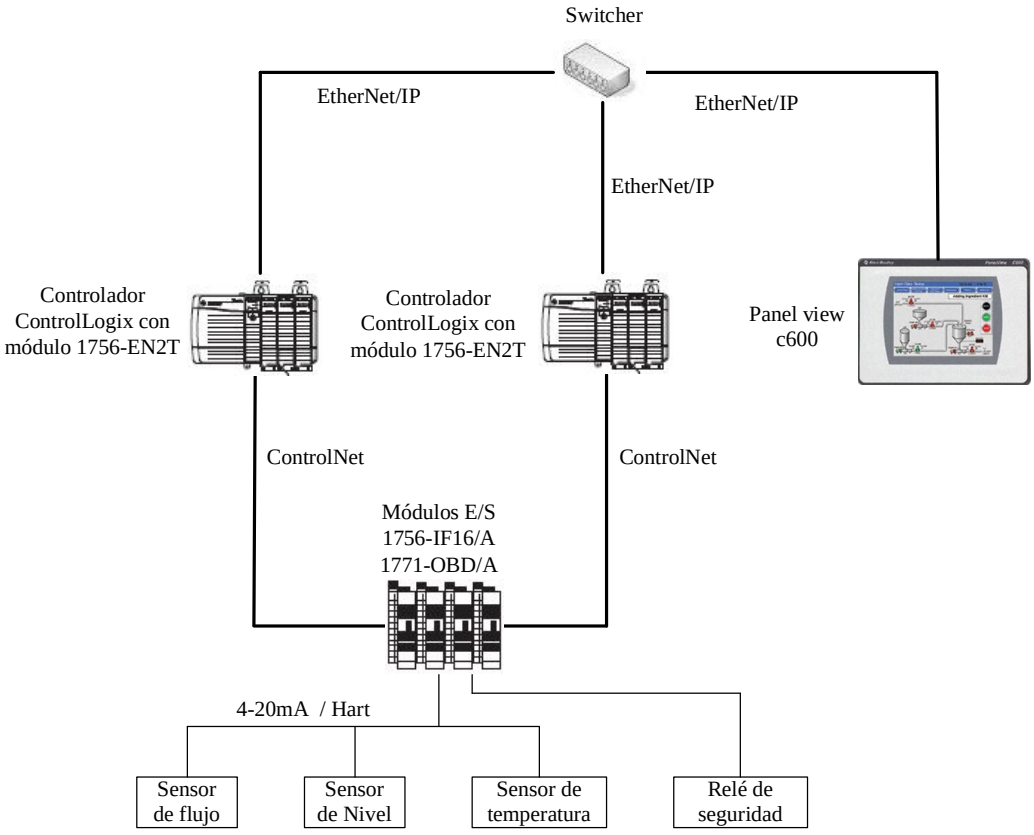


Figura 4.5.1 *Arquitectura del SIS.*

La comunicación entre los PLC's de seguridad y el dispositivo HMI se realiza mediante protocolo EtherNet/IP, para ello es necesario instalar módulo de comunicación 1756-EN2T. Los módulos de entradas y salidas se comunican con los controladores lógicos mediante el protocolo ContolNet. Ya que los elementos de campo proveen señales eléctricas de 4-20 mA, se ha considerado el protocolo HART para la comunicación de dichos elementos.

4.6 Elementos a utilizar para implementación de SIS.

Item	Descripción	Cantidad	Precio	Total
ControlLogix 1756-A7	Chasis para ensamblaje	1	634.80	634.80
ControlLogix 1756-L61	PLC de seguridad	2	7776	15552
ControlLogix 13-32 V DC 10A	Fuente de alimentación	2	1093.20	2186.40
ControlLogix 1756-IF16/A	Módulo de entradas analógicas	2	1620	3260
ControlLogix 1756-IA32I	Módulo de entradas digitales	2	733.20	1466.40
ControlLogix 1771-OBD/A	Módulo de salidas digitales	1	1188	1188
ControlLogix comunicación Ethernet/IP 1756-EN2T/A	Módulo de comunicación Ethernet	2	982.80	1965.60
ControlLogix comunicación controlNet 1756-CN2	Módulo de comunicación controlNet	2	2604	5208
ControlLogix 1756-RM	Módulo de redundancia	1	4625	4625
Allen-Bradley 2711C-T6T PanelView C600	Pantalla de diagnóstico	1	908.40	908.40
Rockwell MSR121RT	Relé de seguridad	24	405.60	9734.40

OMEGA FP85A	Transmisor de flujo	16	445.20	7123.20
INOR C520S	Transmisor de temperatura	1	395.47	395.47
MAGNETROL 705	Transmisor de nivel	8	522.84	4182.72
M&M International D225DBJ	Válvula de seguridad	4	896	3584
Cable multipar STP	Cable para conexión de sensores y procesadores lógicos	1200 mts	1.20	1440

El layout de la disposición de elementos en el armario de control se muestra en el anexo 6.

4.7 Configuración de controlLogix para aplicaciones SIL 2

Los sistemas controlLogix con certificación SIL2 se pueden utilizar en configuraciones redundantes o no-redundantes. Los distintos niveles de disponibilidad que se puede lograr mediante el uso de diferentes configuraciones del sistema ControlLogix se refieren a prueba de fallos, alta disponibilidad o tolerancia a fallas [37].

1.Configuración de falla segura

En la configuración de falla segura, el hardware utilizado en el circuito de seguridad no es redundante. Por lo tanto, si se produce un fallo en cualquier parte del sistema de SIL2, el sistema está programado para fallar de forma segura. La falla segura es típicamente un apagado de emergencia.

2.Configuración de alta disponibilidad.

En la configuración de alta disponibilidad, el controlador y el chasis de comunicaciones son tolerante a fallas, pero el módulo remoto de entradas y salidas no lo es. En esta configuración, si una falla ocurre en el chasis primario o secundario, el sistema puede continuar desempeñando la función de seguridad requerida. Si una falla tiene lugar en el módulo de E/S remotas, el sistema falla de forma segura (Figura 4.7.1).

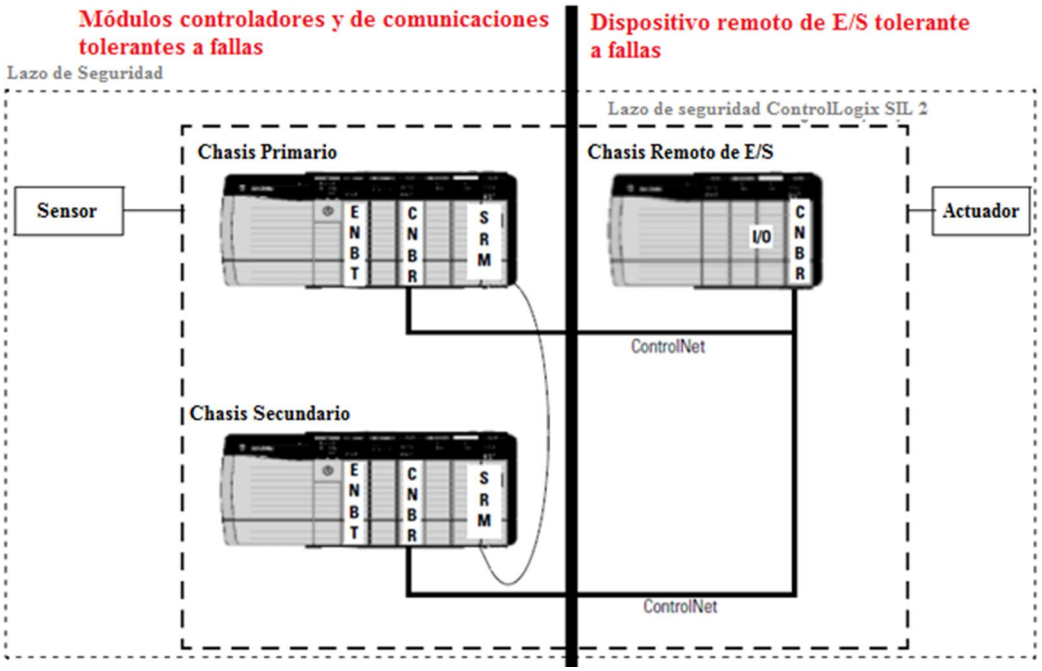


Figura 4.7.1 *Topología para configuración de alta disponibilidad [37].*

3.Configuración de tolerancia a fallas

La norma IEC 61508-4 define la tolerancia a fallos como "la capacidad de una unidad funcional de continuar realizando una función requerida en la presencia de fallas o errores."

La configuración tolerante a fallas es más eficiente que la configuración de alta disponibilidad debido a que el chasis de E/S remotas es configurado como tolerante a fallas. Un sistema ControlLogix SIL2 tolerante a fallas es alcanzado mediante el uso de chasis de comunicaciones y controlador redundantes, chasis redundante de E/S remotas, placas terminales de E/S especializadas y la aplicación de programación especial.

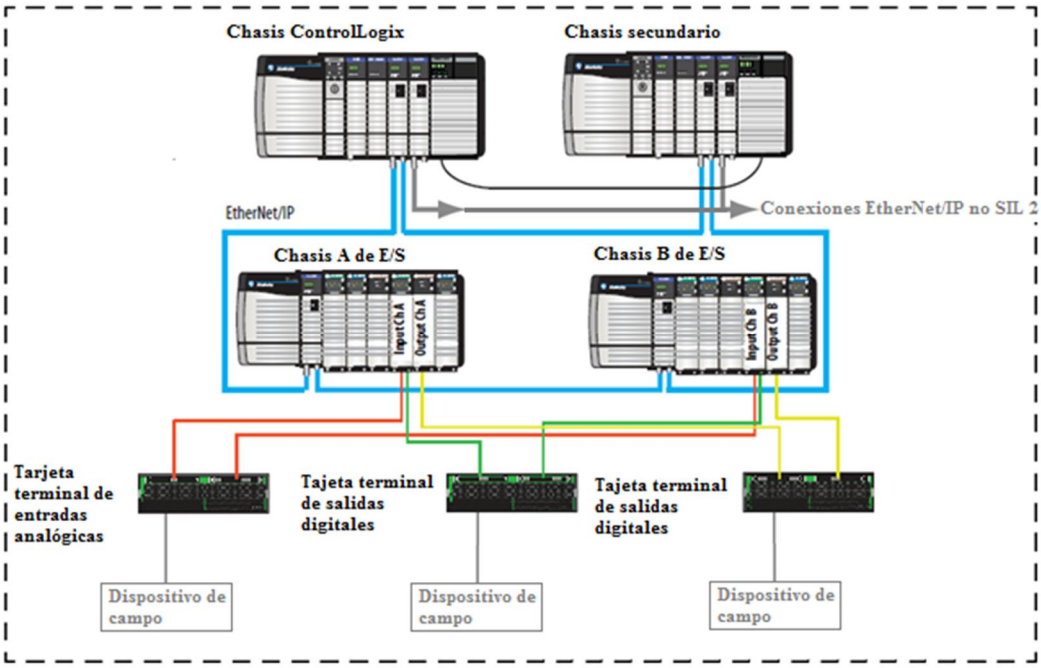


Figura 4.7.2 *Topología para configuración tolerante a fallas [37].*

Para el sistema diseñado, la configuración de alta disponibilidad (Figura 4.7.1) es la opción más favorable debido principalmente a costos, ya que dicha configuración dispone de elementos redundantes únicamente en la etapa de control. Esto implica un ahorro significativo en la implementación del sistema ya que la utilización de elementos de campo redundantes eleva su costo inicial. El proceso de distribución de combustible dentro de la planta de análisis trabaja de forma continua permanentemente, por ello el sistema debe evitar que el proceso se detenga ya que esto genera pérdidas económicas considerables a la empresa.

El principal inconveniente con esta configuración se da en los elementos de campo ya que si uno de estos dispositivos falla, no podrá ejecutar su función en el caso de un evento inesperado. Es decir, en lo que respecta a las SIF estas actuarán según lo esperado pero los elementos finales deben ser sometidos a mantenimiento periódico para asegurar su disponibilidad bajo demanda.

4.8 Etapas finales del ciclo de vida del SIS

Debido a que el presente trabajo consiste en el diseño del SIS, las etapas posteriores correspondientes a la instalación, validación, pruebas, modificaciones y desmantelamiento, serán únicamente analizadas, es decir, se detallarán sus objetivos y requerimientos principales. Para ello se ha tomado como referencia a la descripción de cada etapa mostrada en la norma IEC 61511 [4].

4.8.1 Instalación [4]

Objetivos

- Instalar el SIS de acuerdo a las especificaciones y diagramas.
- Poner en servicio el SIS de tal manera que esté listo para la validación final del sistema.

Requerimientos

1. La planificación de la instalación y puesta en servicio debería definir las actividades a realizar. La planificación debería proveer la información sobre:

    - Actividades de instalación y comisionamiento.
    - Los procedimientos, medidas y técnicas a ser utilizadas para la instalación y comisionamiento.
    - Cuándo tendrán lugar estas actividades.
    - Las personas, departamentos y organizaciones responsables de estas actividades.

2. La planificación de instalación y puesta en servicio debería ser integrada a lo largo de toda la planificación del proyecto.

3. Todos los componentes del SIS deberán instalarse correctamente de acuerdo con el diseño y el plan de instalación.

4. El SIS será puesto en servicio de conformidad con la planificación de la preparación para la validación final del sistema. Las actividades de puesta en marcha deberán incluir, pero no limitarse a, la confirmación de los siguientes puntos:

- Puesta a tierra conectada correctamente.
- Fuentes de energía conectadas correctamente y en funcionamiento.
- Paradas de transporte y materiales de embalaje hayan sido retirados.
- Ningún daño físico presente.
- Todos los instrumentos han sido debidamente calibrados.
- Todos los dispositivos de campo están en funcionamiento.
- Solucionador lógico, entradas y salidas operativos.

5. Un apropiado registro de la puesta en marcha del SIS debería realizarse, estableciendo los resultados de las pruebas, si los objetivos y el criterio en la fase de diseño son alcanzados. Si hay una falla, las razones que originaron la falla deben ser registradas.

4.8.2 Validación del SIS [4]

Objetivos

El objetivo de los requerimientos en esta etapa es validar, a través de inspección y pruebas, que el SIS instalado y puesto en servicio así como sus SIF asociadas, alcancen los requerimientos establecidos en la SRS.

Requerimientos

1. La planificación de la validación del SIS deberá definir todas las actividades necesarias para su validación. Los siguientes temas serán incluidos.

    - Las actividades de validación, incluyendo la validación del SIS con respecto a la SRS.
    - La validación de todos los modos de funcionamiento pertinentes del proceso y sus equipos auxiliares, incluidas las:

        - Preparación para su uso, incluyendo ajustes y configuración.
        - Estados de operación de arranque, automático, manual, semi-automático.

    - Los procedimientos, las medidas y las técnicas que se utilizarán para la validación.
    - Cuando estas actividades se llevarán a cabo.

- Las personas, departamentos y organizaciones responsables de estas actividades y los niveles de independencia para las actividades de validación.
- Hacer referencia a la información contra la que la validación se llevará a cabo.

2. Planificación adicional de validación para el software de aplicación de seguridad incluirá lo siguiente.

    - La identificación del software de seguridad que debe ser validado para cada modo de operación del proceso antes de que la puesta en marcha comience.
    - Información sobre la estrategia técnica para la validación que deberá incluir:

        - Técnicas manuales y automáticas.
        - Técnicas estáticas y dinámicas.
        - Técnicas analíticas y estadísticas.

    - Las técnicas de medidas y los procedimientos que deberían utilizarse para confirmar que cada SIF cumple con los requerimientos del software de las SIF.
    - El ambiente requerido en el cual tengan lugar las actividades de validación.
    - Los criterios de aprobación / falla para llevar a cabo la validación de software, incluyendo:

        - El proceso y las señales de entrada de operador que se requieren con sus secuencias y sus valores.
        - Las señales de salida previstas con sus secuencias y sus valores.
        - Otros criterios de aceptación, por ejemplo, uso de memoria, tiempo y valor de tolerancia.

    - Las políticas y procedimientos para la evaluación de los resultados de la validación, en particular los fracasos.

3. Cuando se requiere precisión de la medición como parte de la validación, los instrumentos utilizados para esta función deben ser calibrados con respecto a una especificación referida a un estándar dentro de una incertidumbre adecuada a la

aplicación. Si esta calibración no es posible, deberá utilizarse un método alternativo y documentado.

4. La validación del SIS y su SIF asociada se llevarán a cabo de acuerdo con la planificación de validación del SIS. Las actividades de validación deberán incluir, pero no limitarse a, lo siguiente:

    - El SIS se desempeña bajo los modos de funcionamiento normales y anormales (por ejemplo, la puesta en marcha, parada) como se identifican en la SRS.
    - La confirmación de que la interacción adversa del BPCS con otros sistemas conectados no afecta al funcionamiento apropiado del SIS.
    - El SIS se comunica correctamente (cuando sea necesario) con el BPCS o cualquier otro sistema o red.
    - Sensores, solucionador lógico y elementos finales actúan de conformidad con la SRS, incluyendo todos los canales redundantes.
    - La documentación del SIS es coherente con el sistema instalado.
    - La confirmación de que la SIF funciona según lo especificado en los valores variables del proceso no válido (por ejemplo, fuera de alcance).
    - La adecuada secuencia de apagado sea activada.
    - El SIS ofrece el anuncio adecuado y buen funcionamiento en pantalla.
    - Los cálculos que se incluyen en el SIS son correctos.
    - Las funciones de re-inicio del SIS actúan como se definió en la SRS.
    - Las funciones de bypass funcionan correctamente.
    - Las anulaciones de arranque funcionan correctamente.
    - El apagado manual de los sistemas funciona correctamente.
    - Los intervalos de prueba son documentados en los procedimientos de mantenimiento.
    - La acción de funciones de alarma de diagnóstico es requerida.
    - La confirmación de que la inmunidad electromagnética especificada en la SRS ha sido alcanzada.

5. La validación del software debería mostrar que todas las especificaciones de seguridad del software son correctamente desempeñadas, y que el software no pone en peligro los requerimientos de seguridad bajo condiciones de falla del SIS y modos degradados de operación por ejecución de software no definido en la SRS. La información de las actividades de validación debería ser disponible.

6. Se produce información adecuada de los resultados de la validación del SIS que proporciona:

    - La versión de la planificación de validación SIS siendo utilizada.
    - La SIF bajo prueba, junto con la referencia específica a las exigencias identificadas durante la planificación de validación del SIS.
    - Herramientas y equipos utilizados, junto con los datos de calibración.
    - Los resultados de cada prueba.
    - La versión de la especificación de prueba utilizada.
    - Los criterios para la aceptación de las pruebas de integración.
    - La versión del hardware y el software que está siendo probado en el SIS.
    - Cualquier discrepancia entre los resultados esperados y los reales.
    - El análisis realizado y las decisiones adoptadas sobre la conveniencia de continuar la prueba o emitir una solicitud de cambio, en el caso de que se produzcan discrepancias.

7. Cuando ocurren discrepancias entre los resultados esperados y los reales, el análisis hecho y las decisiones tomadas sobre la conveniencia de continuar con la validación o emitir una solicitud de cambio y retornar a la primera parte del desarrollo del ciclo de vida, deberían estar disponibles como parte de los resultados de la validación de seguridad.

8. Después de la validación del SIS y antes de identificar los peligros que están presentes, las siguientes actividades se llevarán a cabo:

    - Todas las funciones de bypass (por ejemplo, alarmas anuladas) serán devueltas a su posición normal.
    - Todas las válvulas de aislamiento del proceso se fijarán de acuerdo con los requisitos y procedimientos del proceso de puesta en marcha.
    - Todos los materiales de prueba (por ejemplo, fluidos) será eliminado.

4.8.3 Operación y Mantenimiento del SIS [4]

Objetivos

- Asegurar que el SIL requerido de cada SIF se mantiene durante la operación y mantenimiento.

- Operar y mantener el SIS de manera que se mantenga la seguridad funcional diseñada.

Requerimientos

1. La planificación de la operación y el mantenimiento del SIS se llevará a cabo. Esto proveerá lo siguiente:

    - Actividades de rutina y operación anormal.
    - Actividades de pruebas, mantenimiento preventivo y correctivo.
    - Verificación del cumplimiento de los procedimientos de operación y mantenimiento.
    - Cuando tienen lugar estas actividades.
    - Las personas, departamentos y organizaciones responsables de esas actividades.

2. Los procedimientos de operación y mantenimiento serán desarrollados de acuerdo con la planificación de seguridad relevante y proveerán lo siguiente:

    - Las acciones rutinarias que se necesitan llevar a cabo para mantener la seguridad funcional del SIS como "fue diseñada", por ejemplo, siguiendo los intervalos de prueba definidos por la determinación del SIL.
    - Las acciones y restricciones que son necesarias para prevenir un estado inseguro y/o reducir las consecuencias de un evento peligroso durante la operación o mantenimiento (por ejemplo, cuando un sistema necesita ser anulado para pruebas o mantenimiento, que pasos adicionales de mitigación serán implementados).
    - La información que se necesita mantener en caso de falla del sistema y las tasas de la demanda del SIS.
    - La información mantenida que muestra los resultados de las auditorías y pruebas en el SIS.
    - Los procedimientos de mantenimiento a ser seguidos cuando ocurren fallas en el SIS, incluyendo:

        - Procedimientos para diagnóstico de fallas y reparación.
        - Procedimientos para revalidación.
        - Requerimientos de reportes de mantenimiento.
        - Procedimientos para hacer seguimiento del desempeño de mantenimiento.

- Asegurar que el equipo utilizado durante las actividades de mantenimiento es apropiadamente calibrado.

3. La operación y el mantenimiento deberán proceder de acuerdo con los procedimientos relevantes.

4. Los operadores serán entrenados en el funcionamiento y operación del SIS en sus áreas. Este entrenamiento asegurará lo siguiente:

    - Comprenden cómo funciona el SIS (puntos de activación y las acciones resultantes que son tomadas por el SIS).
    - El peligro del cual los protege el SIS.
    - La operación de todos los interruptores de bypass y bajo qué circunstancias estos interruptores son activados.
    - La operación de algunos interruptores de apagado y encendido manual, así como cuando estos interruptores son activados.
    - Expectativas sobre la activación de las alarmas de diagnóstico (por ejemplo, ¿Qué acción se tomará cuando se activa alguna alarma del SIS indicando que hay un problema?).

5. El personal de mantenimiento debe ser entrenado según sea necesario para mantener el rendimiento funcional completo del SIS (hardware y software).

6. Se analizarán las discrepancias entre el comportamiento esperado y el comportamiento real de la SIS y, en su caso, las modificaciones hechas de tal manera que se mantenga la seguridad requerida. Esto incluirá el seguimiento de lo siguiente:

    - Las acciones adoptadas a raíz de una demanda en el sistema;
    - Las fallas en los equipos que forman parte del SIS establecidas durante las pruebas de rutina o bajo demanda real.
    - La causa de las demandas.
    - la causa de las falsas demandas.

7. Los procedimientos de operación y mantenimiento pueden requerir revisión, debido a lo siguiente:

    - Auditorias de la seguridad funcional.
    - Pruebas del SIS.

8. Procedimientos de prueba escritos se desarrollarán para cada SIF para revelar fallas peligrosas detectadas por diagnóstico. Estos procedimientos de prueba deberán describir cada paso que se va a realizar y deberá incluir:

    - La correcta operación de cada sensor y elemento final.
    - Acción lógica correcta.
    - Alarmas e indicaciones correctas.

4.8.4 Pruebas [4]

1. Pruebas de comprobación periódicas se llevarán a cabo mediante un procedimiento escrito para revelar fallas no detectadas que impidan que el SIS operen de acuerdo con la SRS.

2. El SIS completo deberá ser probado incluyendo sensores, solucionador lógico y los elementos finales.

3. La frecuencia de las pruebas deberá decidirse considerando el cálculo de la PFD promedio.

4. Cualquier deficiencia encontrada durante la prueba deberá ser reparada en forma segura y a tiempo.

5. En algún intervalo periódico (determinado por el usuario), la frecuencia de prueba será re-evaluado en base a varios factores, incluyendo los datos históricos de la prueba, las experiencias en la planta, la degradación del hardware y la fiabilidad del software.

6. Cualquier cambio en la lógica de la aplicación requiere una prueba completa. Se permiten excepciones a este caso si una revisión apropiada y pruebas parciales son llevadas a cabo para asegurar que los cambios fueron realizados correctamente.

4.8.4.1 Inspección

Cada SIS será periódicamente inspeccionado visualmente para asegurarse de que no hay modificaciones no autorizadas y no existe deterioro observable (por ejemplo, tornillos faltantes o tapas de instrumentos, soportes oxidados, cables abiertos, conductos rotos y aislamiento faltante).

4.8.4.2 Documentación de pruebas e inspección

El usuario deberá mantener registros que certifican que las pruebas a e inspecciones fueron completadas según sea requerido. Estos registros deben incluir la siguiente información como mínimo:

- Descripción de las pruebas e inspecciones realizadas.
- Las fechas de las pruebas e inspecciones.
- Nombre de la persona(s) que desempeñó las pruebas e inspecciones;
- El número de serie u otra identificación única del sistema de prueba (por ejemplo, número de lazo, número de etiqueta, número de equipo, y el número de la SIF).
- Los resultados de las pruebas e inspección (por ejemplo, condiciones de "cómo se encuentra", "cómo se dejó").

4.8.5 Modificación [4]

Objetivos

- Las modificaciones para cualquier SIS son planeadas adecuadamente, revisadas y previamente aprobadas para hacer los cambios.
- Asegurar que la integridad de la seguridad requerida del SIS se mantiene a pesar de los cambios realizados.

Requerimientos

1. Antes de llevar a cabo cualquier modificación de un SIS, deberán realizarse procedimientos de autorización y el control de los cambios.

2. Los procedimientos deben incluir un método claro de identificación y solicitud del trabajo a realizar, así como los riesgos que podrían afectar.

3. Un análisis debe llevarse a cabo para determinar el impacto en la seguridad funcional como resultado de la modificación propuesta. Cuando el análisis muestra que la modificación propuesta tendrá un impacto en la seguridad entonces se retorna a la primera fase del ciclo de vida de seguridad afectada por la modificación.

4. La actividad de modificación no se iniciará sin la debida autorización.

5. La información adecuada se mantiene para todos los cambios en el SIS. La información incluirá:

    - Una descripción de la modificación o cambio.
    - La razón para el cambio;
    - Peligros identificados que pueden verse afectados.
    - Un análisis del impacto de la actividad de modificación en el SIS.
    - Todas las aprobaciones necesarias para los cambios;
    - Pruebas utilizadas para verificar que el cambio fue implementado correctamente y el SIS trabaja como es requerido.
    - Un apropiado historial de configuración.
    - Pruebas utilizadas para verificar que el cambio no ha afectado negativamente a las partes del SIS que no se han modificado.

6. La modificación se realizará con personal cualificado que han sido debidamente capacitados. Todo el personal afectado y apropiados deben ser notificados del cambio y capacitación en relación con el cambio.

4.8.6 Decomisionamiento (Desinstalación) [4]

Objetivos

- Asegurar de que antes de la desinstalación de cualquier SIS del servicio activo, una adecuada revisión se lleva a cabo y se obtiene la autorización requerida.
- Garantizar que las SIF permanezcan operacionales durante las actividades de desinstalación.

Requerimientos

1. Antes de llevar a cabo cualquier desmantelamiento de un SIS, deben realizarse procedimientos de autorización y el control de los cambios.

2. Los procedimientos deben incluir un método claro de identificar y solicitar el trabajo a realizar, así como identificar los peligros que podrían afectar.

3. Un análisis se llevará a cabo sobre el impacto en la seguridad funcional como resultado de la actividad de desmantelamiento. La evaluación incluirá una actualización de la evaluación de peligros y riesgos suficiente para determinar la amplitud y profundidad que deberá ser retomada en fases subsecuentes del ciclo de vida. La evaluación también tendrá en cuenta:

    - La seguridad funcional durante la ejecución de las actividades de desmantelamiento.
    - El impacto de la puesta fuera de servicio de un SIS vinculado a la seguridad en las unidades operativas adyacentes y servicios de la infraestructura.

4. Los resultados del análisis de impacto se utilizarán durante la planificación de seguridad para volver a activar los requisitos de esta norma, incluyendo re-verificación y re-validación.

5. Las actividades de puesta fuera de servicio no se iniciarán sin la debida autorización.

Algunos ejemplos de checklist desarrollados para las etapas antes descritas se muestran en el anexo 5 [10].

4.9 Justificación del SIS.

Se requiere del conocimiento del personal de ingeniería de sistemas de control para justificar un sistema de seguridad debido a que poseen los datos de costos para la instalación del sistema de seguridad y operación, dicha justificación puede basarse en un análisis de costo-beneficio, en donde, los costos incluyen la ingeniería, adquisición, instalación, operación y mantenimiento del sistema, mientras que los beneficios son el ahorro de costos asociados a la reducción del número de lesiones, incidentes y pérdida de producción [10].

La justificación de cualquier sistema generalmente se realiza en base a un análisis financiero, en el cual se considera la forma en la que el valor del dinero varía con el tiempo.

El valor futuro del dinero (*Future Value*, FV) varía con el tiempo así como la tasa de interés. Si uno realiza una inversión anual fija M, el valor futuro de la inversión después de N años, a una tasa de interés R, puede ser expresada como:

$$FV = M\frac{[1+R]^N-1}{R} \qquad (4.4.1)$$

También se puede calcular el valor actual (*Present Value*, PV) de inversiones hechas en intervalos fijos en el futuro. Si se realiza una inversión anual fija M por N años, a una tasa de interés R, el valor actual de la inversión puede expresarse como:

$$PV = M\frac{1-[1+R]^N}{R} \qquad (4.4.2)$$

Al justificar un sistema de seguridad, la atención se centra en el valor actual del dinero en base a las pérdidas que se pueden cuantificar en forma anual durante varios años. Es decir, se puede calcular el impacto de un evento peligroso y/o falsas activaciones sobre una base anual, calcular el valor actual de las pérdidas futuras y determinar el gasto límite para el sistema de seguridad. La idea fundamental es justificar si los beneficios son mayores al costo, caso contrario dicha justificación es cuestionable [10].

4.9.1 Costos del ciclo de vida.

Una forma de justificar un gasto del sistema de seguridad es completar un análisis de costo del ciclo de vida de las diversas opciones que se están considerando.

Los costes del ciclo de vida reflejan el costo total de propiedad del sistema. Mediante el cálculo de los costos del ciclo de vida, las diversas opciones se pueden analizar de una manera más cuantitativa y consistente. La Tabla 4.4.1.1 describe los costos predominantes incurridos durante la vida de un sistema de seguridad. La lista se divide en costos fijos iniciales (Ej. los costos para el diseño, adquisición, instalación, puesta en marcha y operación del sistema), y los costos anuales (Ej. mantenimiento y otros costos actuales relacionados con el sistema). En cierta medida, los costos reflejan los puntos enumerados en el modelo de ciclo de vida analizado en el Capítulo 1 [10].

Ítem de Costo	Comentarios
Costos Iniciales	
Determinación del SIL	Costos que competen a la determinación del SIL.
Requerimientos de seguridad y especificaciones de diseño	Costos por el diseño detallado completo e ingeniería.
Diseño detallado e ingeniería	Costos de mano de obra para completar las especificaciones de requisitos de seguridad, el diseño conceptual y especificaciones de diseño detallados.
Sensores	Costos de compra de sensores
Elementos Finales	Costos de compra de válvulas y otros elementos finales.
Sistema Lógico	Costos de compra del sistema lógico.
Misceláneos: Cableado, alimentación, interface de operador.	Costos para otros equipos requeridos para instalar y monitorear el sistema de seguridad.
Entrenamiento inicial	Costos de entrenamiento, operación y personal de soporte para diseñar, instalar y probar el sistema.
FAT/Instalación/PSAT	Costos de pruebas de aceptación en la fábrica, instalación de equipos y pruebas de pre-arranque.
Inicio y corrección	Muchos sistemas requieren alguna corrección para operar a total capacidad.
Costos Anuales	
Formación continua	Cursos de actualización permanente para el personal de operaciones y de apoyo.
Cambios de ingeniería	Estos costos pueden ser significantes

	debido a requisitos de revisión y actualizaciones.
Contrato de Servicio	El sistema lógico programable usualmente requiere un contrato de mantenimiento de acuerdo al fabricante para resolver problemas “difíciles”.
Costos de reparación y mantenimiento	Programas de mantenimiento preventivo
Repuestos	Partes críticas son recomendadas por los fabricantes.
Pruebas en línea	Pruebas periódicas llevadas a cabo por personal de operaciones y soporte.
Costos de Reparación	Costos por reparación o reemplazo de módulos defectuosos basados en tasa predictiva de fallas.
Costos de riesgo	Costos basados en el análisis de riesgos. La tasa de riesgo es una función de la PFD del sistema y la tasa de demanda.
Valor actual por costos anuales	El valor presente de los costos anuales basados en las tasas de interés actuales y la vida prevista del sistema. Estos costos se suman a los costos fijos iniciales para obtener el valor actual de todos los costos.
Costos totales del ciclo de vida	Costos totales por la vida del sistema. Esta es la suma de los costos iniciales y el valor actual de los costos anuales.

4.9.2 Costos de lazos de seguridad.

Para el cálculo de los costos de inicio se han considerado los siguientes valores por hora:

- Ingeniero líder: $250/hora
- Ingeniero de desarrollo: $180/hora
- Ayudantes y dibujantes: $100/hora

El tiempo de vida del sistema de seguridad es de 20 años con una tasa de interés del 5%.

Debido a que algunos lazos de seguridad son iguales, el cálculo se realizará sobre uno de ellos y se considerará la cantidad de lazos existentes en el sistema.

Para todos los lazos en común se determinaron los siguientes costos iniciales:

	Material	Trabajo	Costo total	Subtotal
Costos Iniciales				
Determinación del SIL		2 000	2 000	
SRS/especificaciones de diseño		3 500	3 500	
Sistema Lógico		7 776	7 776	
Diseño detallado e ingeniería		10 000	10 000	
Entrenamiento inicial		1 230	1 230	
FAT/Instalación/PSAT	2 500	5 000	7 500	
Subtotal de costos fijos				**32 006**

Lazos de seguridad correspondiente a control de flujo:

1. Lazo 100A
2. Lazo 100C
3. Lazo 100E
4. Lazo 100G
5. Lazo 100H
6. Lazo 100I
7. Lazo 200A
8. Lazo 200C
9. Lazo 200E
10. Lazo 200F
11. Lazo 200G
12. Lazo 200H
13. Lazo 200I
14. Lazo 200J

	Material	Trabajo	Costo total	Subtotal	Total lazos
Costos Iniciales					
Sensores	445.20		445.20		
Elementos Finales	405.60		405.60		
Sistema Lógico					
Misceláneos: Cableado, alimentación, interface de operador.	80		80		
Subtotal de costos fijos				**930.80**	**13 031.20**
Costos Anuales					
Formación continua		135	135		
Cambios de ingeniería					
Contrato de Servicio					
Costos de reparación y mantenimiento		70	70		
Repuestos	150		150		
Pruebas en línea		200	200		
Costos de Reparación	150		150		
Costos de riesgo					
Subtotal de costos				**705**	**9 870**
Valor actual por costos anuales (20 años, tasa de interés 5%)				**8 785.86**	**123 002**
Costos total del ciclo de vida				**9716.66**	**136 033.22**

Lazos de seguridad correspondiente a control de nivel en tanques primarios:

1. Lazo 100B
2. Lazo 100F
3. Lazo 200B
4. Lazo 200F

	Material	**Trabajo**	**Costo total**	**Subtotal**	**Total lazos**
Costos Iniciales					
Sensores	522.84		522.84		
Elementos Finales	1 301.60		1 301.60		
Sistema Lógico					
Misceláneos: Cableado, alimentación, interface de operador.	80		80		
Subtotal de costos fijos				**1 904.44**	**7 617.76**
Costos Anuales					
Formación continua		120	120		
Cambios de ingeniería					
Contrato de Servicio					
Costos de reparación y mantenimiento		250	250		
Repuestos	375		375		
Pruebas en línea		200	200		
Costos de Reparación	250		250		
Costos de riesgo					
Subtotal de costos				**1 195**	**4 780**
Valor actual por costos anuales (20 años, tasa de interés 5%)				**14 892.34**	**59 569.37**
Costos total del ciclo de vida				**16 796.78**	**67 186.13**

Lazos de seguridad correspondiente a control de temperatura:

Lazo 100D

	Material	**Trabajo**	**Costo total**	**Subtotal**
Costos Iniciales				
Sensores	840.67		840.67	
Elementos Finales	1 301.60		1 301.60	
Sistema Lógico				
Misceláneos: Cableado, alimentación, interface de operador.	80		80	
Subtotal de costos fijos				**2 222.27**
Costos Anuales				
Formación continua		200	200	
Cambios de ingeniería				
Contrato de Servicio				
Costos de reparación y mantenimiento		400	400	
Repuestos	500		500	
Pruebas en línea		200	200	
Costos de Reparación	600		600	
Costos de riesgo				
Subtotal de costos				**1 900**
Valor actual por costos anuales (20 años, tasa de interés 5%)				**23 678.19**
Costos total del ciclo de vida				**25 900.47**

Lazos de seguridad correspondiente a control de nivel en tanques secundarios:

1. Lazo 200K
2. Lazo 200L
3. Lazo 200M
4. Lazo 200N

	Material	**Trabajo**	**Costo total**	**Subtotal**	**Total lazos**
Costos Iniciales					
Sensores	522.84		522.84		
Elementos Finales	1 301.60		1 301.60		
Sistema Lógico					
Misceláneos: Cableado, alimentación, interface de operador.	80		80		
Subtotal de costos fijos				**1 904.44**	**7 617.76**
Costos Anuales					
Formación continua		125	125		
Cambios de ingeniería					
Contrato de Servicio					
Costos de reparación y mantenimiento		200	200		
Repuestos	350		350		
Pruebas en línea		200	200		
Costos de Reparación	250		250		
Costos de riesgo					
Subtotal de costos				**1 125**	**4 500**
Valor actual por costos anuales (20 años, tasa de interés 5%)				**14 019.99**	**56 079.95**
Costos total del ciclo de vida				**15 924.43**	**63 637.71**

El costo total de todos los lazos de seguridad incluyendo los costos iniciales se muestra a continuación:

	Material	**Trabajo**	**Costo total**	**Subtotal**
Costos Iniciales				
Subtotal de costos de ingeniería	2 500	29 506	**32 006**	
Subtotal de costos fijos (Lazos de control de Flujo)	13 031.20		**13 031.20**	
Subtotal de costos fijos (Lazos de control de nivel primario)	7 617.76		**7 617.76**	
Subtotal de costos fijos (Lazos de control de temperatura)	2 222.27		**2 222.27**	
Subtotal de costos fijos (Lazos de control de nivel secundario)	7 617.76		**7 617.76**	
Subtotal costos iniciales				**62 475.99**
Costos Anuales				
Subtotal de costos fijos (Lazos de control de Flujo)	4 200	5 670	**9 870**	
Subtotal de costos fijos (Lazos de control de nivel primario)	2 500	2 280	**4 780**	
Subtotal de costos fijos (Lazos de control de temperatura)	1 100	800	**1 900**	
Subtotal de costos fijos (Lazos de control de nivel secundario)	2 400	2 100	**4 500**	
Subtotal costos anuales				**21 050**
Valor actual por costos anuales (20 años, tasa de interés 5%)				**262 329.53**
Costos total del ciclo de vida del SIS				**324 805.52**

Para justificar los costos del sistema de seguridad, se debe realizar un análisis de las pérdidas que tiene la empresa debido a paro en la producción y reparación de elementos críticos.

Mediante cifras se demuestra que la implementación de un SIS reduce considerablemente las pérdidas económicas, para ello se han considerado los dos casos más significativos en cuanto al proceso analizado.

1. Bomba de llenado estropeada.

Descripción	Cant. De horas	Costo por hora	Total
Costo de bomba nueva			112 000
Costo Reparación de bomba			25 000
Costo por paro	9	4 300	38 700
TOTAL			**175 700**

2. Niquelina del calentador de bunker deteriorada.

Descripción	Cant. De horas	Costo por hora	Total
Costo de bomba nueva			77 300
Costo por paro	48	4 500	216 000
TOTAL			**293 300**

Como se puede observar, ambos eventos representan pérdidas económicas muy importantes para la empresa. Las mismas son dimensionadas en un período de 20 años (tiempo de vida del SIS diseñado), lo que revela que los gastos a largo plazo alcanzan valores muy elevados.

1. Bomba de llenado estropeada.

Descripción	Total
Costos dimensionados a 20 años	**527 100**

2. Niquelina del calentador de bunker deteriorada.

Descripción	Total
Costos dimensionados a 20 años	**879 900**

A los costos antes indicados se debe incluir las indemnizaciones por muerte, que dimensionadas a un plazo de 20 años equivalen a $ 146 000. Esto nos da un resultado global:

Descripción	Total
Subtotal de costos	**1 407 000**
Indemnizaciones por muerte	**146 000**
TOTAL	**1 553 000**

Esto evidencia que los costos de reparación de maquinaria, horas de para e indemnizaciones por muerte dimensionados a 20 años implica una pérdida total de $1 553 000, mientras que el costo de vida del SIS es de $ 324 805.52 (20.92% del valor total de pérdidas). Esto representa un ahorro de $ 1 228 194.48 (79.09% del valor total de pérdidas) que la empresa no perderá en paros de producción por accidentes evitables gracias al SIS. Por ello la implementación del SIS es una inversión rentable que asegurará un ambiente de trabajo seguro para el personal y principalmente contribuirá al desarrollo sustentable.

En la etapa de diseño del SIS se revelaron los puntos más débiles del proceso en la actualidad, uno de los más importantes es el intervalo de mantenimiento que se realiza a todos los instrumentos y actuadores del proceso de distribución de combustible. Debido a que es un proceso permanente, el personal de mantenimiento no puede detener el mismo para realizar el mantenimiento necesario, por ello se realiza una vez al año generalmente en el mes de diciembre. Otra gran deficiencia es el poco interés del personal de mantenimiento en implementar nuevas medidas que contribuyan al monitoreo del estado de la maquinaria y su buen funcionamiento.

Además la implementación del SIS para el proceso de distribución de combustible representa un ahorro muy significativo a largo plazo. Esto quiere decir, que los gastos debidos a daño de equipos que generan paros en la producción son reducidos de manera considerable además de prolongar la vida laboral de la empresa de manera segura.

Con la implementación del SIS en la empresa analizada se establecen las bases para promover una cultura de seguridad funcional generando entornos de trabajo más seguros garantizando el bienestar del personal, del ambiente, de la maquinaria y de la producción.

Al realizar la justificación del SIS, se pudo evidenciar el beneficio económico para la empresa. Se demostró mediante cifras que la implementación del sistema de seguridad evita pérdidas económicas considerables debido a accidentes que pueden ser evitados.

El SIS resultante del estudio realizado deja trazados los lineamientos fundamentales para la implementación del mismo en la industria. Depende ahora del personal de seguridad de planta, pero más aún, del personal administrativo que decida adoptar e implementar el sistema de seguridad en sus instalaciones.

Capítulo 5

CONCLUSIONES Y RECOMENDACIONES.

5.1 Conclusiones

El riesgo es una variable que se encuentra siempre presente en la industria de procesos, por ello, un evento peligroso puede resultar un accidente muy grave que puede implicar múltiples daños en la maquinaria, infraestructura, medio ambiente y la muerte de las personas.

El personal de planta que ha escuchado o tiene conocimientos sobre seguridad funcional, estaría de acuerdo con que la aplicación de un SIS aseguraría un entorno de trabajo más seguro en aquellas instalaciones en donde se ha realizado una identificación de peligros de seguridad y operativos, relacionados con los procesos desarrollados en planta en donde se han suscitado accidentes graves y no se dispone de un sistema de seguridad automatizado.

La seguridad funcional en la industria de procesos en la actualidad es un campo que aún es desconocido. Por este motivo, algunas empresas carecen de sistemas que actúan ante eventos inesperados, lo que ha producido pérdidas muy significativas en lo referente a producción debido a paras no planificadas. Esto se traduce en la necesidad de implementar sistemas especiales, independientes de cualquier otro sistema, para que en caso de fallo del resto de capas de prevención, pueda actuar y llevar el proceso a un estado seguro. Por este motivo aparecen los SIS como la tercera capa de prevención, con el objetivo de reducir situaciones de riesgo para los receptores vulnerables.

La presencia de elementos que puedan constituir un riesgo de accidente en cualquier instalación industrial requiere la adopción de medidas de seguridad con criterios exigentes. No sólo se trata de comprar elementos muy fiables con bajas tasas de probabilidad de falla a la demanda, sino que se debe comprobar las múltiples restricciones son impuestas por las normativas IEC-61508 o IEC-61511 para el adecuado cumplimiento de la arquitectura de los sistemas instrumentados de seguridad (SIS) como la independencia o la redundancia de los elementos, en función del SIL requerido.

La tecnología aplicada en los SIS ha evolucionado con el pasar del tiempo y hoy en día se disponen de elementos de alta confiabilidad con altas velocidades de respuesta y con una amplia gama de parámetros de operación (voltaje, potencia y dimensiones). Actualmente se disponen de SIS que realizan autodiagnóstico para detección de fallas.

El avance en el desarrollo de los SIS ha provocado que muchos fabricantes de elementos de control fijen su atención en la fabricación de elementos de seguridad. Este hecho ha generado que muchos de sus elementos sean compatibles con elementos de otros fabricantes, esto provee una amplia variedad de elementos (Sensores, solucionadores lógicos y elementos finales).

La revisión periódica de los elementos de control contribuye a la prevención de eventos peligrosos, por ello, es necesario que se establezcan métodos documentados que indiquen los procedimientos así como los períodos en los cuales deben realizarse pruebas en el sistema de control.

La implementación de SIS en la industria de procesos podría evitar que accidentes graves como la pérdida de extremidades, quemaduras y la muerte de obreros en ciertos casos, tengan lugar. Mediante el diseño del SIS se pudo determinar algunos puntos críticos en el proceso analizado de los cuales tanto el personal de planta, como el de seguridad no estaban enterados.

Durante el proceso de diseño del SIS se detectaron fallas en el proceso que fueron atendidas por el personal de mantenimiento. Dichas fallas comprendían cableado deteriorado, fugas en acoples mecánicos, instrumentos de medición averiados y falta de mantenimiento en algunos actuadores finales. Todas esas fallas pudieron tener consecuencias muy graves, por lo que la implementación del SIS evitaría que situaciones como aquellas tengan lugar.

La seguridad funcional debe tener su espacio dentro del marco de la seguridad industrial en lo que se refiere a la industria de procesos. De la misma manera que se regula el cumplimiento de normas y lineamientos para la seguridad ocupacional, se debería establecer reglamentos que contemplen la implementación de sistemas de seguridad que cumplan con normas internacionales tales como la IEC 61508 e IEC 61511.

5.2 Investigación Futura

Actualmente las empresas analizadas no disponen de métodos ni técnicas que les permitan conocer el estado actual de la maquinaria, es decir, se manejan procedimientos de diagnóstico que en muchas ocasiones debe realizarse de manera más frecuente, pero por motivos de producción no es posible hacerlo ya que implica el paro de la maquinaria. Es por ello, que el desarrollo de nuevas técnicas de diagnóstico y análisis es un campo que necesita atención ya que ofrece muchas posibilidades de investigación.

La seguridad funcional en la industria de procesos, es un campo que ofrece nuevas áreas de investigación; una de ellas es la integración de normas de seguridad que controlen y regularicen la implementación de SIS en los procesos llevados a cabo en diferentes industrias. Al momento, muchos profesionales responsables de la seguridad industrial no conocen las normativas que rigen la seguridad funcional.

Hoy en día, una nueva tendencia ha surgido para automatizar sistemas de extinción, pero no hay ninguna referencia para poder llevarla a cabo. Por ello, algunas medidas generales partiendo de los estándares de seguridad funcional pueden ser aplicadas. Esto indica que un estudio particular se debe desarrollar para poder determinar o proponer lineamientos para la automatización de sistemas de extinción en función de los resultados esperados.

En la actualidad existe un debate en cuanto a los Sistemas de Fuego y Gas con respecto a considerarlos SIS o parte de las funciones de seguridad. La norma ISA- TR84.00.07 - 2010 ha entregado las primeras pautas sobre dichos sistemas pero aún hay muchos conceptos por especificar y mejorar en términos de análisis de confiabilidad y riesgo.

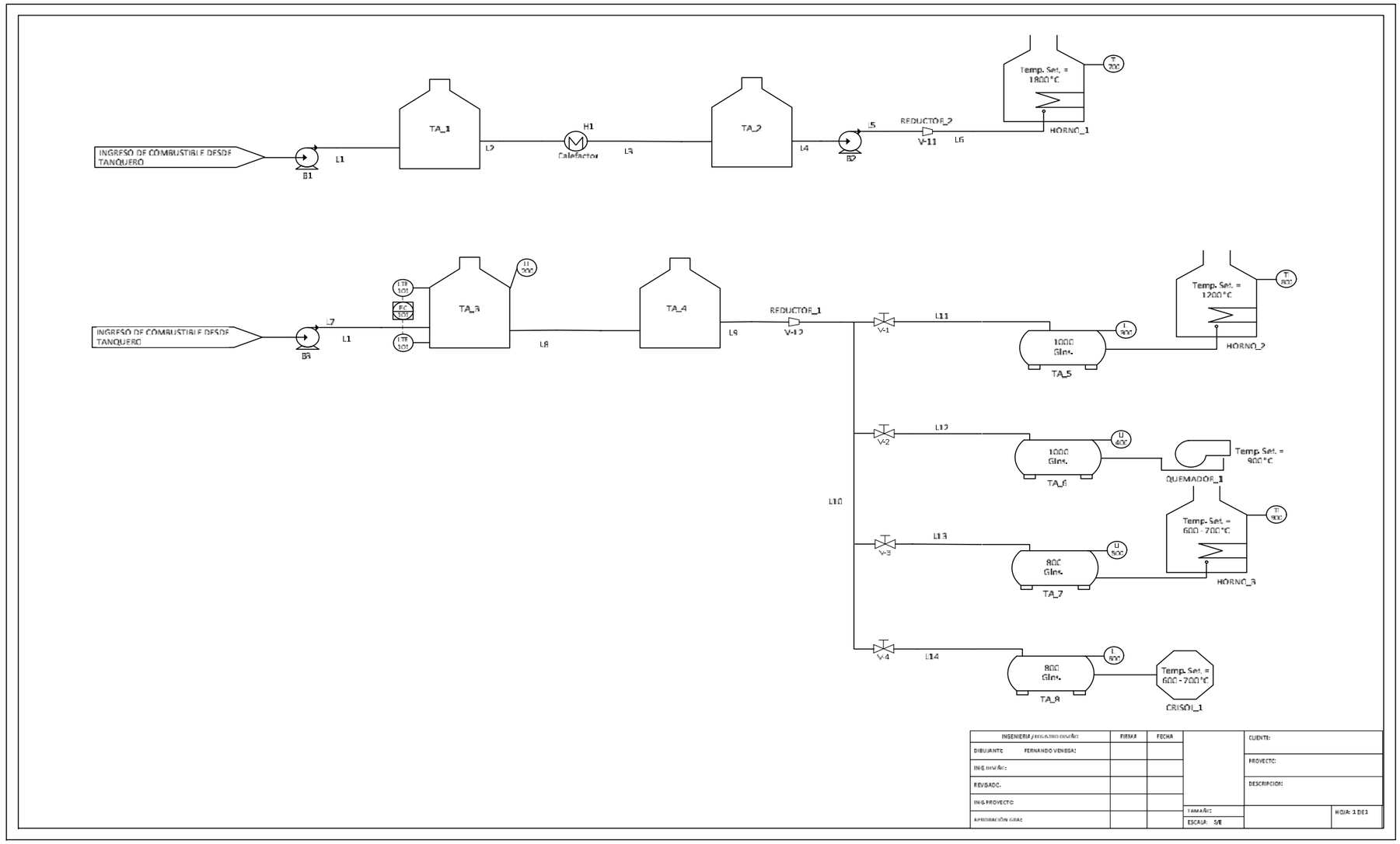
Las normas internacionales sobre la seguridad funcional se concentran principalmente en fallas peligrosas. Por ejemplo, en la IEC- 61511 se mencionan las activaciones esporádicas pero no son analizadas. Este tipo de activaciones afectan la seguridad. Por otra parte, las activaciones esporádicas muchas veces funcionan como una "prueba no programada" para muchos dispositivos que si son bien gestionados y registrados, podrían reducir la PFD.

Los organismos reguladores como el Ministerio de Salud Pública y el Instituto Ecuatoriano de Seguridad Social, encargados de inspeccionar y registrar el cumplimiento de las normativas de seguridad laboral en la industria de procesos, deben considerar dentro de sus regulaciones a la seguridad funcional. No basta solo considerar el impacto humano, sino también ambiental y material que puede resultar de la ocurrencia de un

evento peligroso. Por esto, se debe incorporar normativas de seguridad funcional a las ya existentes en nuestro país.

ANEXOS

ANEXO 1


INGRESO DE COMBUSTIBLE DESDE TANQUERO
B1
L1
TA_1
L2
H1
Calefactor
L3
TA_2
L4
B2
L5
REDUCTOR_2
V-11
L6
Temp. Set. = 1800 °C
HORNO_1
INGRESO DE COMBUSTIBLE DESDE TANQUERO
B3
L7
L1
LTP 101
FC 101
LTP 101
TA_3
L8
TA_4
L9
REDUCTOR_1
V-10
V-1
L11
1000 Gln.
TA_5
Temp. Set. = 1200 °C
HORNO_2
L10
V-2
L12
1000 Gln.
TA_6
Temp. Set. = 900 °C
QUEMADOR_1
V-3
L13
800 Gln.
TA_7
Temp. Set. = 600 - 700 °C
HORNO_3
V-4
L14
800 Gln.
TA_8
Temp. Set. = 600 - 700 °C
CRISOL_1
INGENIERÍA / registro diseño
FIRMA
FECHA
DIBUJANTE FERNANDO VENEGAS:
ING diseño:
REVISADO:
ING PROYECTO:
APROBACIÓN GRAL:
TAMAÑO:
ESCALA: S/E
CLIENTE:
PROYECTO:
DESCRIPCION:
HOJA: 1 DE 1

Anexo 2- HAZOP

NODO	DESVIACION	CAUSAS	CONSECUENCIAS	SALVAGUARDAS	RIESGO			RECOMENDACIÓN	RESPONSABLE	FECHA DE CUMPLIMIENTO
					CONSECUENCIA	PROBABILIDAD	RIESGO			
L1	Alto flujo	ninguna			S	F				
	Bajo flujo	Falla bomba B1	bomba B1 se va a quemar		4	4	B	Instalar un lazo de seguridad que apague la bomba, debe disponer de un sensor de flujo y activar una alarma de bajo flujo.		
	No flujo	Falla bomba B1	bomba B1 se va a quemar		4	4	B	Instalar un lazo de seguridad que apague la bomba, debe disponer de un sensor de flujo y activar una alarma de bajo flujo.		
	Alta temperatura	ninguna								
	Baja temperatura	ninguna								
	Alta presión	ninguna								
	Baja presión	ninguna								
TA_1	Alto flujo	ninguna								
	Bajo flujo	ninguna								
	Alta temperatura	ninguna								
	Baja temperatura	ninguna								
	Alta presión	ninguna								
	Baja presión	ninguna								
	Alto nivel	Falla en calefactor	Obstrucción salida del tanque		5	2	M	Instalar un lazo de seguridad que disponga de un sensor de nivel que active una alarma de alto nivel, apague la bomba B1 y cierre una electroválvula localizada al ingreso del tanque.		
	Bajo nivel	Falla bomba B1	bomba B1 se va a quemar		4	4	B	Instalar un lazo de seguridad que apague la bomba B1, debe disponer de un sensor de nivel y activar una alarma de bajo nivel.		
L2	Alto flujo	ninguna								
	Bajo flujo	Falla bomba B1	bomba B1 se va a quemar		4	4	B	Instalar un lazo de seguridad que apague la bomba, debe disponer de un sensor de flujo y activar una alarma de bajo flujo.		
	No flujo	Falla bomba B1	bomba B1 se va a quemar		4	4	B	Instalar un lazo de seguridad que apague la bomba, debe disponer de un sensor de flujo y activar una alarma de bajo flujo.		
	Alta temperatura	ninguna								
	Baja temperatura	ninguna								
	Alta presión	ninguna								

	Baja presión	ninguna								
H1	Alto flujo	ninguna								
	Bajo flujo	ninguna								
	Alta temperatura	Falla control de temperatura	Daño en niquelina		5	3	M	Instalar un lazo de control que disponga de un sensor de temperatura que active una alarma de alta temperatura y desconecte la niquelina.		
	Baja temperatura	Falla control de temperatura	Obstrucción de lineas hidráulicas		4	3	M	Instalar un lazo de control que disponga de un sensor de temperatura que active una alarma de baja temperatura y cierre una electroválvula localizada a la salida del tanque TA_1.		
	Alta presión	ninguna								
	Baja presión	ninguna								
L3	Alto flujo	ninguna								
	Bajo flujo	Falla en calefactor	Obstrucción de lineas hidráulicas		5	3	M	Instalar un lazo de control que disponga de un sensor de temperatura que active una alarma de baja temperatura en el calefactor.		
		Falla bomba B1	bomba B1 se va a quemar		4	4	B	Instalar un lazo de seguridad que apague la bomba, debe disponer de un sensor de flujo y activar una alarma de bajo flujo.		
	No flujo	Falla en calefactor	Obstrucción de lineas hidráulicas		5	3	M	Instalar un lazo de control que disponga de un sensor de temperatura que active una alarma de baja temperatura y cierre una electroválvula localizada a la salida del tanque TA_1.		
		Falla bomba B1	bomba B1 se va a quemar		4	4	B	Instalar un lazo de seguridad que apague la bomba, debe disponer de un sensor de flujo y activar una alarma de bajo flujo.		
	Alta temperatura	ninguna								
	Baja temperatura	ninguna								
	Alta presión	ninguna								
	Baja presión	ninguna								
TA_2	Alto flujo	ninguna								
	Bajo flujo	ninguna								
	Alta temperatura	ninguna								
	Baja temperatura	ninguna								
	Alta presión	ninguna								
	Baja presión	ninguna								
	Alto nivel	Bomba B2 está dañada	Desbordamiento del tanque		5	3	M	Instalar un lazo de control que disponga de un sensor de nivel que active una alarma de alto nivel y cierre una electroválvula localizada al ingreso del tanque TA_2.		

	Bajo nivel	Falla en calefactor	Obstrucción de lineas hidráulicas		5	3	M	Instalar un lazo de seguridad que disponga de un sensor de nivel y que activar una alarma de baja temperatura.		
		Falla bomba B1	bomba B1 se va a quemar		4	4	B	Instalar un lazo de seguridad que apague la bomba, debe disponer de un sensor de flujo y activar una alarma de bajo flujo.		
L4	Alto flujo	ninguna								
	Bajo flujo	Falla en calefactor	Obstrucción de lineas hidráulicas		5	3	M	Instalar un lazo de seguridad que disponga de un sensor de flujo que active una alarma de baja temperatura.		
		Falla bomba B1	bomba B1 se va a quemar		4	4	B	Instalar un lazo de seguridad que apague la bomba, debe disponer de un sensor de flujo y activar una alarma de bajo flujo.		
	No flujo	Falla en calefactor	Obstrucción de lineas hidráulicas		5	3	M	Instalar un lazo de seguridad que disponga de un sensor de flujo que active una alarma de baja temperatura.		
		Falla bomba B1	bomba B1 se va a quemar		4	4	B	Instalar un lazo de seguridad que apague la bomba, debe disponer de un sensor de flujo y activar una alarma de bajo flujo.		
	Alta temperatura	ninguna								
	Baja temperatura	ninguna								
	Alta presión	ninguna								
	Baja presión	ninguna								
L5	Alto flujo	ninguna								
	Bajo flujo	Falla en calefactor	Obstrucción de lineas hidráulicas		5	3	M	Instalar un lazo de seguridad que disponga de un sensor de flujo que active una alarma de baja temperatura.		
		Falla bomba B1	bomba B1 se va a quemar		4	4	B	Instalar un lazo de seguridad que apague la bomba, debe disponer de un sensor de flujo y activar una alarma de bajo flujo.		
		Falla bomba B2	bomba B2 se va a quemar		4	4	B	Instalar un lazo de seguridad que apague la bomba, debe disponer de un sensor de flujo y activar una alarma de bajo flujo.		
	No flujo	Falla en calefactor	Obstrucción de lineas hidráulicas		5	3	M	Instalar un lazo de seguridad que disponga de un sensor de flujo que active una alarma de baja temperatura.		

		Falla bomba B1	bomba B1 se va a quemar		4	4	B	Instalar un lazo de seguridad que apague la bomba, debe disponer de un sensor de flujo y activar una alarma de bajo flujo.		
		Falla bomba B2	bomba B2 se va a quemar		4	4	B	Instalar un lazo de seguridad que apague la bomba, debe disponer de un sensor de flujo y activar una alarma de bajo flujo.		
	Alta temperatura	ninguna								
	Baja temperatura	ninguna								
	Alta presión	ninguna								
	Baja presión	ninguna								
L6	Alto flujo	ninguna								
	Bajo flujo	Falla en calefactor	Obstrucción de lineas hidráulicas		5	3	M	Instalar un lazo de seguridad que disponga de un sensor de flujo que active una alarma de baja temperatura.		
		Falla bomba B1	bomba B1 se va a quemar		4	4	B	Instalar un lazo de seguridad que apague la bomba, debe disponer de un sensor de flujo y activar una alarma de bajo flujo.		
		Falla bomba B2	bomba B2 se va a quemar		4	4	B	Instalar un lazo de seguridad que apague la bomba, debe disponer de un sensor de flujo y activar una alarma de bajo flujo.		
		Bloqueo en reductor	Menos paso de combustible al horno		5	4	M	Instalar un lazo de seguridad que disponga de un sensor de flujo y activar una alarma de bajo flujo.		
	No flujo	Falla en calefactor	Obstrucción de lineas hidráulicas		5	3	M	Instalar un lazo de seguridad que disponga de un sensor de flujo que active una alarma de baja temperatura.		
		Falla bomba B1	bomba B1 se va a quemar		4	4	B	Instalar un lazo de seguridad que apague la bomba, debe disponer de un sensor de flujo y activar una alarma de bajo flujo.		
		Falla bomba B2	bomba B2 se va a quemar		4	4	B	Instalar un lazo de seguridad que apague la bomba, debe disponer de un sensor de flujo y activar una alarma de bajo flujo.		
		Bloqueo en reductor	Menos paso de combustible al horno		5	4	M	Instalar un lazo de seguridad que disponga de un sensor de flujo y activar una alarma de bajo flujo.		
	Alta temperatura	ninguna								
	Baja temperatura	ninguna								
	Alta presión	ninguna								
	Baja presión	ninguna								
L7	Alto flujo	ninguna								
	Bajo flujo	Falla bomba B3	bomba B3 se va a quemar		4	4	B	Instalar un lazo de seguridad que apague la bomba, debe disponer de un sensor de flujo y activar una alarma de bajo flujo.		

	No flujo	Falla bomba B3	bomba B3 se va a quemar		4	4	B	Instalar un lazo de seguridad que apague la bomba, debe disponer de un sensor de flujo y activar una alarma de bajo flujo.		
	Alta temperatura	ninguna								
	Baja temperatura	ninguna								
	Alta presión	ninguna								
	Baja presión	ninguna								
TA_3	Alto flujo	ninguna								
	Bajo flujo	ninguna								
	Alta temperatura	ninguna								
	Baja temperatura	ninguna								
	Alta presión	ninguna								
	Baja presión	ninguna								
	Alto nivel	Bloqueo en reductor	Desbordamiento del tanque		5	4	M	Instalar un lazo de seguridad que disponga de un sensor de nivel que active una alarma de alto nivel, apague la bomba B3 y cierre una electroválvula localizada al ingreso del tanque.		
	Bajo nivel	Falla bomba B3	bomba B3 se va a quemar		4	4	B	Instalar un lazo de seguridad que apague la bomba, debe disponer de un sensor de flujo y activar una alarma de bajo flujo.		
L8	Alto flujo	ninguna								
	Bajo flujo	Falla bomba B3	bomba B3 se va a quemar		4	4	B	Instalar un lazo de seguridad que apague la bomba, debe disponer de un sensor de flujo y activar una alarma de bajo flujo.		
	No flujo	Falla bomba B3	bomba B3 se va a quemar		4	4	B	Instalar un lazo de seguridad que apague la bomba, debe disponer de un sensor de flujo y activar una alarma de bajo flujo.		
	Alta temperatura	ninguna								
	Baja temperatura	ninguna								
	Alta presión	ninguna								
	Baja presión	ninguna								
TA_4	Alto flujo	ninguna								
	Bajo flujo	ninguna								
	Alta temperatura	ninguna								
	Baja temperatura	ninguna								
	Alta presión	ninguna								
	Baja presión	ninguna								
	Alto nivel	Bloqueo en reductor	Desbordamiento del tanque		5	4	M	Instalar un lazo de seguridad que disponga de un sensor de nivel que active una alarma de alto nivel, apague la bomba B3 y cierre una electroválvula localizada al ingreso del tanque.		

	Bajo nivel	Falla bomba B3	bomba B3 se va a quemar		4	4	B	Instalar un lazo de seguridad que apague la bomba, debe disponer de un sensor de flujo y activar una alarma de bajo flujo.		
L9	Alto flujo	ninguna								
	Bajo flujo	Falla bomba B3	bomba B3 se va a quemar		4	4	B	Instalar un lazo de seguridad que apague la bomba, debe disponer de un sensor de flujo y activar una alarma de bajo flujo.		
	No flujo	Falla bomba B3	bomba B3 se va a quemar		4	4	B	Instalar un lazo de seguridad que apague la bomba, debe disponer de un sensor de flujo y activar una alarma de bajo flujo.		
	Alta temperatura	ninguna								
	Baja temperatura	ninguna								
	Alta presión	ninguna								
	Baja presión	ninguna								
L10	Alto flujo	ninguna								
	Bajo flujo	Falla bomba B3	bomba B3 se va a quemar		4	4	B	Instalar un lazo de seguridad que apague la bomba, debe disponer de un sensor de flujo y activar una alarma de bajo flujo.		
		Bloqueo en reductor	Menos paso de combustible a tanques secundarios		5	4	M	Instalar un lazo de seguridad que disponga de un sensor de flujo y activar una alarma de bajo flujo.		
	No flujo	Falla bomba B3	bomba B3 se va a quemar		4	4	B	Instalar un lazo de seguridad que apague la bomba, debe disponer de un sensor de flujo y activar una alarma de bajo flujo.		
		Bloqueo en reductor	Menos paso de combustible a tanques secundarios		5	4	M	Instalar un lazo de seguridad que disponga de un sensor de flujo y activar una alarma de bajo flujo.		
	Alta temperatura	ninguna								
	Baja temperatura	ninguna								
	Alta presión	ninguna								
	Baja presión	ninguna								
L11	Alto flujo	ninguna								
	Bajo flujo	Falla bomba B3	bomba B3 se va a quemar		4	4	B	Instalar un lazo de seguridad que apague la bomba, debe disponer de un sensor de flujo y activar una alarma de bajo flujo.		
		Bloqueo en reductor	Menos paso de combustible a tanques secundarios		5	4	M	Instalar un lazo de seguridad que disponga de un sensor de flujo y activar una alarma de bajo flujo.		
		Válvula V-1 está parcialmente cerrada	Menos paso de combustible a tanques secundarios		5	4	M	Instalar un lazo de seguridad que disponga de un sensor de flujo y activar una alarma de bajo flujo.		

	No flujo	Falla bomba B3	bomba B3 se va a quemar		4	4	B	Instalar un lazo de seguridad que apague la bomba, debe disponer de un sensor de flujo y activar una alarma de bajo flujo.		
		Bloqueo en reductor	Menos paso de combustible a tanques secundarios		5	4	M	Instalar un lazo de seguridad que disponga de un sensor de flujo y activar una alarma de bajo flujo.		
		Válvula V-1 está cerrada o bloqueada	Menos paso de combustible a tanques secundarios		5	4	M	Instalar un lazo de seguridad que disponga de un sensor de flujo y activar una alarma de bajo flujo.		
	Alta temperatura	ninguna								
	Baja temperatura	ninguna								
	Alta presión	ninguna								
	Baja presión	ninguna								
TA_5	Alto flujo	ninguna								
	Bajo flujo	ninguna								
	Alta temperatura	ninguna								
	Baja temperatura	ninguna								
	Alta presión	ninguna								
	Baja presión	ninguna								
	Alto nivel	Válvula V-1 no se cierra	Desbordamiento del tanque		5	3	M	Instalar un lazo de seguridad que disponga de un sensor de nivel que active una alarma de alto nivel y cierre una electroválvula localizada al ingreso del tanque.		
	Bajo nivel	Falla bomba B3	bomba B3 se va a quemar		4	4	B	Instalar un lazo de seguridad que apague la bomba, debe disponer de un sensor de flujo y activar una alarma de bajo flujo.		
		Bloqueo en reductor	Menos paso de combustible a tanques secundarios		5	4	M	Instalar un lazo de seguridad que disponga de un sensor de flujo y activar una alarma de bajo flujo.		
		Válvula V-1 está parcialmente cerrada	Menos paso de combustible a tanques secundarios		5	4	M	Instalar un lazo de seguridad que disponga de un sensor de flujo y activar una alarma de bajo flujo.		
L12	Alto flujo	ninguna								
	Bajo flujo	Falla bomba B3	bomba B3 se va a quemar		4	4	B	Instalar un lazo de seguridad que apague la bomba, debe disponer de un sensor de flujo y activar una alarma de bajo flujo.		
		Bloqueo en reductor	Menos paso de combustible a tanques secundarios		5	4	M	Instalar un lazo de seguridad que disponga de un sensor de flujo y activar una alarma de bajo flujo.		
		Válvula V-2 está parcialmente cerrada	Menos paso de combustible a tanques secundarios		5	4	M	Instalar un lazo de seguridad que disponga de un sensor de flujo y activar una alarma de bajo flujo.		
	No flujo	Falla bomba B3	bomba B3 se va a quemar		4	4	B	Instalar un lazo de seguridad que apague la bomba, debe disponer de un sensor de flujo y activar una alarma de bajo flujo.		

		Bloqueo en reductor	Menos paso de combustible a tanques secundarios		5	4	M	Instalar un lazo de seguridad que disponga de un sensor de flujo y activar una alarma de bajo flujo.		
		Válvula V-2 está cerrada o bloqueada	Menos paso de combustible a tanques secundarios		5	4	M	Instalar un lazo de seguridad que disponga de un sensor de flujo y activar una alarma de bajo flujo.		
	Alta temperatura	ninguna								
	Baja temperatura	ninguna								
	Alta presión	ninguna								
	Baja presión	ninguna								
TA_6	Alto flujo	ninguna								
	Bajo flujo	ninguna								
	Alta temperatura	ninguna								
	Baja temperatura	ninguna								
	Alta presión	ninguna								
	Baja presión	ninguna								
	Alto nivel	Válvula V-2 no se cierra	Desbordamiento del tanque		5	3	M	Instalar un lazo de seguridad que disponga de un sensor de nivel que active una alarma de alto nivel y cierre una electroválvula localizada al ingreso del tanque.		
	Bajo nivel	Falla bomba B3	bomba B3 se va a quemar		4	4	B	Instalar un lazo de seguridad que apague la bomba, debe disponer de un sensor de flujo y activar una alarma de bajo flujo.		
		Bloqueo en reductor	Menos paso de combustible a tanques secundarios		5	4	M	Instalar un lazo de seguridad que disponga de un sensor de flujo y activar una alarma de bajo flujo.		
		Válvula V-2 está parcialmente cerrada	Menos paso de combustible a tanques secundarios		5	4	M	Instalar un lazo de seguridad que disponga de un sensor de flujo y activar una alarma de bajo flujo.		
L13	Alto flujo	ninguna								
	Bajo flujo	Falla bomba B3	bomba B3 se va a quemar		4	4	B	Instalar un lazo de seguridad que apague la bomba, debe disponer de un sensor de flujo y activar una alarma de bajo flujo.		
		Bloqueo en reductor	Menos paso de combustible a tanques secundarios		5	4	M	Instalar un lazo de seguridad que disponga de un sensor de flujo y activar una alarma de bajo flujo.		
		Válvula V-3 está parcialmente cerrada	Menos paso de combustible a tanques secundarios		5	4	M	Instalar un lazo de seguridad que disponga de un sensor de flujo y activar una alarma de bajo flujo.		
	No flujo	Falla bomba B3	bomba B3 se va a quemar		4	4	B	Instalar un lazo de seguridad que apague la bomba, debe disponer de un sensor de flujo y activar una alarma de bajo flujo.		
		Bloqueo en reductor	Menos paso de combustible a tanques secundarios		5	4	M	Instalar un lazo de seguridad que disponga de un sensor de flujo y activar una alarma de bajo flujo.		

		Válvula V-3 está cerrada o bloqueada	Menos paso de combustible a tanques secundarios		5	4	M	Instalar un lazo de seguridad que disponga de un sensor de flujo y activar una alarma de bajo flujo.		
	Alta temperatura	ninguna								
	Baja temperatura	ninguna								
	Alta presión	ninguna								
	Baja presión	ninguna								
TA_7	Alto flujo	ninguna								
	Bajo flujo	ninguna								
	Alta temperatura	ninguna								
	Baja temperatura	ninguna								
	Alta presión	ninguna								
	Baja presión	ninguna								
	Alto nivel	Válvula V-3 no se cierra	Desbordamiento del tanque		5	3	M	Instalar un lazo de seguridad que disponga de un sensor de nivel que active una alarma de alto nivel y cierre una electroválvula localizada al ingreso del tanque.		
	Bajo nivel	Falla bomba B3	bomba B3 se va a quemar		4	4	B	Instalar un lazo de seguridad que apague la bomba, debe disponer de un sensor de flujo y activar una alarma de bajo flujo.		
		Bloqueo en reductor	Menos paso de combustible a tanques secundarios		5	4	M	Instalar un lazo de seguridad que disponga de un sensor de flujo y activar una alarma de bajo flujo.		
		Válvula V-3 está parcialmente cerrada	Menos paso de combustible a tanques secundarios		5	4	M	Instalar un lazo de seguridad que disponga de un sensor de flujo y activar una alarma de bajo flujo.		
L14	Alto flujo	ninguna								
	Bajo flujo	Falla bomba B3	bomba B3 se va a quemar		4	4	B	Instalar un lazo de seguridad que apague la bomba, debe disponer de un sensor de flujo y activar una alarma de bajo flujo.		
		Bloqueo en reductor	Menos paso de combustible a tanques secundarios		5	4	M	Instalar un lazo de seguridad que disponga de un sensor de flujo y activar una alarma de bajo flujo.		
		Válvula V-4 está parcialmente cerrada	Menos paso de combustible a tanques secundarios		5	4	M	Instalar un lazo de seguridad que disponga de un sensor de flujo y activar una alarma de bajo flujo.		
	No flujo	Falla bomba B3	bomba B3 se va a quemar		4	4	B	Instalar un lazo de seguridad que apague la bomba, debe disponer de un sensor de flujo y activar una alarma de bajo flujo.		
		Bloqueo en reductor	Menos paso de combustible a tanques secundarios		5	4	M	Instalar un lazo de seguridad que disponga de un sensor de flujo y activar una alarma de bajo flujo.		
		Válvula V-4 está cerrada o bloqueada	Menos paso de combustible a tanques secundarios		5	4	M	Instalar un lazo de seguridad que disponga de un sensor de flujo y activar una alarma de bajo flujo.		
	Alta temperatura	ninguna								
	Baja temperatura	ninguna								

	Alta presión	ninguna								
	Baja presión	ninguna								
TA_8	Alto flujo	ninguna								
	Bajo flujo	ninguna								
	Alta temperatura	ninguna								
	Baja temperatura	ninguna								
	Alta presión	ninguna								
	Baja presión	ninguna								
	Alto nivel	Válvula V-4 no se cierra	Desbordamiento del tanque		5	3	M	Instalar un lazo de seguridad que disponga de un sensor de nivel que active una alarma de alto nivel y cierre una electroválvula localizada al ingreso del tanque.		
	Bajo nivel	Falla bomba B3	bomba B3 se va a quemar		4	4	B	Instalar un lazo de seguridad que apague la bomba, debe disponer de un sensor de flujo y activar una alarma de bajo flujo.		
		Bloqueo en reductor	Menos paso de combustible a tanques secundarios		5	4	M	Instalar un lazo de seguridad que disponga de un sensor de flujo y activar una alarma de bajo flujo.		
		Válvula V-4 está parcialmente cerrada	Menos paso de combustible a tanques secundarios		5	4	M	Instalar un lazo de seguridad que disponga de un sensor de flujo y activar una alarma de bajo flujo.		

ANEXO 3-LOPA

Estado con Aplicación de SIS

						CAPAS DE PROTECCIÓN								
#	Descripción del evento de impacto	Nivel de severidad	Causa de inicio	Probabilidad de inicio	Ocurrencia por año	Diseño del proceso general	Alarma	Capas de mitigación adicionales		Probabilidad de evento intermedio	Nivel de integridad de la SIF	Nivel de SIL requerido	Probabilidad de mitigación del evento	Notas
1	Bomba B1 se va a quemar	M	Falla bomba B1	0,001	0,156	1	0,1	0,1	Relé térmico	1,56E-03	0,071225071	SIL 1	1,11E-04	Falta de fluido provoca daño en la bomba
2	Obstrucción salida del tanque	M	Falla en calefactor	0,001	0,35	1	0,1	0,1	Válvula de alivio	3,50E-03	0,031746032	SIL 1	1,11E-04	Caída de temperatura no disuelve suficiente el combustible
3	Daño en niquelina	S	Falla control de temperatura	0,001	0,35	1	0,1	0,1	Sensor auxiliar	3,50E-03	0,031746032	SIL 1	1,11E-04	Niquelina deteriorada
4	Obstrucción de lineas hidráulicas	S	Falla control de temperatura	0,001	0,365	1	0,1	0,1	Sensor auxiliar	3,65E-03	0,0304414	SIL 1	1,11E-04	Combustible muy espeso para fluir por cañerías
5	Desbordamiento del tanque	M	Bomba B2 está dañada	0,001	0,365	1	0,1	0,1	Relé térmico/Dique	3,65E-03	0,0304414	SIL 1	1,11E-04	Salida del tanque se encuentra obstruída
6	Bomba B2 se va a quemar	M	Falla bomba B2	0,001	0,35	1	0,1	0,1	Relé térmico	3,50E-03	0,031746032	SIL 1	1,11E-04	Falta de fluido provoca daño en la bomba
7	Menos paso de combustible al horno	S	Bloqueo en reductor	0,001	0,365	1	0,1	0,1	Válvula de bypass	3,65E-03	0,0304414	SIL 1	1,11E-04	Reducción de combustible provoca caída de temperatura en el horno
8	Bomba B3 se va a quemar	M	Bomba B3 está dañada	0,001	0,26	1	0,1	0,1	Relé térmico	2,60E-03	3,02E-04	SIL 2	1,11E-04	Falta de fluido provoca daño en la bomba
		M	Fallo del PLC de llenado	0,01	3,65	1	0,1	1	PLC redundante	3,65E-01				Falla en el PLC de llenado de tanque
9	Menos paso de combustible a tanques secundarios	S	Bloqueo en reductor	0,1	36,5	1	0,1	0,1	Válvula de bypass	3,65E-01	0,000304414	SIL 1	1,11E-04	Reducida cantidad de combustible ingresa a tanques secundarios.

M = Medio
S= Severo

El riesgo tolerable fijado es de:	0,001
Posibles eventos de riesgo:	9

Nuevo factor de riesgo:	**0,00011111**

ANEXO 3-LOPA

Estado con Aplicación de SIS

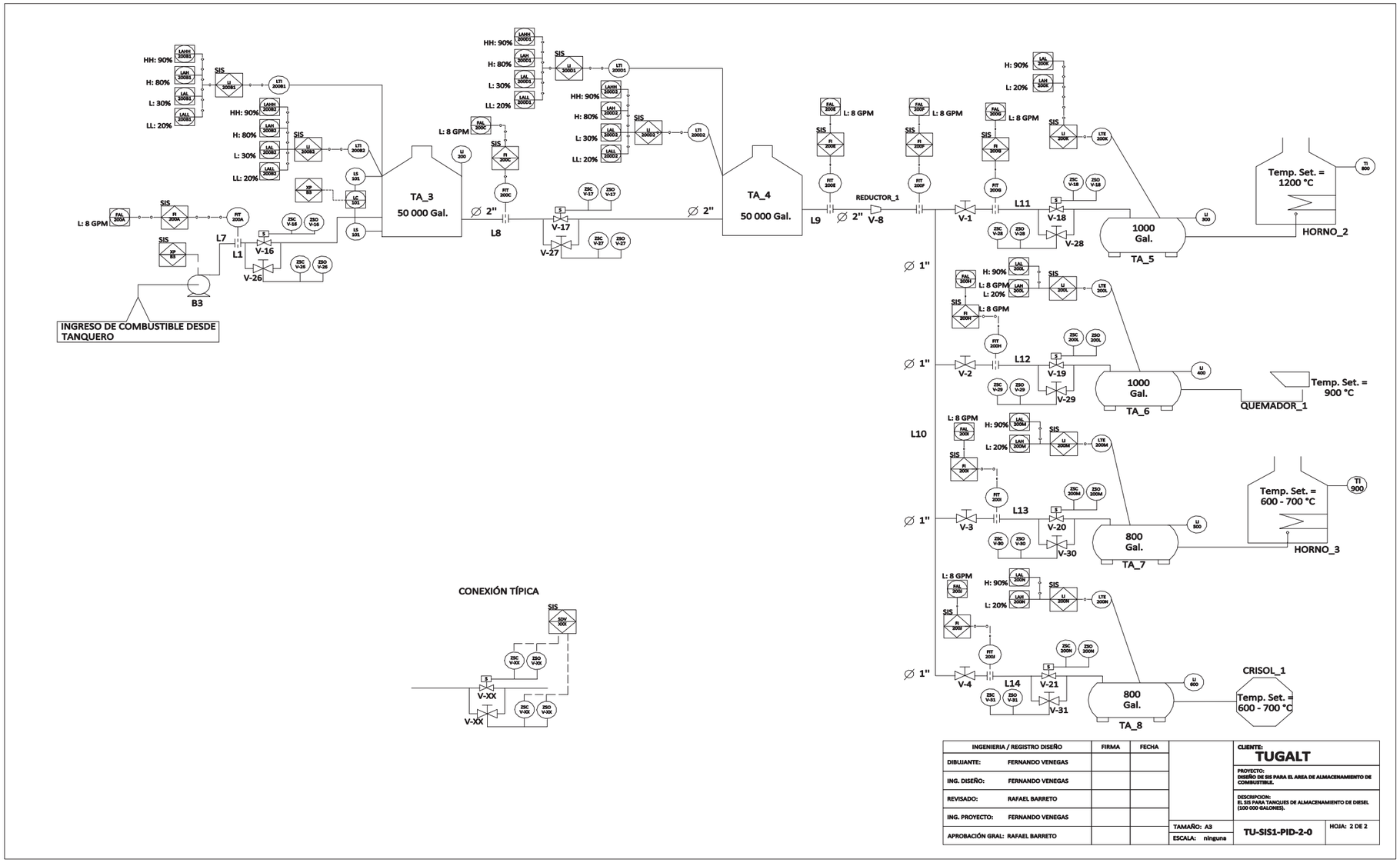
#	Descripción del evento de impacto	Nivel de severidad	Causa de inicio	Probabilidad de inicio	Ocurrencia por año	CAPAS DE PROTECCIÓN: Diseño del proceso general	Alarma	Capas de mitigación adicionales		Probabilidad de evento intermedio	Nivel de integridad de la SIF	Nivel de SIL requerido	Probabilidad de mitigación del evento	Notas
1	Bomba B1 se va a quemar	M	Falla bomba B1	0,001	0,156	1	0,1	0,1	Relé térmico	1,56E-03	0,071225071	SIL 1	1,11E-04	Falta de fluido provoca daño en la bomba
2	Obstrucción salida del tanque	M	Falla en calefactor	0,001	0,35	1	0,1	0,1	Válvula de alivio	3,50E-03	0,031746032	SIL 1	1,11E-04	Caída de temperatura no disuelve suficiente el combustible
3	Daño en niquelina	S	Falla control de temperatura	0,001	0,35	1	0,1	0,1	Sensor auxiliar	3,50E-03	0,031746032	SIL 1	1,11E-04	Niquelina deteriorada
4	Obstrucción de lineas hidráulicas	S	Falla control de temperatura	0,001	0,365	1	0,1	0,1	Sensor auxiliar	3,65E-03	0,0304414	SIL 1	1,11E-04	Combustible muy espeso para fluir por cañerías
5	Desbordamiento del tanque	M	Bomba B2 está dañada	0,001	0,365	1	0,1	0,1	Relé térmico/Dique	3,65E-03	0,0304414	SIL 1	1,11E-04	Salida del tanque se encuentra obstruída
6	Bomba B2 se va a quemar	M	Falla bomba B2	0,001	0,35	1	0,1	0,1	Relé térmico	3,50E-03	0,031746032	SIL 1	1,11E-04	Falta de fluido provoca daño en la bomba
7	Menos paso de combustible al horno	S	Bloqueo en reductor	0,001	0,365	1	0,1	0,1	Válvula de bypass	3,65E-03	0,0304414	SIL 1	1,11E-04	Reducción de combustible provoca caída de temperatura en el horno
8	Bomba B3 se va a quemar	M	Bomba B3 está dañada	0,001	0,26	1	0,1	0,1	Relé térmico	2,60E-03	3,02E-04	SIL 2	1,11E-04	Falta de fluido provoca daño en la bomba
		M	Fallo del PLC de llenado	0,01	3,65	1	0,1	1	PLC redundante	3,65E-01				Falla en el PLC de llenado de tanque
9	Menos paso de combustible a tanques secundarios	S	Bloqueo en reductor	0,1	36,5	1	0,1	0,1	Válvula de bypass	3,65E-01	0,000304414	SIL 1	1,11E-04	Reducida cantidad de combustible ingresa a tanques secundarios.

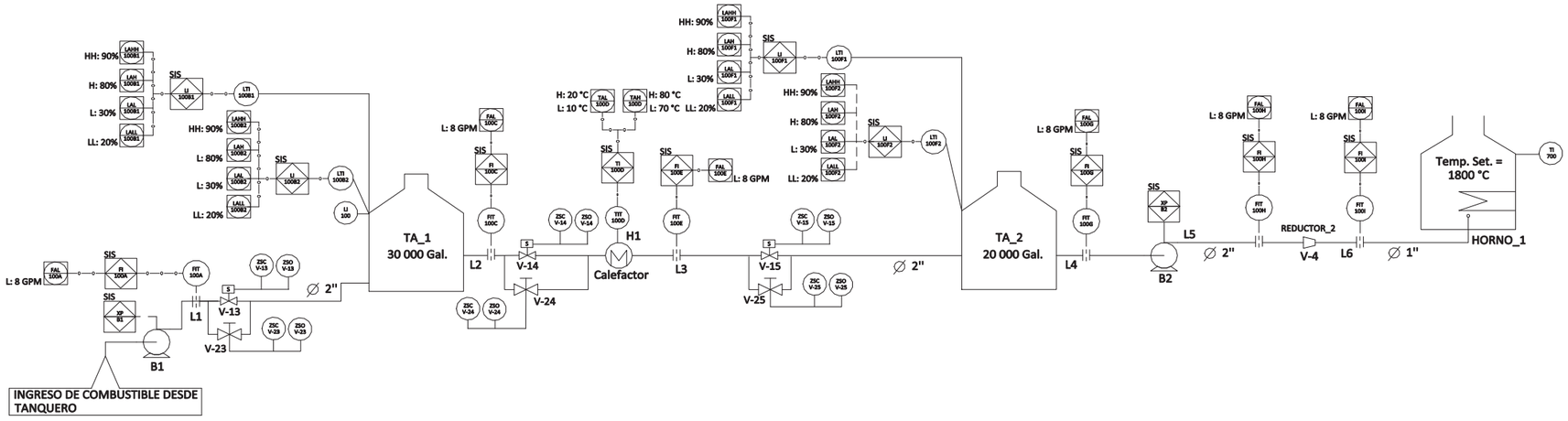
M = Medio
S= Severo

El riesgo tolerable fijado es de:	0,001
Posibles eventos de riesgo:	9

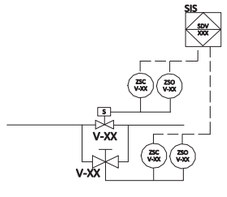
Nuevo factor de riesgo:	**0,000111**

ANEXO 4


HH: 90%
H: 80%
L: 30%
LL: 20%
SIS
LAHH 200B3
LAH 200B3
LAL 200B3
LALL 200B3
LTI 200B3
LI 200B3
XP B3
LS 101
LC 101
LS 103
FAL 200A
L: 8 GPM
FI 200A
FIT 200A
B3
INGRESO DE COMBUSTIBLE DESDE TANQUERO
L7
L1
V-16
V-26
ZSC V-16
ZSO V-16
ZSC V-26
ZSO V-26
TA_3
50 000 Gal.
LAHH 300D1
LAH 300D1
LAL 300D1
LALL 300D1
LTI 300D1
LI 300D1
LAHH 300D2
LAH 300D2
LAL 300D2
LALL 300D2
LTI 300D2
LI 300D2
FAL 200C
LI 200
FI 200C
FIT 200C
∅ 2"
L8
V-17
V-27
ZSC V-17
ZSO V-17
ZSC V-27
ZSO V-27
TA_4
50 000 Gal.
FAL 200E
FI 200E
FIT 200E
L9
REDUCTOR_1
FAL 200F
FI 200F
FIT 200F
V-8
V-1
FAL 200G
FI 200G
FIT 200G
L11
V-18
V-28
ZSC V-18
ZSO V-18
ZSC V-28
ZSO V-28
1000 Gal.
TA_5
LAL 200K
LAH 200K
LTE 200K
TI 200
Temp. Set. = 1200 °C
HORNO_2
∅ 1"
V-2
L12
V-19
V-29
ZSC V-29
ZSO V-29
LI 400
Temp. Set. = 900 °C
QUEMADOR_1
L10
FAL 200I
FI 200I
FIT 200I
V-3
L13
V-20
V-30
ZSC V-30
ZSO V-30
800 Gal.
TA_7
LI 500
TI 900
Temp. Set. = 600 - 700 °C
HORNO_3
FAL 200J
FI 200J
FIT 200J
V-4
L14
V-21
V-31
ZSC V-31
ZSO V-31
800 Gal.
TA_8
LI 600
CRISOL_1
Temp. Set. = 600 - 700 °C
CONEXIÓN TÍPICA
SDV 200X
V-XX
ZSC V-XX
ZSO V-XX
INGENIERIA / REGISTRO DISEÑO
FIRMA
FECHA
DIBUJANTE: FERNANDO VENEGAS
ING. DISEÑO: FERNANDO VENEGAS
REVISADO: RAFAEL BARRETO
ING. PROYECTO: FERNANDO VENEGAS
APROBACIÓN GRAL: RAFAEL BARRETO
TAMAÑO: A3
ESCALA: ninguna
CLIENTE:
TUGALT
PROYECTO:
DISEÑO DE SIS PARA EL AREA DE ALMACENAMIENTO DE COMBUSTIBLE.
DESCRIPCION:
EL SIS PARA TANQUES DE ALMACENAMIENTO DE DIESEL (100 000 GALONES).
TU-SIS1-PID-2-0
HOJA: 2 DE 2



CONEXIÓN TÍPICA



INGENIERIA / REGISTRO DISEÑO		FIRMA	FECHA
DIBUJANTE:	FERNANDO VENEGAS		
ING. DISEÑO:	FERNANDO VENEGAS		
REVISADO:	RAFAEL BARRETO		
ING. PROYECTO:	FERNANDO VENEGAS		
APROBACIÓN GRAL:	RAFAEL BARRETO		

CLIENTE: **TUGALT**

PROYECTO: DISEÑO DE SIS PARA EL AREA DE ALMACENAMIENTO DE COMBUSTIBLE.

DESCRIPCION: EL SIS PARA TANQUES DE ALMACENAMIENTO DE BUNKER (50 000 GALONES).

TAMAÑO: A3 | ESCALA: ninguna | **TU-SIS1-PID-1-0** | HOJA: 1 DE 2

Anexo 5

Checklist para Instalación y Arranque del sistema.

Item #	Item	Elegir una opción			Comentarios
1	¿El personal ha recibido el entrenamiento apropiado?	SI	NO	N/A	
2	¿Hay la suficiente independencia entre los que realizan el trabajo y quienes lo inspeccionan?	SI	NO	N/A	
3	¿Se han tomado precauciones adecuadas para el almacenamiento de artículos durante la instalación?	SI	NO	N/A	
4	¿Son los procedimientos de instalación lo suficientemente claros como para no dejar interpretaciones del personal?	SI	NO	N/A	
5	¿El SIS ha sido inspeccionado con el fin de revelar algún daño causado durante la instalación?	SI	NO	N/A	
6	Los artículos como armarios, cajas y cables están protejidos de:				
	a)fuga de vapor	SI	NO	N/A	
	b)fuga de agua	SI	NO	N/A	
	c)fuga de aceite	SI	NO	N/A	
	d)fuentes de calor	SI	NO	N/A	
	e)daño mecánico	SI	NO	N/A	
	f)corrosión (óxido)	SI	NO	N/A	
7	¿Están los sistemas de seguridad claramente identificados para evitar manipulación involuntaria?	SI	NO	N/A	
8	¿La operación de los siguientes artículos ha sido probada?:	SI	NO	N/A	
	a)adecuada instalación del equipo y cableado				
	b)fuentes de energía son operaciona	SI	NO	N/A	
	c)todos los dispositivos han sido calibrados	SI	NO	N/A	
	d)todos los dispositivos son operativ	SI	NO	N/A	

	e)solucionador lógico es operaciona	SI	NO	N/A	
	f)comuncación con otros sistemas	SI	NO	N/A	
	g)operación e indicación de bypass	SI	NO	N/A	
	h)operación de re-inicio	SI	NO	N/A	
	i)operación de apagado manual	SI	NO	N/A	
9	¿Es la documentación consistente con la instalación actual?	SI	NO	N/A	
10	¿Hay información mostrando lo siguiente?	SI	NO	N/A	
	a)Identificación del sistema siendo arrancado	SI	NO	N/A	
	b)confirmación de que la instalación ha sido realizada exitosamente	SI	NO	N/A	
	c)La fecha en la que el sistema fue instalado	SI	NO	N/A	
	d)el procedimiento utilzado para instalar el sistema	SI	NO	N/A	
	e)firmas autorizadas indicando que el sistema fue instalado exitosamente.	SI	NO	N/A	

Checklist para Operación y Mantenimiento.

Item #	Item	Elegir una opción			Comentarios
1	¿Los empleados han sido adecuadamente entrenados en los procedimientos de operación y manejo del sistem?	SI	NO	N/A	
2	¿Los procedimientos de operación están adecuadamente documentados?	SI	NO	N/A	
3	¿Hay un manual de usuario/operador/mantenimiento para el sistema?	SI	NO	N/A	
4	El manual describe:				
	a)límites de operación segura y las implicaciones de excederlos	SI	NO	N/A	
	b)como el sistema lleva el proceso a un estado seguro	SI	NO	N/A	
	c)los riesgos asociados con las fallas del sistemas y las acciones requeridas para diferentes fallas	SI	NO	N/A	
5	¿Hay medios para limitar el acceso solo a personal autorizado?	SI	NO	N/A	
6	¿Pueden todos los parámetros operacionales ser inspeccionados para asegurar que sean correctos?	SI	NO	N/A	
7	¿Hay medios para limitar el rango de variación de los parámetros de activación?	SI	NO	N/A	
8	¿Se han establedido medioas adecuados para el bypass de funciones de seguridad?	SI	NO	N/A	
9	¿Cuándo a las funciones se les realiza un bypass, son claramente indicadas?	SI	NO	N/A	
10	¿Se han establecido procedimientos documentados para controlar la aplicación y eliminación de bypass?	SI	NO	N/A	
11	¿Se han establecido procedimientos documentados que aseguren la seguridad en la planta mientras el SIS está en mantenimiento?	SI	NO	N/A	

12	¿Son los procedimientos de mantenimiento lo suficiente detallados de manera que no dejen importantes interpretaciones o decisiones al personal de mantenimiento?	SI	NO	N/A	
13	¿Las actividades de mantenimiento planificadas son definidas para todas las porciones del sistema?	SI	NO	N/A	
14	¿Los procedimientos son periódicamente revisados?	SI	NO	N/A	
15	¿Se encuentran los procedimientos en el lugar para prevenir manipulación involuntaria?	SI	NO	N/A	
16	¿Hay medios para verificar que la reparación llevada a cabo en un determinado tiempo sea consistente con la evaluación de seguridad?	SI	NO	N/A	
17	¿Los procedimientos de operación y mantenimiento reducen la introducción de potenciales problemas de causa común?	SI	NO	N/A	
18	¿La documentación está de acuerdo con los procedimientos de operación y mantenimiento actuales?	SI	NO	N/A	

Checklist para Pruebas.

Item #	Item	Elegir una opción			Comentarios
1	¿Los procedimientos documentados se encuentran en lugar para permitir pruebas de todas las SIF, incluyendo los dispositivos de campo?	SI	NO	N/A	
2	¿Son los procedimientos de prueba lo suficiente detallados para no dejar interpretaciones o decisiones al personal de mantenimiento?	SI	NO	N/A	
3	¿La base para intervalos de prueba periódicos ha sido documentado?	SI	NO	N/A	
4	¿Se probaron los siguientes artículos?				
	a)líneas de impulso	SI	NO	N/A	
	b)dispositivos de sensado	SI	NO	N/A	
	c)aplicaciones lógicas, computacionales y/o secuencias	SI	NO	N/A	
	d)puntos de activación	SI	NO	N/A	
	e)funciones de alarma	SI	NO	N/A	
	f)velocidad de respuesta	SI	NO	N/A	
	g)elementos finales	SI	NO	N/A	
	h)activaciones manuales	SI	NO	N/A	
	i)diagnósticos	SI	NO	N/A	
5	¿Hay un sistema de reporte de fallas?	SI	NO	N/A	
6	¿Se encuentran los procedimientos en el lugar para comparar el desempeño actual con respecto al predecido o requerido?	SI	NO	N/A	
7	¿Hay procedimientos documentados para corregir deficiencias encontradas?	SI	NO	N/A	
8	¿Se verificó la calibración de los instrumentos?	SI	NO	N/A	
9	¿Se mantienen registros de pruebas?	SI	NO	N/A	
10	Los registros de pruebas muestran:				
	a)fecha de la inspección/prueba	SI	NO	N/A	
	b)nombre de la persona que realizó la prueba	SI	NO	N/A	
	c)identificación del dispositivo probado	SI	NO	N/A	
	d)resultados de la prueba	SI	NO	N/A	

11	¿Los procedimientos de prueba en el lugar minimizan la introducción de potenciales problemas de causa común?	SI	NO	N/A	
12	¿La tasa de falla es revisada periódicamente y comparada con los datos utilizados durante el diseño/análisis del sistema?	SI	NO	N/A	

Checklist para Manejo de Cambios.

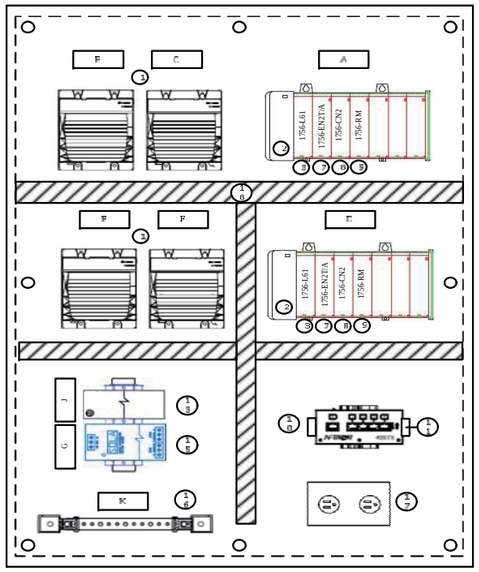
Item #	Item	Elegir una opción			Comentarios
1	¿Existen procedimientos de aprobación que consideren las implicaciones de seguridad?, tal como:				
	a)base técnica para el cambio	SI	NO	N/A	
	b)impacto en la seguridad y salud	SI	NO	N/A	
	c)impacto en los procedimientos de operación/mantenimiento				
	d)tiempo requerido	SI	NO	N/A	
	e)efecto en el tiempo de respuesta	SI	NO	N/A	
2	¿Hay procedimientos que definan el nivel de revisión/aprobación requerido dependiendo de la naturaleza del cambio?	SI	NO	N/A	
3	El cambio propuesto ha iniciado un retorno a la fase apropiada del ciclo de vida?	SI	NO	N/A	
4	¿La documentación del proyecto ha sido alterada para reflejar el cambio?	SI	NO	N/A	
5	¿El sistema completo ha sido probado después de que los cambios han sido introducidos y los resultados se han documentado?	SI	NO	N/A	
6	¿Hay procedimientos documentados para verificar que los cambios se han hecho satisfactoriamente?	SI	NO	N/A	
7	¿Todos los departamentos afectados fueron informados del cambio?	SI	NO	N/A	
8	¿El acceso al hardware y al software esta limitado al personal autorizado y competente?	SI	NO	N/A	
9	¿El acceso a la documentación del proyecto está limitada a personal autorizado?	SI	NO	N/A	
10	¿Los documentos del proyecto están sujetos a una revisión de control apropiada?	SI	NO	N/A	
11	¿Se han considerado las consecuencias de incorporar nuevas versiones de software?	SI	NO	N/A	

Checklist para el Desmantelamiento.

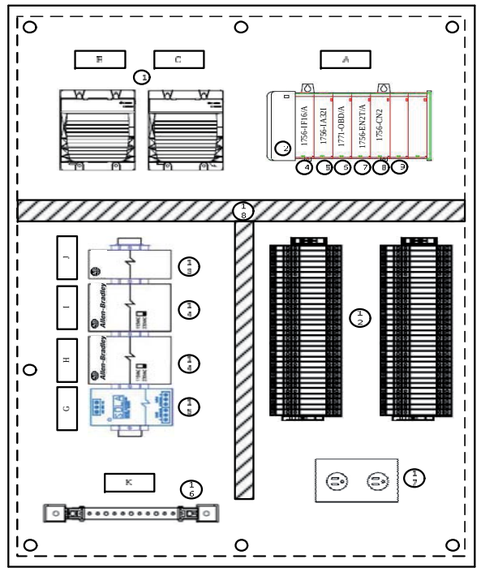
Item #	Item	Elegir una opción			Comentarios
1	¿Los procedimientos para manejo de cambios han sido seguidos para las actividades de desmantelamiento?	SI	NO	N/A	
2	¿Se ha evaluado el impacto en unidades de operación adyacentes e infraestructura?	SI	NO	N/A	
3	¿Hay procedimientos para mantener la seguridad del proceso durante el desmantelamiento?	SI	NO	N/A	
4	¿Hay procedimientos que definan el nivel de autorizacion requerida para el desmantelamiento?	SI	NO	N/A	

ANEXO 6

ARMARIO PRIMARIO



ARMARIO SECUNDARIO



Lista de Materiales			
ITEM	CANT.	NUM. DE PARTE	DESCRIPCIÓN
1	3	1756-PAR2	FUENTE DE ALIMENTACION 85-265 VAC
2	3	1756-A7	CHASIS PARA ENSAMBLAJE (7 SLOTS)
3	2	1756-L61	PROCESADOR CONTROLLOGIX
4	1	1756-IF16/A	MODULO DE ENTRADAS ANALOGICAS
5	1	1756-IA16I	MODULO DE ENTRADAS DIGITALES
6	1	1771-OBD/A	MODULO DE SALIDAS DIGITALES
7	3	1756-EN2T/A	MODULO DE COMUNICACIÓN ETHERNET
8	3	1756-CN2	MODULO DE COMUNICACIÓN CONTROLNET
9	2	1756-RM	MODULO REDUNDANTE
10	1	DLINK	SWITCH ETHERNET
11	2	-	RIEL DIN
12	24	1492-H6	BLOQUE DE FUSIBLES
13	3	-	FUENTE DE ALIMENTACION MODULO REDUNDANTE
14	2	-	FUENTE DE ALIMENTACION 110 VAC -13/32 VDC 10A
15	2	STV 25K-10S	SUPRESOR DE PICOS 110 VAC
16	2	-	BARRA PARA ATERRAMIENTO
17	2	-	TOMA ELECTRICA 110 VAC
18	4	-	CONDUCTO PARA CABLEADO

Placa de identificación		
ITEM	CANT.	ETIQUETA
A	1	PLC PRINCIPAL
B	1	FUENTE DE ALIMENTACION DE PLC 1
C	1	FUENTE DE ALIMENTACION DE PLC 2
D	1	PLC SECUNDARIO
E	1	FUENTE DE ALIMENTACION DE PLC 3
F	1	FUENTE DE ALIMENTACION DE PLC 4
G	1	MODULO SUPRESOR
H	1	FUENTE DE ALIMENTACION
I	1	FUENTE DE ALIMENTACION
J	1	FUENTE DE ALIMENTACION MODULO REDUNDANTE
K	1	PUESTA A TIERRA

INGENIERIA/REGISTRO DISEÑO	FIRMA	FECHA
DIBUJANTE: FERNANDO VENEGAS		
ING. DISEÑO: FERNANDO VENEGAS		
REVISADO: RAFAEL BARRETO		
ING. PROYECTO: FERNANDO VENEGAS		
APROBACIÓN GRAL: RAFAEL BARRETO		

CLIENTE: TUGALT

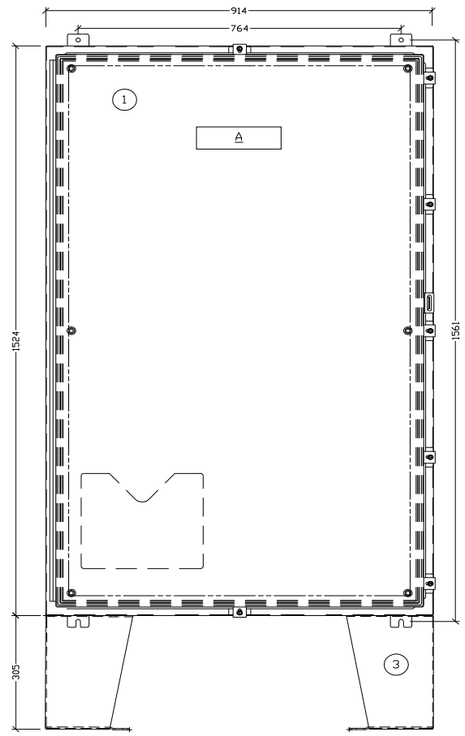
PROYECTO: DISEÑO DE SIS PARA EL AREA DE ALMACENAMIENTO DE COMBUSTIBLE

DESCRIPCION: LAYOUT DE ARMARIOS PARA EQUIPOS DEL SISTEMA DE SEGURIDAD.

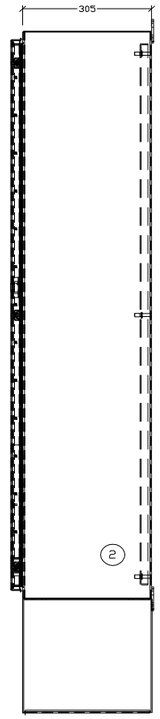
TAMAÑO:

ESCALA: S/E

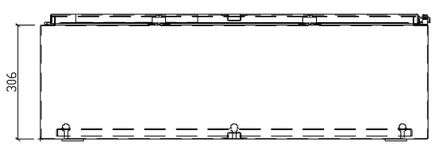
HOJA: 1 DE 1



(FRONT VIEW)



(SIDE VIEW)



(TOP VIEW)

Lista de Materiales			
ITEM	CANT	NUM. DE PARTE	DESCRIPCIÓN
1	1	A603612LP	ARMARIO IP 65
2	1	A60P36	PANEL (57"X33")
3	1	AFK1212SS	KIT DE SOPORTE

Placa de identificación		
ITEM	CANT	ETIQUETA
A	1	ARMARIO PARA PLC (PRINCIPAL Y SECUNDARIO)

INGENIERIA/ REGISTRO DISEÑO		FIRMA	FECHA
DIBUJANTE:	FERNANDO VENEGAS		
ING. DISEÑO:	FERNANDO VENEGAS		
REVISADO:	RAFAEL BARRETO		
ING. PROYECTO:	FERNANDO VENEGAS		
APROBACIÓN GRAL:	RAFAEL BARRETO		

CLIENTE: **TUGALT**

PROYECTO: **DISEÑO DE SIS PARA EL AREA DE ALMACENAMIENTO DE COMBUSTIBLE**

DESCRIPCION: LAYOUT DE ARMARIOS PARA EQUIPOS DEL SISTEMA DE SEGURIDAD.

TAMAÑO:

ESCALA: S/E

HOJA: 2 DE 2

Glosario

ALARP	As Low As Reasonably Practical (Tan bajo como sea razonablemente factible).
BPCS	Basic Process Control System (Sistema de Control Básico de Procesos) **.**
$\boldsymbol{\beta}$	Factor de falla común.
CCF	Common Cause Failure (Fallas de causa común).
DC	Diagnostic Coverage (Cobertura del Diagnóstico).
DCS	Distribuited Control System (Sistema de Control Distribuido).
DD	Dangerous Detected (Peligro detectado).
DN	Dangerous No Detected (Peligro nunca detectado).
DU	Dangerous Undetected (Peligro no detectado).
E/E/PE	Electrical/Electronic/Programmable Electronic (Eléctricos/Electrónicos/Electrónicos Programables).
EMI	ElectroMagnetic Interference (Interferencias Electromagnéticas).
EUC	Equipment Under Control (Equipo bajo control).
FAT	Factory Acceptance Test (Pruebas de aceptación en la fábrica).
FTA	Fault Tree Analysis (Análisis de árboles de falla).
FMEA	Failure Mode and Effect Analysis (Análisis de Modo y Efecto de Falla).
HAZOP	Hazards and Operability Studies (Estudio de Peligros y Operabilidad).
HHT	Horas Hombre Trabajadas.
HMI	Human Machine Interface (Interfaz humano-máquina).
IEC	International Electrotechnical Commission (Comisión Electrotécnica Internacional).
IF	Índice de Frecuencia.
IG	Índice de Gravedad.
ISA	International Society of Automation. (Sociedad Internacional de Automatización).
LOPA	Layers Of Protection Analysis (Análisis de la capa de protección).
LVL	Limited Variability Language (Lenguaje de Variabilidad Limitada).
$\boldsymbol{\lambda_S}$	Tasa de fallas seguras.
$\boldsymbol{\lambda_{DU}}$	Tasa de fallas peligrosas no detectadas.
$\boldsymbol{\lambda_{DD}}$	Tasa de fallas peligrosas detectadas.
MDT	Mean Down Time (Tiempo medio de paro).
MTTF	Mean Time To Fail (Tiempo Medio para Fallas).
$\boldsymbol{MTTF_{SP}}$	Mean Time To Fail Spurious (Tiempo Medio para Fallas Esporádicas).
MTTR	Mean Time To Repair (Tiempo medio para reparación).
OSD	Operational Sequence Diagrams (Diagramas de secuencia operacional).

PFD	Probability of Failure on Demand (Probabilidad de Falla a la Demanda).
PST	Partial Stroke Test (Pruebas de cierre parcial).
RBD	Reability Block Diagrams (Diagramas de Bloque de Confiabilidad).
RFI	Radio Frecuency Interference (Interferencias por Radio Frecuencia).
RRF	Risk Reduction Factor (Factor de Reducción de Riesgo).
SAT	Site Acceptance Test (Pruebas de aceptación en el sitio).
SFF	Safe Failure Fraction **(**Fracción de Falla Seguro).
SIF	Safety Instrumented Function (Función Instrumentada de Seguridad).
SIL	Safety Integrity Level (Nivel de Integridad de Seguridad).
SIS	Safety Instrumented System (Sistema Instrumentado de Seguridad).
SO	Spurious Operation (Operación esporádica).
SRS	Safety Requirements Specification (Especificación de Requerimientos de Seguridad).
SS	Spurious Shutdown (Apagado esporádico).
ST	Spurious Trip (Activación esporádica).
STR	Spurious Trip Rate (Tasa de activaciones esporádicas).
TD	Test Duration (Duración de la prueba).
$\boldsymbol{TI_A}$	Automatic Test Interval (Intervalo de prueba automático).
$\boldsymbol{TI_M}$	Manual Test Interval (Intervalo de prueba manual).
TR	Tasa de Riesgo.
TÜV	Technischer Überwachungs-Verein.
$\boldsymbol{\tau_{FT}}$	Intervalo de prueba funcional.
$\boldsymbol{\tau_{DT}}$	Intervalo de prueba de diagnóstico.

BIBLIOGRAFIA

[1]. H. S. E. (2003). *Out of control*. HSE Books.

[2]. G. D. Castro. (2000). *La tragedia de Bhopal*. Centro de Investigaciones Toxicológicas.

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

[4]. IEC 61511. (2003). *Funtional safety-safety instrumented systems for the process industry*. International Electrotechnical Commission.

[5]. Cyr, M. (2013, Abril). *The West Texas Fertilizer Plant Explosion Was Not a Freak Event.* Scientific American.

[6]. Guía para procedimientos. (2009). *Clasificación de las emergencias y otros servicios*. Benemérito Cuerpo de Bomberos, Valparaíso.

[7]. Del Collado, F. (2012, Septiembre). *Incendio en refinería de ciudad Madero, no hay lesionados.* Noticias Terra.

[8]. C. R. R. Fire. (2012). Interim investigation report.

[9]. Ghosh, A. (2004). *Trains in Process Safety*. ARC Adevisory Group.

[10]. Gruhn, P. y Cheddie, H. (2006) *Safety instrumented systems: design, analysis, and justification.* The Instrumentation, Systems, and Automation Society.

[11]. Hauge, S., Lundteigen, M. A., Hokstad, P. y Håbrekke, S. (2010). *Reliability Prediction Method for Safety Instrumented Systems*, SINTEF report STF50A, 6031.

[12]. ISATR 84.00.02. (2002). *ISA-TR84.00.02-2002-Part 4*: *safety instrumented functions (SIF), safety integrity level (SIL) evaluation techniques part 4: determining the SIL of a SIF via Markov analysis*. Research Triangle Park, NC: The Instrumentation, Systems, and Automation Society.

[13]. ISA. (2002). *Safety Instrumented Functions (SIF)-Safety Integrity Level (SIL) Evaluation Techniques Part 2: Determining the SIL of a SIF via Siplified Equations*. Systems ISA International Society of Automation. Technical Report, p44.

[14]. Lagori, J. F. (2003). *El Accidente de Chernobil: La Utilización de un Sistema de Unidades Adecuado*. Universidad de Alcalá, p20 – 55.

[15]. Langeron, Y., Barros, A., Grall, A., y Bérenguer, C. (2007). *Safe failures impact on safety instrumented systems. Risk, reliability, and societal safety*, vol:1, p641 – 648.

[16]. Lloret, C. (2012, Agosto). *Reporta Pemex cuatro heridos durante incendio en refinería Madero*. Noticias Excelsior.

[17]. Lundteigen, M. A. (2009). *Safety instrumented systems in the oil and gas industry.* (Tesis PhD), Departamento de Producción e Ingeniería de Calidad. Universidad Trondheim. Noruega.

[18]. Lundteigen, M. A. y Rausand, M. (2007). *Common cause failures in safety instrumented systems on oil and gas installations: Implementing defense measures through function testing.* Journal of Loss Prevention in the process industries, 20(3), p218 – 229.

[19]. Lundteigen, M. A. y Rausand, M. (2007). *The effect of partial stroke testing on the reliability of safety valves*. Risk, Reliability and Societal Safety. Londres.

[20]. Lundteigen, M. A. y Rausand, M. (2008). *Spurious activation of safety instrumented systems in the oil and gas industry: Basic concepts and formula*s. Reliability engineering & system safety, 93(8), p1208 – 1217.

[21]. Macdonald, D. (2004, Marzo). *Practical hazops, trips and alarms*. Newnes.

[22]. Marzal, E. y Scharpf, E. (2002). *Safety Integrity Level Selection*. The Instrumentation and Automation Society.

[23]. PDS method handbook. (2006). *Reliability prediction methods for safety instrumented systems*.

[24]. Naranjo, E. (2012, Noviembre). *Incendio en La Fabril*. Diario La Hora.

[25]. Parry, G. W. (1991). *Common cause failure analysis: A critique and some suggestions*. Reliability Engineering & System Safety, 34(3), p309 – 326.

[26]. Paula, H. M., Campbell, D. J. y Rasmuson, D. M. (1991). *Qualitative cause-defense matrices: Engineering tools to support the analysis and prevention of common cause failures*. Reliability Engineering & System Safety, 34(3), p389 – 415.

[27]. Rausand, M. y Høyland, A. (2004). *System reliability theory: Models, statistical methods, and applications*, vol.3, John Wiley & Sons.

[28]. Smith, D. J. (2011). *Reliability, maintainability and risk: Practical safety-related systems engineering methods*. Access Online via Elsevier.

[29]. Smith, D. J. y Simpson K. G. L. (2010). *Safety Critical Systems Handbook: A Straightfoward Guide to Functional Safety, IEC 61508 and Related Standards, Including process IEC 61511*. *Access Online via Elsevier*.

[30]. Summers A. y Zachary B. (2002). *Improve facility SIS performance and reliability: Plant safety and reliability*. Hydrocarbon processing, 81(10), p71 – 74.

[31]. Summers, A. E. (2002). *Viewpoint on ISA TR84. 0.02 Simplified methods and fault tree analysis*. ISA transactions, 39(2), p125 – 132.

[32]. Summers, A. E. y Raney G. (1999). *Common cause and common sense, designing failure out of your safety instrumented systems (SIS)*. ISA transactions, 38(3), p291 – 299.

[33]. Summers, A. E., Raney G. y Dejmek, K. A. (1999). *Safeguard safety instrumented systems*. Chem. Eng. Prog., 95(11), p85 – 90.

[34]. Vincoli, J. W. (2006). *Basic guide to system safety*. Wiley-Interscience, New York.

[35]. Watson, I. A. y Edwards, G. T. (2001). *Common-mode failures in redundancy systems*. Nucl. Technol. 46(2).

[36]. SINTEF Industrial Management. (2004*). Offshore Reliability Data for Worldwide Oil Company Operations*, fases VII-VIII. OREDA project.

[37]. Rockwell Automation. (2008). *ControlLogix SIL2 System Configuration, Application Techniques* (Catalog Numbers 1756 and 1492).

UNIVERSIDAD POLITÉCNICA SALESIANA

UNIDAD DE POSGRADOS

MAESTRÍA EN CONTROL Y AUTOMATIZACIÓN INDUSTRIALES

Autor:
Ing. Klever Fernando Benegas Riera.

Director:
Ing. Rafael Barreto J., M. Sc.

LA SEGURIDAD FUNCIONAL EN LA INDUSTRIA DE PROCESOS: CONCEPTOS Y METODOLOGIAS DE DISEÑO

Esta tesis es el resultado de un proyecto de tesis de maestría en control y automatización industriales para la Universidad Politécnica Salesiana (UPS). El trabajo fue llevado a cabo entre abril de 2013 y enero de 2014, en estrecha colaboración con el director de tesis, Rafael Barreto Jijón, y su contribución se refleja a lo largo del desarrollo de este proyecto. El Ing. Giovanny Quinde, jefe de seguridad del grupo Graiman ha contribuido como supervisor debido a su amplia experiencia en la seguridad industrial.

El proyecto de tesis de maestría ha sido una oportunidad para hacer contribuciones a un campo en el que se ha tomado gran interés, a saber, la fiabilidad de los sistemas instrumentados de seguridad. Se espera que el conocimiento aquí desarrollado sea utilizado como base para el avance e implementación de sistemas instrumentados de seguridad en la industria de procesos, desarrollando diseños fiables y garantizando el funcionamiento de tales sistemas.