Criterios para el diseño de un Sistema Instrumentado de Seguridad en calderas industriales

Hanns Peter Hurtado Patiño
Ángela Marcela Luna Ordoñez

Universidad del Cauca
Facultad de Ingeniería Electrónica y Telecomunicaciones
Departamento de Electrónica, Instrumentación y Control
Ingeniería en Automática Industrial
Popayán, Mayo de 2012

Criterios para el diseño de un Sistema Instrumentado de Seguridad en calderas industriales

Documento Final de Trabajo de Grado para optar al título de
Ingeniero en Automática Industrial

Hanns Peter Hurtado Patiño
Ángela Marcela Luna Ordoñez

Director: Ing. Oscar Amaury Rojas Alvarado

Universidad del Cauca
Facultad de Ingeniería Electrónica y Telecomunicaciones
Departamento de Electrónica, Instrumentación y Control
Ingeniería en Automática Industrial
Popayán, Mayo de 2012

TABLA DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

INTRODUCCIÓN

Para las empresas sigue siendo primordial el empleo de calderas industriales por su buen rendimiento y bajo costo, pero la desviación de variables como el nivel, la presión, la temperatura o la combustión, pueden originar implosiones o explosiones, provocando daños por la propagación de la onda de presión liberada, llamas, escapes de fluidos, fragmentos que salen proyectados, entre otros peligros. Las calderas industriales tienen un sistema de seguridad interno y deben cumplir con un estricto mantenimiento en su estructura física para prevenir accidentes en activos de la empresa, comunidad y medio ambiente, pero estos procedimientos de seguridad no son suficientes; por esta razón las normas internacionales de seguridad han establecido estrategias, como lo es la implementación de un sistema instrumentado de seguridad adicional al sistema de seguridad interno de las unidades de proceso que generan más riesgo, para poder prevenirlos.

La necesidad de diseñar y operar sistemas de forma más segura y económica se convirtió en una necesidad que va en aumento y que se puede conseguir con la aplicación de estándares internacionales de seguridad funcional como el estándar ANSI/ISA 84 que describe las etapas del ciclo de vida de un sistema instrumentado de seguridad, el cual constituye la última capa de seguridad preventiva y es definido como: un sistema compuesto por sensores, controladores de lógica y elementos finales con el propósito de llevar el proceso a un estado seguro por medio de funciones de seguridad e índices de seguridad de disminución del riesgo cuando determinadas condiciones pre-establecidas son violadas [1].

Diseñar un sistema instrumentado de seguridad basándose en la norma ISA 84 es una labor compleja porque suministra definiciones, un marco amplio de referencias y una guía de implementación de un sistema instrumentado de seguridad genérico no prescriptivo, haciendo difícil su comprensión y aplicación. Desde la etapa inicial, análisis del nivel del riesgo en procesos industriales, hasta la determinación de las funciones instrumentadas de seguridad; los requisitos de seguridad y la instrumentación, no especifica bajo que criterios se debe realizar [2], dejando al personal de empresas manufactureras y expertos en seguridad funcional en libertad para efectuar de manera autónoma y flexible la aplicación de sus lineamientos.

El presente trabajo aborda los criterios para desarrollar las etapas de diseño de un sistema instrumentado de seguridad en calderas industriales pirotubulares, basados en los lineamientos de la norma ISA 84, una guía de aplicación y el resultado en una empresa caso de estudio.

1. DESCRIPCION DE LA NORMA ANSI/ISA 84

Estándares internacionales de seguridad funcional como lo son IEC 61508, IEC 61511 y ANSI/ISA 84 orientan sobre el diseño, instalación, operación y mantenimiento de un sistema instrumentado de seguridad para la protección contra peligros por errores funcionales y/o humanos en plantas químicas, petroquímicas, siderúrgicas, metalúrgicas, plantas donde haya generación de energía no nuclear, en procesos donde se pueden presentar fugas de sustancias tóxicas, fluidos de alta presión y temperatura, como lo es en calderas, hornos, torres de destilación, quemadores y en general en cualquier proceso industrial. Estas normas además fueron creadas para que empresas manufactureras pudieran demostrar que sus procesos operan de forma segura y de esta manera cumplan con entes reguladores de seguridad a nivel nacional e internacional.

En 1995, El Ejecutivo Británico de Salud y Seguridad (Health and Safety Executive - HSE) publicó un artículo titulado “Fuera de control” (Out of Control) donde se discute por qué los sistemas fallan y como prever que los mismos fallen. En él se analiza el origen de las causas de varios accidentes industriales los cuales fueron iniciados por fallas en los equipos de control, creando un importante precedente como lo es la publicación de esta famosa gráfica sobre el origen que ocasionaron las fallas en el ciclo de vida de los sistemas [3].

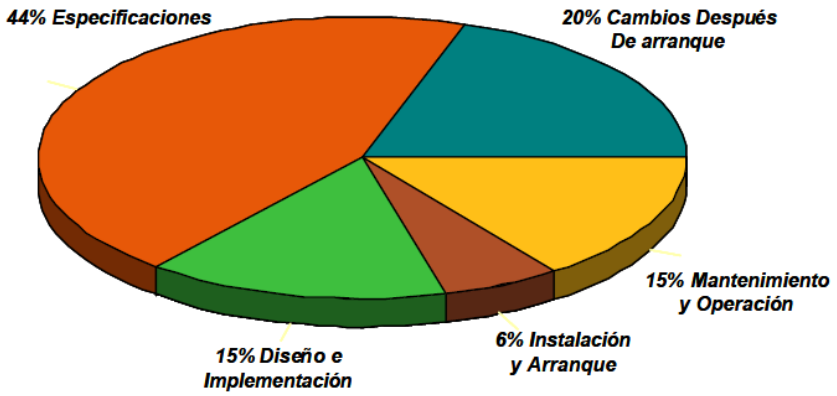

Figura 1. Origen de accidentes

El resultado de este estudio llevó al desarrollo de “el ciclo de vida” de seguridad funcional, definido en estándares internacionales como la ISA S84.01 de 1996, la IEC 61508 de 1998, la IEC 61511 del 2003 y la ANSI/ISA S84.00.01 del año 2004.

El Ciclo de Vida de Seguridad Funcional (CVSF) es simplemente una metodología práctica que orienta los pasos necesarios a seguir para alcanzar la seguridad integral de las plantas de proceso documentando cada fase, ayudando a prevenir las fallas identificadas en el estudio del Ejecutivo Británico de Seguridad y Salud.

Las fases del CVSF están dirigidas a resolver el origen de los accidentes como los identifica el estudio de UK HSE. En la fase de análisis, el CVSF está enfocado en resolver y evitar el 44% de las fallas debidas a especificaciones inadecuadas. Esto

se busca mediante técnicas en el análisis de riesgo y en reducción de riesgo cuyos resultados finales son las “Especificaciones y Requerimientos de Seguridad Funcional”. La fase de diseño, está enfocada a disminuir el 15% de los accidentes causados por errores y/u omisiones durante el diseño, la implementación, la instalación y la puesta en servicio. También se señala la necesidad de la verificación documentada de que el diseño alcanza el nivel integral de seguridad funcional definido en la fase de análisis. La fase de implementación y operación busca disminuir o eliminar el 41% de los accidentes que son causados por incorrecta operación o mal mantenimiento además de cambios realizados después de que el sistema ha sido puesto en servicio.

La norma internacional ANSI/ISA 84 hace referencia a la aplicación de los sistemas instrumentados de seguridad para la industria de proceso. Tiene dos conceptos, que son fundamentales para su aplicación: ciclo de vida de seguridad y los niveles de integridad de seguridad. El ciclo de vida de la seguridad constituye el marco fundamental que une a la mayoría de los conceptos, orientando sobre el diseño, instalación, operación y mantenimiento de un sistema instrumentado de seguridad, para la protección contra peligros por errores funcionales y/o humanos en plantas.

Diseñar un sistema instrumentado de seguridad basándose en la norma ANSI/ISA 84 es una labor compleja porque esta norma sólo suministra definiciones, un marco amplio de referencias de un sistema instrumentado de seguridad y una guía para la determinación del nivel integrado de seguridad genérico no prescriptivo, haciendo difícil su comprensión y aplicación.

Desde la etapa inicial, análisis del nivel del riesgo en procesos industriales, hasta la determinación de las funciones instrumentadas de seguridad, la instrumentación y los requisitos de seguridad, no hay criterios y especificaciones sobre cómo realizarlas, dejando al personal de empresas manufactureras y expertos en seguridad funcional en libertad para efectuar de manera autónoma y flexible la aplicación de sus lineamientos.

La Figura 2 muestra el ciclo de vida de seguridad funcional como se define en la norma ANSI/ISA 84.00.01 – 2004, y la Tabla 1, describe la información requerida para desarrollar cada etapa y los resultados obtenidos en cada una de estas [1].

Para obtener un buen diseño y reducir el 50% el origen de las fallas de los procesos, particularmente en las calderas industriales es necesario profundizar en los temas del ciclo de vida definidos por la norma ANSI/ISA 84 sombreados en color azul.

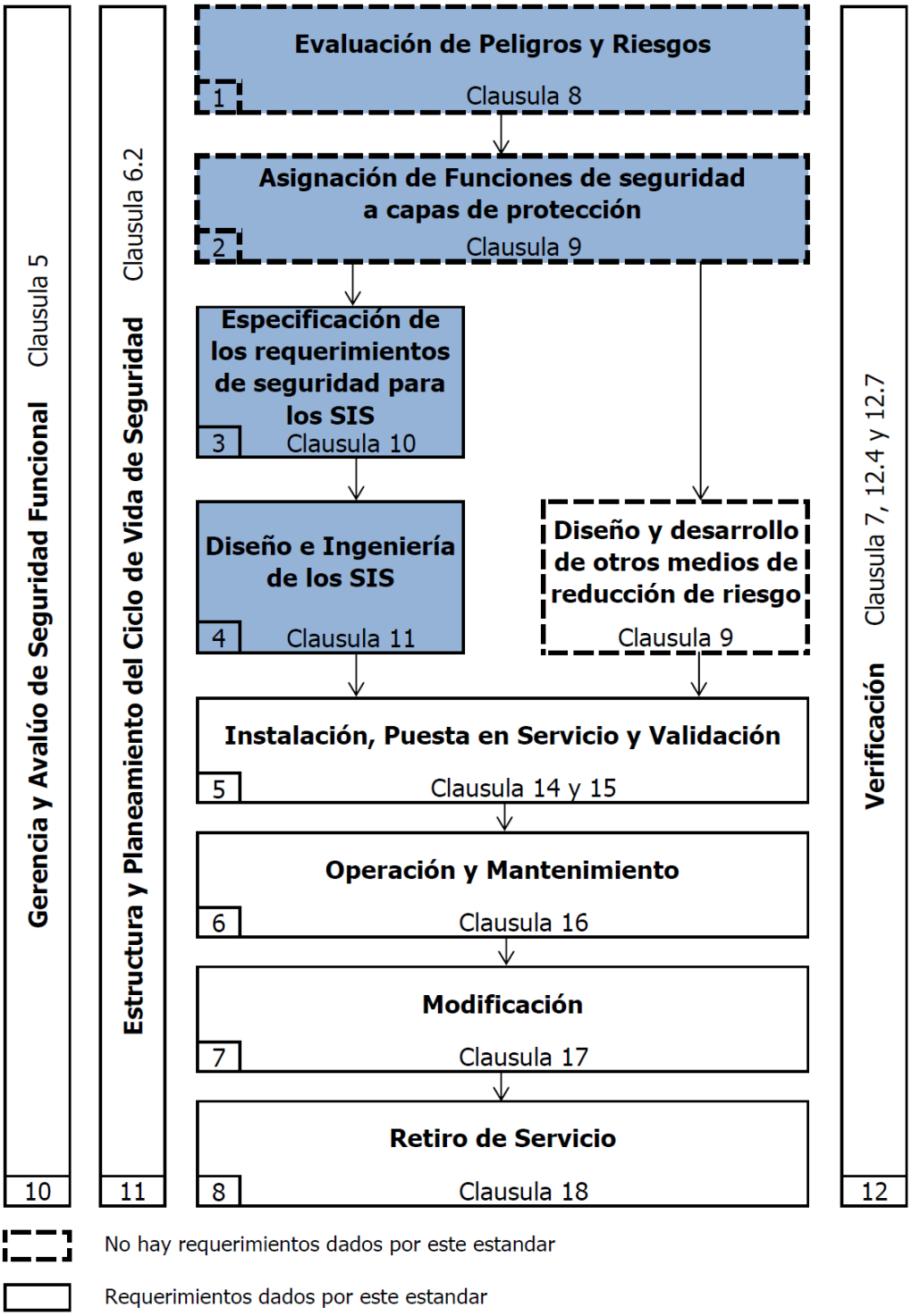

Figura 2. Fases del Ciclo de Vidad de Seguridad del SIS y Evaluacion Funcional de Seguridad

El objetivo por el cual se requiere cada etapa del ciclo de vida de un sistema instrumentado de seguridad es:

- **Evaluación de peligros y riesgos:** El objetivo es determinar los peligros y los eventos peligrosos del proceso y su equipo asociado, la secuencia de eventos

que lleven a un evento peligroso, el riesgo del proceso asociado a los eventos peligrosos, los requerimientos de reducción de riesgo y las funciones de seguridad requeridas para alcanzar la reducción de riesgo necesaria. En esta etapa las técnicas PHA (Process Hazard Analysis) permiten llevar a cabo este objetivo.

- **Asignación de funciones de seguridad a capas de protección:** El objetivo es la asignación de las funciones de seguridad o medidas de reducción del riesgo a las capas de protección y luego a cada función instrumentada de seguridad su respectivo nivel de integridad de seguridad, por medio de técnicas de determinación SIL.

- **Especificación de los requerimientos de seguridad del SIS:** El objetivo es especificar los requerimientos para cada una de las funciones instrumentadas de seguridad, con la finalidad de cumplir con los requerimientos de seguridad funcional.

- **Diseño e ingeniería del SIS:** El objetivo es diseñar el SIS para que cumpla con los requerimientos de las funciones instrumentadas de seguridad e integridad de seguridad.

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

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

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

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

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

- **Asignación de seguridad funcional del SIS**: El objetivo es investigar y llegar a la conclusión de que la seguridad funcional del SIS ha sido alcanzada.

En la siguiente tabla se describe las entradas y salidas de cada etapa [1]:

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

Tabla 1. Entradas y Salidas de las Etapas del Ciclo de Vida de Seguridad

La norma ANSI/ISA 84.00.01 se divide en tres partes bajo el título genérico de: **“Seguridad Funcional: Sistemas Instrumentados de Seguridad para el sector de la Industria del Proceso”.**

Parte 1: Estructura, Definiciones, Sistema, Requerimientos de Hardware y Software – Normativa [1].

Esta parte de la norma describe sobre el diseño, instalación, operación y mantenimiento de un sistema instrumentado de seguridad, partiendo de que los sistemas de protección pueden depender de diferentes tecnologías (química, mecánica, hidráulica, neumáticos, eléctricos, electrónicos, electrónica programable).

Para facilitar este enfoque, la norma requiere el desarrollo de evaluación de peligros y riesgos para identificar los requisitos de seguridad. Además, demanda la asignación de los requisitos de seguridad para el sistema instrumentado de seguridad.

Parte 2: Orientación para la aplicación de la ANSI/ISA-84.00.01-2004 Part 1 [4].

Ofrece orientación sobre el diseño, instalación, operación y mantenimiento de las funciones instrumentadas de seguridad y relacionadas con la seguridad del sistema instrumentado como se define en ANSI/ISA-84.00.01 -2004 Parte 1 (IEC 61511-1 MOD).

Parte 3: Guia para la determinación de los Niveles Integrales de Seguridad (SIL – Safety Integrity Levels) – Informativa. [5]

Proporciona una visión general sobre diferentes métodos que permiten calcular el nivel integrado de seguridad de cada función instrumentada de seguridad. Estos métodos son cualitativos, semi-cuantitativos y cuantitativos.

La norma ISA 84.00.01 sugiere iniciar el análisis de riesgo con la definición del objetivo de seguridad. Seguidamente se debe recurrir a las técnicas de análisis de riesgo en procesos (PHA), para calcular el nivel del riesgo y determinar las medidas de reducción del riesgo, para asignar estas funciones de seguridad a las capas de protección. Las funciones de seguridad que hacen parte de la capa de protección de un sistema instrumentado de seguridad se denominan funciones instrumentadas de seguridad, las cuales requieren la asignación de un nivel integrado de seguridad (SIL) con sus respectivas especificaciones de requerimientos para llevar a cabo el diseño del SIS.

En general este estándar ilustra y aborda las actividades del ciclo de vida de seguridad funcional que ayudarían al usuario a alcanzar los requerimientos mínimos definidos. Este enfoque ha sido adoptado para que siempre se use la misma política racional y consistente. Para facilitar esta tarea, el estándar:

1. Requiere que se haga una evaluación del peligro y el riesgo envuelto, para identificar los requerimientos de seguridad.
2. Especifica que los requerimientos de seguridad sean asignados al sistema instrumentado de seguridad.

3. Está enmarcado en un ambiente en el cual puede ser aplicable a todos los métodos para alcanzar seguridad funcional.
4. Detalla ciertas actividades tales como la gestión de seguridad funcional, que pueden aplicarse a cualquier método para alcanzar seguridad funcional.

De igual manera, el estándar, identifica varias condiciones o cláusulas que deben de ser cumplidas para acreditar el seguimiento del mismo [1].

Cláusula 5 – Gestión de la Seguridad Funcional: La norma exige que la política y estrategia para alcanzar la Seguridad Funcional, deba estar definida e identificada junto con los medios para evaluar si se ha alcanzado el nivel requerido, y debe ser comunicada dentro de la organización.

Cláusula 6 – Requerimientos del Ciclo de Vida de Seguridad Funcional: La norma orienta en cada fase además de establecer los requerimientos de las actividades técnicas del ciclo de vida de Seguridad Funcional, de forma que puedan organizarse para asegurar que existe o está siendo desarrollada una planificación adecuada que permita alcanzar los requerimientos de seguridad funcional.

Cláusula 8 – Peligros en el Proceso y Análisis de Riesgo: La norma sugiere realizar una identificación del peligro o eventos peligrosos del proceso y los equipos asociados al mismo que pueden provocar daños irreversibles al personal, equipos y medio ambiente.

Cláusula 9 – Asignación de Funciones de Seguridad a las capas de Protección: El objetivo de esta cláusula es que el usuario pueda asignar funciones de Seguridad a cada capa de protección y determine su nivel integral de seguridad asociado a dicha función.

Cláusula10 – Especificaciones de los Requerimientos de Seguridad Funcional de un SIS: La norma recomiendo algunos de los requerimientos de la o las Funciones Instrumentadas de Seguridad Funcional (SIF). Los requerimientos de seguridad funcional serán derivados de las asignaciones de SIF y de los requerimientos identificados durante la planificación de la seguridad funcional.

Cláusula 11 – Diseño e Ingeniería de un SIS: El objetivo de los requerimientos de esta cláusula es el diseñar uno o varios SIS para proveer las SIF y alcanzar el nivel integral de seguridad (SIL) especificado.

2. ANÁLISIS DE RIESGO

Actualmente la industria debe realizar estudios sobre los peligros en sus procesos para minimizar el nivel del riesgo, ya que dejar el proceso en manos de equipos significa una mayor producción pero inherentemente tiene un nivel de riesgo, que podría implicar grandes pérdidas económicas, lesiones o muertes en el personal y/o comunidad, daños al medio ambiente y a la imagen corporativa de la empresa.

Numerosas compañías de la industria implantan su propio sistema de gestión de seguridad, porque se ha comprobado a largo plazo que operar una planta más segura conduce a una industria más eficiente y así obtener las exigentes certificaciones de organismos nacionales y/o internacionales.

En las empresas ocurren eventos que se pueden clasificar como accidentes indeseados, como escapes tóxicos, explosiones e incendios, teniendo como causas más comunes los fallos en los dispositivos electrónicos, exceso de límites de operación, perturbaciones externas y fallos humanos.

Los efectos de dichos accidentes se multiplican debido a la proximidad entre las instalaciones industriales, facilitando que se produzca el llamado efecto dominó, que no es más que la propagación de accidentes entre diferentes instalaciones.

El Peligro, de acuerdo con la Administración de Seguridad y Salud Ocupacional (OSHA) "una característica física o química que tiene el potencial para causar daño a las personas, los bienes o el medio ambiente, por la combinación de un material peligroso, un entorno operativo, y ciertos eventos no planificados que podrían resultar en un accidente" [6]. **El riesgo es el producto de las consecuencias y frecuencias de un evento peligroso** y se puede expresar cuantitativamente de la siguiente manera:

a) Interrupción en la producción (costo/año).
b) Daños a Equipos (costo).
c) Lesiones a personas (costo/año) o (Fatalidades /año).
d) Impacto Ambiental (costo/año).

Los estándares en seguridad funcional fueron desarrollados para garantizar la seguridad que depende del funcionamiento correcto del proceso o equipo en respuesta a sus entradas y para ayudar a evitar que ocurran accidentes en la planta. La seguridad funcional cubre una amplia gama de dispositivos que son utilizados para crear sistemas de seguridad. Dispositivos como enclavamientos, cortinas de luz, relés, PLC, contactores y variadores de velocidad se interconectan para formar un sistema de seguridad, para realizar una función de seguridad.

La norma ISA 84.00.01 en sus tres partes sugiere diferentes técnicas para iniciar el análisis de riesgos en procesos (PHA) para determinar el nivel del riesgo y establecer medidas de reducción del riesgo.

2.1. DEFINICION DE OBJETIVO DE SEGURIDAD

La definición de un objetivo de seguridad debe ser descrita con el apoyo de normas nacionales e internacionales, reglamentos nacionales como el reglamento técnico colombiano, políticas corporativas y los aportes de las partes interesadas, como la comunidad, la jurisdicción local y empresas aseguradoras. ***EL riesgo aceptable o el objetivo de seguridad se puede definir como el nivel del riesgo que permite establecer hasta qué punto se puede aceptar que una operación pueda causar eventuales daños y que nivel de gravedad es aceptable para ese daño*** [7]. Los objetivos de seguridad o los niveles de aceptación del riesgo son específicos por cada empresa, por lo tanto, no se debe generalizar a menos que los reglamentos y normas existentes brinden apoyo.

Al analizar la consecuencia sobre los efectos de los riesgos en la población, medio ambiente y empresa, se debe categorizar las consecuencias en escalas de severidad, por ejemplo: consecuencias catastróficas, graves, moderadas o menores.

Los factores que se deben tener en cuenta para determinar las consecuencias son:

- **Las personas:** involucra daños en la salud, incapacidades temporal o permanente, lesiones, hospitalizaciones, muertes y seguridad al personal de la empresa y la comunidad, considerando costos de litigio o costos legales asociados con estos daños.

- **Medio ambiente:** contaminar ríos, lagos, causar erosión en la tierra, generar olores desagradables, ruidos fuertes, emisión de polvo, humo, nubes toxicas y partículas en el aire implican altas sumas de dinero en sanciones legales.

- **La empresa:** el patrimonio de la empresa, la imagen de la empresa, pérdidas de producción, la instalación, los costos asociados con el remplazo o reparación de equipos dañados, construcción o modificación a la estructura física de la empresa.

La probabilidad o frecuencia de un riesgo se basa en la mayoría de los casos en el historial (cuántas veces se produjo el hecho en un período de tiempo, en la organización). En la determinación de la frecuencia se utiliza un soporte cuantitativo basado en una estimación de eventos ocurridos en el pasado, con lo cual se obtiene una mejor aproximación a la probabilidad de ocurrencia del evento.

Un ejemplo de valorización de la frecuencia se puede determinar cualitativamente asignando a los riesgos calificaciones dentro de un rango, que podría ser de 1 a 4 (remota (1), baja (2), media (3), alta (4)) o se podría estimar cuantitativamente utilizando rangos de tiempo en años de las veces que ocurriría, un accidente se podría presentar entre 1 y 10 años, entre 10 y 100 años y entre 100 y 1.000 años.

La Tabla 3 ejemplifica los riesgos valorizados en sus regiones para una serie de consecuencias y frecuencias considerando factores sociales, políticos y económicos [5]. En esta matriz donde se cruzan el nivel de la consecuencia y la probabilidad, indica el nivel de riesgo de cada escenario de peligro identificado. No existe un tamaño definido de la matriz, este queda a criterio de cada empresa.

PROBABILIDAD	CLASES DE RIESGOS			
	CONSECUENCIA CATASTROFICA	CONSECUENCIA CRITICA	CONSECUENCIA MARGINAL	CONSECUENCIA DESPRECIABLE
Muy Probable	I	I	I	II
Probable	I	I	II	II
Posible	I	II	II	II
Remoto	II	II	II	III
Improbable	II	III	III	III
Imposible	II	III	III	III
Las clases de riesgo I, II y III será la clasificación realizada por la empresa				

Tabla 2. Ejemplo de matriz de valorización de riesgos

2.2. SELECCIÓN DE TECNICAS PHA.

Las técnicas PHA representan un eslabón muy importante dentro de la cadena de seguridad y es una parte fundamental de todo sistema de gestión de seguridad. Las técnicas PHA deben dar como resultado la identificación de los eventos peligrosos del proceso y sus equipos asociados en cualquier instalación industrial, la valoración y clasificación del riesgo, la evaluación de las capas de seguridad existentes y acciones para prevenir riesgos, entre los que destacan:

- **Fuego:** incendios de charco, dardo de fuego (Jet Fire), incendio de llamarada, bola de fuego, fuegos en edificios y almacenes.

- **Explosión:** físicas y químicas, confinadas o no confinadas, BLEVE, por polvo, descomposición térmica, reacciones fuera de control.

- **Fuga tóxica:** emisión o escape de sustancias nocivas y/o tóxicas para la salud de las personas o para el medio ambiente.

- **Reactividad de sustancias:** descomposición descontrolada y compuestos inestables.

- Posibles peligros asociados a las sustancias industriales que son guardadas o procesadas en cantidades que superan los umbrales definidos para el nivel de riesgo por unidad de masa de la sustancia.

- Peligros asociados a las características de las sustancias presentes en el proceso:

  - ✓ Materias primas.
  - ✓ Productos intermedios.
  - ✓ Productos finales.
  - ✓ Subproductos.
  - ✓ Aditivos.
  - ✓ Catalizadores.
  - ✓ Corrientes de desecho.

- Posibles peligros debidos a materiales, equipos y sus condiciones de operación, como por ejemplo:

  - ✓ Altas presiones.
  - ✓ Altas temperaturas.
  - ✓ Salpicaduras de aceite caliente o contactos con vapor.
  - ✓ Superficies calientes.
  - ✓ Materiales criogénicos[1].
  - ✓ Alta energía cinética.
  - ✓ Alto voltaje / corriente / electricidad estática.

La evaluación de riesgos en un proceso por medio de las técnicas PHA se lleva a cabo como se muestra en la figura 3:

Figura 3. Entrada y salida de las técnicas PHA

Estas técnicas pueden determinar el nivel de riesgo presente en un equipo industrial de manera cualitativa y cuantitativa. Algunas técnicas son más especializadas e involucran una mayor complejidad matemática, de las cuales se aplican principalmente en el sector nuclear, en procesos industriales de sustancias altamente tóxicas, en escenarios de fallos complejos o si los cambios potenciales considerados son costosos.

[1] Criogénico: Produce o se relaciona a bajas temperaturas

La norma ISA 84.00.01 reconoce varias técnicas para realizar el análisis de riesgos, sin respaldar alguna en particular [5], y sugiere que las empresas desarrollen alguna técnica dependiendo de su necesidad, impulsando a conocer las siguientes técnicas PHA:

- **What if** (Que pasa si).
- **PrHA:** Preliminary Hazard Analysis (Análisis preliminar de peligros).
- **Check list** (Lista de chequeo).
- **Safety review** (Revisión de seguridad).
- **FMEA:** Failure Mode and Effects analysis (Análisis de modo de falla y de efectos).
- **HAZOP:** Hazard Operability analysis (Análisis de peligros y operatividad).
- **ETA:** Event Tree analysis (Análisis de árbol de eventos).
- **Relative Ranking** (Clasificación relativa de peligros).
- **FTA:** Fault Tree Analysis (Análisis de árbol de fallas).
- **CCA:** Cause and Consequence Analysis (Análisis de causa y consecuencia).
- **HRA:** Human Reliability Analysis (Análisis de fiabilidad humana).

Cada una de estas técnicas permite realizar un análisis de riesgo en cualquier proceso industrial; para ello sugieren descomponer el proceso en áreas, unidades de proceso, líneas de producción o máquinas, con el fin de identificar puntualmente el origen de peligros.

Estas técnicas permiten al usuario realizar un análisis de riesgo conforme a su experiencia, conocimientos del proceso o equipo a estudiar. Tienen las siguientes aplicaciones y características:

a) **What-if y Checklist:** identifican de forma cualitativa gran variedad de peligros generales de los procesos/sistemas con niveles bajos de peligrosidad. Es la técnica que requiere menor cantidad de información y de detalle de la misma, pero es muy importante disponer de experiencia en la operación del proceso.
b) **Relative ranking y PrHA:** se utilizan para tener una idea general de los peligros de un proceso a través de la realización de una clasificación de los mismos. En esta técnica se requiere alta experiencia del personal en el proceso e información sobre la distribución de la planta, tipos y tamaños del equipo e inventario de sustancias químicas.
c) **FMEA:** permite identificar los modos en los que pueden fallar los componentes del equipo eléctrico y mecánico. Requiere un conocimiento profundo de los modos de operación y fallo del equipo estudiado.
d) **Safety Review:** verifica el estado de un proceso existente que se puede adaptar para revisar zonas específicas donde hay mayor probabilidad de encontrar problemas de operación. Requiere información sobre accidentes previos y medidas de seguridad.

e) **HAZOP**: se utiliza para identificar y evaluar cualitativamente peligros y problemas de operabilidad de procesos con alto nivel de peligro. Requiere información detallada del proceso o equipo
f) **FTA**: determina de forma gráfica las causas y la probabilidad de que suceda un accidente o suceso importante (top event) en un sistema complejo.
g) **ETA**: establece de forma gráfica las consecuencias de un accidente o suceso iniciador en un sistema complejo.

FTA y ETA requieren gran cantidad de información, sobre todo en lo referente a medidas de seguridad y probabilidades de falla de los equipos. Evalúan escenarios de accidentes específicos provocados por fallos múltiples y que requieren resultados cuantitativos sobre la probabilidad de ocurrencia. Son muy apropiadas para sistemas altamente instrumentados, redundantes (sistemas de seguridad y de emergencia de varios niveles), como los sistemas de alarma y de cierre.

h) **HRA**: realiza un análisis cuantitativo de la actuación humana en sistemas complejos, evaluando la probabilidad de que ocurran los diferentes errores humanos en los escenarios de accidentes donde la actividad humana es relevante. Requiere información sobre la actuación humana en la operación del proceso y sobre las probabilidades de fallo humano.
i) **CCA**: proporciona un modelo gráfico que relaciona las causas y las consecuencias de escenarios de accidentes específicos en sistemas sencillos, donde la lógica del fallo que lo provoca es simple. Requiere gran cantidad de información, sobre todo en lo referente a medidas de seguridad y probabilidades de fiabilidad de los equipos.

Decidir qué técnica PHA se debe utilizar depende de la etapa del ciclo de vida en la que se encuentre el proyecto [8]. En la tabla 4 se resume la técnica que se debe aplicar de acuerdo con la complejidad de la etapa.

- **Investigación y desarrollo:**
  Esta etapa aparece en aquellos proyectos que se diseñan a partir de nuevas tecnologías o innovaciones de alguno existente, por lo que normalmente se carece de información detallada y sobretodo de experiencia en la operación del proceso.

- **Diseño conceptual:**
  Esta etapa es muy importante para el desarrollo posterior del diseño del proyecto, porque se intentan identificar los principales peligros asociados al mismo.

  Normalmente no se dispone de la suficiente información sobre el proceso para hacer recomendaciones de alternativas para controlar los peligros. Puede ser aconsejable realizar una clasificación de los peligros para ayudar

a tener una idea más visual del riesgo asociado al proceso. Todos los resultados son cualitativos.

- **Ingeniería básica o definición del diseño:**
  En esta etapa, si la información disponible lo permite, se debe realizar un análisis más profundo de aquellos escenarios de accidentes cuyo peligro percibido es alto. También cobran importancia las alternativas planteadas para eliminar o controlar los peligros identificados en las etapas anteriores.
  Se debe disponer de la suficiente información sobre el proceso para recomendar alternativas o modificaciones que permitan mejorar la seguridad. Todos los resultados son cualitativos.

- **Ingeniería detallada:**
  Normalmente se realizan estudios PHA con el objetivo de identificar de forma precisa los peligros y los problemas de operación antes de empezar la construcción de la instalación. También se pueden evaluar, de forma cuantitativa, los peligros específicos que han sido identificados y catalogados como importantes en las etapas anteriores.

  Se debe analizar todos los peligros generales, por ello los resultados están más enfocados a identificar y evaluar escenarios de accidente y generar información para poder realizar análisis cuantitativos de riesgo.

- **Operación rutinaria:**
  En esta fase el objetivo principal es realizar estudios periódicos para identificar y evaluar los peligros nuevos y escenarios de accidentes que surgen debido a la operación continuada del proceso y a las modificaciones del diseño original. Por ello se aconseja la utilización de técnicas optimizadas para procesos en operación.

  Para la evaluación de escenarios de accidente complejos y de los errores humanos se generan resultados cuantitativos para tener una idea sobre la probabilidad de que sucedan y sobre las causas y/o efectos de los mismos.

- **Proceso de modificación:**
  En esta etapa, cuando el proceso está en modificación se realizan evaluaciones de las modificaciones o mejoras del diseño original del proceso, con el objetivo de no introducir nuevos peligros. En función del peligro potencial percibido asociado a la modificación o al tipo de fallo que puede introducir la misma, se utilizarán técnicas que pueden cubrir la identificación de un gran rango de peligros o aquéllas que se centran en escenarios específicos.

- **Investigación de incidentes:**
  En esta fase se recomienda utilizar las técnicas que permiten revisar y/o evaluar de forma detallada aquellas zonas o áreas del proceso que han

sufrido algún tipo de accidente/incidente con el objetivo de identificar el fallo que lo originó y sugerir alternativas que permitan eliminar, reducir la probabilidad de que se vuelva a producir dicho accidente.

- **Construcción y puesta en funcionamiento:**
  El objetivo de realizar un estudio PHA en esta fase del proyecto es verificar que la instalación se ha construido según lo diseñado y cumpliendo las prácticas de la industria y que los peligros para la seguridad no han sido ignorados. Por todo ello, se aconseja utilizar técnicas que puedan identificar una amplia gama de peligros.

  En esta etapa cobra especial interés la información relacionada con los materiales y procedimientos de construcción y los requisitos o estándares de la compañía que operará el proceso.

- **Cierre y/o desmantelamiento:**
  El cierre y/o desmantelamiento de una instalación o parte de la misma puede exponer al personal a diferentes peligros, por ello se recomienda utilizar una técnica que pueda examinar una gran variedad de peligros y que sea apta para procesos que no están en operación.

La utilización combinada de varias técnicas PHA es una metodología habitual. El método más utilizado es identificar los peligros con una técnica PHA cualitativa, para luego evaluar los problemas más importantes con una técnica cuantitativa.

- **HAZOP + FTA:** Se utiliza cuando después de haber examinado una desviación de un elemento con la técnica HAZOP se requiere evaluar el efecto de las desviaciones múltiples o cuantificar la probabilidad de los fallos.
- **FMEA + FTA:** Se utiliza cuando la lógica del fallo es compleja.
- **MIMAH** (Methodology for the Identification of Major Accident Hazards): Combinación de las técnicas FTA y ETA.

También se utilizan combinaciones de técnicas cualitativas, aunque esta práctica no está tan extendida:

- **HAZOP + FMEA:** Se utiliza cuando el HAZOP indica que un componente del equipo necesita ser examinado en profundidad por tener un papel crítico.

- **CHECKLIST + HAZOP:** La técnica Checklist se utiliza para identificar las áreas de peligro más importantes, las cuales se evalúan con más detalle aplicando la técnica HAZOP.

FASE DEL CICLO DE VIDA	TÉCNICA PHA REQUERIDA
Investigación y desarrollo	PrHA, What if, Relative ranking
Diseño conceptual	prHA, What if, Checklist, Relative ranking
Ingeniería básica o definición del diseño	PrHA, What if, Checklist, HAZOP, FMEA
Ingeniería detallada	What if, Checklist, HAZOP, FMEA, FTA, ETA
Construcción	What if, Checklist, Safety review
Operación rutinaria	Checklist, HAZOP, FMEA, Safety review, FTA, ETA HRA, CCA
Proceso de modificación o expansión	What if, Checklist, HAZOP, FMEA, FTA, ETA, Safety review, HRA, CCA
Cierre o desmantelamiento	What if, Checklist, Safety review

Tabla 3. Técnica PHA requerida para cada etapa del proyecto.

2.3. IDENTIFICACIÓN DE PELIGROS

Las condiciones de un proceso pueden crear peligros asociados a los materiales del proceso. Por tanto, no es suficiente considerar sólo las propiedades de los materiales cuando se identifican peligros. También hay que considerar las condiciones normales y anormales del proceso.

Identificar los peligros potenciales, las desviaciones en las variables de control de un proceso y los factores o causas que contribuyen a ello (incluyendo los errores humanos) se puede realizar de la siguiente manera como lo plantean las técnicas PHA:

- **What if:** se basa en plantear situaciones de fallo del proceso a estudiar y preguntar cuál sería el resultado con la condición **si** sucediesen y qué lo causaría.

- **PrHA** (Preliminary Hazard Analysis): radica en hacer una lista de los escenarios de peligro de acuerdo con la experiencia y/o conocimiento del personal y sus causas.

- **Check list:** consiste en un listado de preguntas, en forma de cuestionario, que se pueden basar en la información de los códigos actuales relevantes, estándares que valoran, a través de un examen detallado de la experiencia en la operación y los incidentes ocurridos en procesos similares, el grado de cumplimiento de los procedimientos o normas establecidas.

- **Safety Review:** revisa detalladamente el proceso existente, en la que se identifican los procedimientos de operación que necesitan ser revisados, las modificaciones en el proceso o en el equipo que pueden introducir nuevos peligros y el equipo mantenido de forma inadecuada.

- **FMEA:** divide el equipo industrial de acuerdo con las funciones o localización, considerando todos los posibles modos de fallo de cada división en condiciones de operación.

- **HAZOP:** enlista y asigna palabras guía a los parámetros y variables del equipo a examinar, dando como resultado todas las posibles desviaciones significativas de las condiciones normales de operación para realizar un estudio de los posibles funcionamientos anormales. Por ejemplo, palabras guías: Menos, Mas, No y variables: presión, temperatura; las desviaciones serian: menos presión, más temperatura, entre otras.

A través del estudio de las desviaciones se identifican las **causas** de cada desviación.

- **ETA:** identifica un suceso iniciador de accidentes, las funciones de seguridad diseñadas para reducir este suceso; luego se elabora el árbol de sucesos y determina la secuencia mínima de fallos para que se produzca el accidente.

- **Relative Ranking** (Clasificación relativa de peligros): Inicialmente se selecciona un método de relative ranking que esté publicado, luego se deben seguir las instrucciones de la guía técnica del método seleccionado.

- **FTA – Fault Tree Analysis** (análisis de árbol de fallas): inicialmente se debe considerar el evento principal más peligroso y se identifican las causas. Esta técnica proporciona un modelo gráfico, utiliza símbolos de la lógica Booleana (puertas AND, OR) que muestra las combinaciones de fallos del equipo y errores humanos (causas) que pueden producir el fallo principal del sistema.

- **CCA - Cause and Consequence Analysis** (Análisis de causa y consecuencia): selecciona un suceso o situación de accidente a evaluar, los cuales se puede definir como FTA evento principal o ETA suceso iniciador, el resultado da la relación entre causa y consecuencia.

- **HRA - Human Reliability Analysis** (análisis de fiabilidad humana): inicia realizando un análisis de las tareas funcionales y de los errores humanos en estas tareas, por parte de los operadores, personal de mantenimiento, técnicos y otro personal de la planta.

Identificar y evaluar los errores humanos, que han sido declarados como importantes por otras técnicas PHA (HAZOP, FMEA). Enlista los posibles errores humanos que pueden aparecer durante la operación normal o de emergencia del proceso y factores que contribuyen a dichos errores.

Para las demás técnicas la causa se realiza describiendo que origina la desviación en la caldera.

2.3.1. IDENTIFICACION DE PELIGROS EN CALDERAS

La caldera es un recipiente cerrado en el cual se calienta agua, se genera vapor, se sobrecalienta vapor, o una combinación de las dos operaciones, por medio de la aplicación de calor proveniente de combustibles de un quemador independiente o anexo [9]. Este proceso se produce a través de una transferencia de calor a presión constante, donde el fluido originalmente en estado líquido se calienta y cambia de estado. Es un recipiente de presión construido en gran parte con acero laminado a semejanza de muchos contenedores de gas.

Figura 4. Caldera Industrial

Para mantener las variables en correcto funcionamiento se necesitan dispositivos que regulen automáticamente los niveles de trabajo deseados. Las calderas requieren de un estricto cuidado porque son recipientes presurizados que contienen un fluido a altas temperaturas superiores a los 100 °C, demandando un continuo seguimiento de operación.

Un número significativo de calderas se encuentran ubicadas en los grandes centros de producción industrial y en algunos casos donde reside población altamente vulnerable a accidentes, explosión e incendio, siendo éstos los principales riesgos de este elemento de ingeniería. Sin embargo, estos riesgos se pueden reducir notablemente cuando se adoptan medidas preventivas como un marco general de exigencias para que cada empresa establezca su propio sistema de prevención.

2.3.1.1. FALLAS FUNCIONALES

Debido a que en las calderas se lleva a cabo un proceso, los errores de las funciones que estén a cargo de sus dispositivos y su lógica de operación será categorizada como errores funcionales. Entre ellos se encuentra [10]:

- **CONTROL DE NIVEL DE AGUA DE LA CALDERA**
  Cuando una caldera piro-tubular produce vapor, baja su nivel de agua; si este nivel es inferior al mínimo de diseño, los tubos quedarán expuestos y esto puede producir averías como la acumulación de sarro, que produce una elevación descontrolada de la temperatura o incluso que explote la caldera.

  Dentro de la caldera en condiciones estables el agua está en movimiento considerable y con gran turbulencia. Cuando el agua es calentada se generan burbujas de vapor que ocupan espacio dentro de la caldera ocasionando un aumento del nivel general aunque la cantidad de agua en sí no ha cambiado. Entre más vigorosa se vuelve la ebullición más se aumenta el nivel. Toda la capa de nivel está llena de burbujas.

  Es importante saber que en caso de detectar el nivel de agua por debajo de la mitad del volumen total, no se debe suministrar agua fría a la caldera porque implotaría por un choque térmico brusco.

  Los dispositivos automáticos de control de nivel y las alarmas de bajo y alto nivel son considerados únicamente como ayuda al operador, en la cuales no se debe tener absoluta confianza.

- **CONTROL DEL AGUA DE ALIMENTACIÓN**
  El nivel de la caldera es una de las variables críticas para la operación segura; un bajo nivel expone los tubos a demasiado calentamiento mientras que el alto nivel permite el arrastre de gotas de líquido que corroen y dañan los equipos que usan este vapor.

  Cuando se le suministra agua fría a la caldera, esto hace que se retrase el calentamiento de toda la cantidad de agua contenida en la caldera, reduciendo la eficiencia del vapor producido. Para ello es muy importante tener precalentada el agua de suministro.

- **CONTROL DE LA PRESIÓN DEL HOGAR**
  El aumento de presión puede ocasionar una falla del quemador que genera un re-encendido. Si el control de presión llega a fallar bien sea por el manómetro u otra circunstancia en el lazo de control, se sobre-eleva la presión y si llega a fallar la válvula de seguridad y no se libera el vapor se plantea otra situación donde se puede provocar una explosión de la caldera.

  La carcasa y algunas de las partes interiores de la caldera pueden ser afectadas por la corrosión, que debilitará sus partes metálicas. Por eso, al mantenerse constante la presión en su interior habrá también riesgo de explosión. Lo mismo sucederá si la temperatura de trabajo excede los límites máximos permitidos.

- **CONTROL DE TEMPERATURA VAPOR SOBRECALENTADO Y RECALENTADO**.
  Por un mal control en la temperatura del vapor puede ocurrir:

  - Fallo en el sobre-calentador, recalentador o turbina, debido a las excesivas temperaturas del metal.
  - Dilataciones térmicas que puedan reducir peligrosamente las holguras en la turbina.
  - Erosión derivada de una excesiva humedad en los últimos escalonamientos de la turbina.

- **CONTROL DE COMBUSTIÓN**
  Con insuficiente aire se desperdicia combustible debido a combustión incompleta; además, esta mezcla puede causar explosiones en puntos calientes. Un exceso de aire también desperdicia combustible, calentando aire que luego sale por la chimenea.

  En las calderas alimentadas por combustibles líquidos, la explosión se puede producir por la ignición del combustible vaporizado en el interior del hogar, es decir, en el corazón de la caldera.

  La operación con regímenes de entrada de combustible excesivos con relación al aire de alimentación o con la capacidad del quemador debe controlarse para evitar temperaturas excesivas de los gases de salida del hogar.

- **OPERACIÓN A BAJA PRESIÓN**
  Al operar la caldera a baja presión la superficie es más turbulenta salpicando agua hacia el punto de salida del vapor. Las burbujas de vapor son más grandes a baja presión causando más turbulencia conforme se rompen en la superficie. Trabajar a baja presión es menos estable y hay más probabilidad que gotas de agua contaminen la calidad del vapor cuando el nivel del agua alcance su punto más alto. Por ello es aconsejable usar la caldera con su presión de diseño.

- **AUMENTO DE LA DEMANDA DE VAPOR**
  Las demandas de vapor reales son raramente estables, varían frecuentemente y las calderas deberían responder a estos cambios. Cuando la demanda de vapor aumenta la caldera tardará un poco en aumentar su generación para igualar la nueva demanda. Sin embargo, durante este periodo de transición la demanda de la planta sobrepasa la cantidad de vapor que la caldera puede producir. El resultado es una caída de presión en el sistema de vapor. Una caída de presión tiene mayor efecto dentro de la caldera.

  Al aumentar temporalmente la demanda de vapor dentro de la capacidad máxima de la caldera, la superficie del agua burbujeante empieza a aumentar

con una rapidez sorprendente. Dentro de poco el nivel es tan alto que el agua y la espuma son arrastradas hasta el punto de salida del vapor.

Cuando la demanda de vapor disminuye la presión aumenta y el nivel de la superficie se restablece al reanudarse una operación normal. Esta respuesta repentina se conoce como dilatación, que es el resultado de la combinación de dos factores:

1) Las burbujas de vapor dentro del agua de la caldera se expanden al reducirse la presión ocasionando un aumento del nivel de la superficie.
2) El agua de la superficie se evaporiza causando mayor turbulencia.

Cuando hay una caída de presión el vapor se convierte en vapor flash; esto se produce cuando la caldera sufre un aumento en la demanda de vapor. La demanda deberá ser aumentada gradualmente, porque es precisamente el aumento brusco la causa de la inestabilidad de la caldera aun cuando la demanda esté dentro de la capacidad de la caldera.

- **DEMANDA MUY ALTA DE VAPOR**

  Si la demanda de vapor es aumentada más allá de la capacidad de generación aun por un periodo muy corto, esto puede ocasionar problemas de golpe de ariete y nivel bajo de agua en la caldera. Es común que la caldera se apague al ser sobre-demandada al accionarse la alarma de bajo nivel.

  Si la demanda de vapor es aumentada suavemente hasta un 15% de la capacidad máxima, entonces la caída de presión ocasiona que el nivel de la superficie aumente y las condiciones se vuelvan más turbulentas debido a la formación de vapor flash[2]. El agua es aspirada sobre la toma de vapor pero esta vez al sostener la sobre-demanda, el nivel turbulento de burbujas sigue subiendo y nada de esto es visible en el visor de nivel, ya que está mostrando agua casi libre de burbujas, mientras que el agua en la parte superior de la caldera consiste principalmente de burbujas de vapor. Los niveles comienzan a caer conforme el agua se re-evaporiza continuamente en el intento de la caldera por satisfacer la demanda excesiva. Por protección se debe generar una alarma de bajo nivel para apagar el quemador, y el agua llena de burbujas bajará rápidamente, pero esto conllevaría dejar expuesta la caldera por la insuficiente cantidad de agua en la caldera. Es importante operar la caldera dentro de los parámetros establecidos con sensores precisos y fiables.

2.3.1.2. FALLAS HUMANAS

Se categorizan como fallas humanas aquéllas que son originadas por los operarios y personal a cargo del funcionamiento de la caldera. Entre los errores humanos se encuentra:

[2] Vapor Flash: Es el vapor que se libera del condensado caliente cuando su presión se reduce.

- Diseño o fabricación deficiente.
- Reparación inadecuada.
- Error en la operación y mantención deficiente.

La seguridad y confiabilidad de la operación dependen de la capacidad y atención por parte del operador y el personal de mantenimiento. Los accidentes asociados a una operación deficiente tienen relación con una mala capacitación del personal a cargo de un equipo tan delicado como una caldera; en muchos casos el operario no tiene conocimientos fundamentales de operación, no hay una previa familiarización con el equipo y no hay preparación adecuada basada en entrenamiento y experiencia.

El uso incompleto de los manuales de operación y mantenimiento desarrollados por el fabricante y en especial los procedimientos preparados para cada instalación por parte de los ingenieros es una de las causas principales de estos accidentes [11].

Procedimientos de operación en los que falla el operario:

- Los modos de operación de las calderas industriales son generalmente manual, automático y emergencia; los operarios solo están relacionados con la operación manual, sin comprender los demás funcionamientos, en especial la programación regular para el cambio de modalidad de operación, que también requieren de su asistencia.

- La programación del encendido de las calderas ha causado muchos accidentes debido a que antes de proceder a aplicar calor no se verifica todo el instrumental con el fin de asegurar que han sido calibrados y se encuentra listo para entrar en servicio. Por ejemplo, el hogar, el banco generador de vapor, el economizador, el pre calentador de aire y los conductos deben purgarse convenientemente antes de que cualquier fuente de encendido (encendedor o llama piloto) se introduzca en el hogar, para asegurar que no se ha acumulado combustible en la unidad.

- El encendido del quemador no debe demorar más de cinco segundos; a partir del momento e abre la llave de paso del gas. Si el encendido sobrepasa los cinco segundos debe cortarse inmediatamente la alimentación del combustible al quemador y desactivarse el encendedor, requiriéndose un procedimiento de purga del hogar antes de encender nuevamente.

- Cuando hay cambio en los turnos de trabajo los operarios no comprueban el estado de operación del generador de vapor, y no establecen las dificultades en cada turno de operación y los procedimientos para solucionar dichas dificultades. No hay registro uniforme de los controles e indicadores de funcionamiento, mantenimiento y modificaciones.

Procedimientos de mantenimiento e inspección en los que falla el operario:

- Tratamiento deficiente en el control químico del agua de alimentación en la caldera.

- Los dispositivos de control no son sometidos a pruebas al vacío, para revisar sus condiciones de operación. No hay verificación de todos los enclavamientos y cortes de combustible, no hay simulación de fallas en los ventiladores, en la llama y presiones de combustible.

- Deficiencia en la limpieza de las superficies de calentamiento y tubería de escape.

- Diseño o fabricación deficiente: los accidentes provocados por calderas mal diseñadas o de fabricación deficiente son bastante frecuentes, debido a que la reglamentación vigente en el país no establece exigencias y controles a los fabricantes. En algunas el personal encargado de la caldera no recurre a estándares internacionales o publicaciones de la asociación nacional de protección contra incendios NFPA 85, donde se encuentran los requerimientos de seguridad para el diseño o fabricación de calderas.

Errores de diseño o instalación:

- Inadecuada instalación de los tanques de almacenamiento de combustible, de válvulas de descarga, válvulas de purga, válvulas de alimentación, de indicadores y sensores de nivel, presión y temperatura. Las válvulas de seguridad generalmente son instaladas en la intemperie o no tienen un fácil acceso por el operario.

- En el diseño del tambor de la caldera suele presentarse un limitado volumen de separación y un tambor desnivelado, ocasionando espuma en vez de vapor que interfiere en el control de nivel.

- Deficiencia en el diseño de las líneas de descarga y drenaje.

Reparación inadecuada:

Los accidentes debidos a reparaciones deficientes se deben principalmente a que no son realizadas por personal especializado, provocando roturas en la tubería, generando fugas de agua y de vapor afectando el funcionamiento normal de la caldera.

Un gran porcentaje de los accidentes en calderas han ocurrido por reparar generadores de vapor, tuberías y equipos auxiliares que se encontraban presurizados.

2.4. EVALUACIÓN DE RIESGOS

Esta etapa consiste en clasificar los riesgos de acuerdo a la cuantificación de las consecuencias y frecuencias de eventos peligrosos identificados en el paso anterior basados en normas nacionales y/o internacionales.

Las técnicas PHA proporcionan diferentes maneras de determinar la evaluación de los peligros, como son:

- **What if:** establece que las consecuencias pueden aparecer si se cumplen las condiciones enunciadas en la pregunta condicional.
- **FMEA**: describe los efectos inmediatos en el lugar del fallo y los efectos esperados del fallo sobre el resto del equipo.
- **ETA, HRA, FTA:** técnicas que muestra gráficamente las posibles consecuencias de un accidente provocado por un suceso iniciador (un fallo específico del equipo o error humano). Dichas consecuencias se definen a través del establecimiento de las relaciones entre el suceso iniciador y los sucesos posteriores (secuencia de un accidente) que conducen al accidente, teniendo en cuenta la respuesta de los sistemas de seguridad y de los operadores. Identificando las combinaciones de fallos que pueden provocar un determinado accidente y la secuencia de consecuencias o accidentes que éste puede provocar.

Estas técnicas se pueden clasificar en función del tipo de evaluación de peligros que realizan:

- Técnicas especializadas en evaluar los peligros de forma cualitativa: what-if, checklist, safety review, HAZOP y FMEA.
- Técnicas especializadas en la evaluación cuantitativa de los peligros: FTA, ETA, CCA y HRA.

La descripción y modo de aplicación de las técnicas se encuentran en el anexo B.

2.4.1. EVALUACIÓN DE RIESGOS DE ACUERDO CON EL REGLAMENTO TECNICO COLOMBIANO (RTC)

El RTC propone para el caso específico de riesgos en calderas, un método basado en la medición del grado de peligrosidad que relaciona las consecuencias, probabilidad de ocurrencia y exposición del personal a cada riesgo [12].

Las **Consecuencias** representan el perjuicio o lesión que se produce sobre elementos vulnerables sometidos a los efectos derivados de situaciones de peligro. La determinación de éstas consiste en realizar un análisis de tipo cualitativo o cuantitativo.

La **frecuencia** es la probabilidad de cada acontecimiento de fallo. Es una magnitud que mide el número de repeticiones por unidad de tiempo de cualquier

suceso periódico. En los análisis de probabilidad se suele utilizar como periodo de tiempo un año.

A continuación se presenta el procedimiento de cálculo a emplear para determinar el grado de peligrosidad de las calderas y las tablas de valoración de consecuencias, probabilidad de ocurrencia y exposición [12].

Grado	Puntaje	Parámetros de evaluación
Leve	1	Pequeñas heridas, lesiones no incapacitantes o daños menores.
Medio	4	Lesiones con incapacidad no permanentes o daños superiores al 20% de las calderas y sus instalaciones
Grave	6	Lesiones con incapacidad permanente o daños superiores al 60% de las calderas y sus instalaciones.
Catastrófica	10	Muerte o daños superiores al 90% de la caldera y sus instalaciones

Tabla 4. Tabla de consecuencias de acuerdo con el RTC

Grado	Puntaje	Parámetro de valoración
Muy baja	1	Cuando es casi imposible que ocurra.
Baja	3	Cuando es remota pero posible(poco común)
Media	6	Cuando es muy posible que ocurra.
Alta	10	Cuando es inminente (ocurre con frecuencia)

Tabla 5. Tabla de probabilidad de acuerdo con el RTC

Frecuencia	Puntaje	Parámetro de valoración
Remota	1	La persona está expuesta al factor de riesgo una vez al mes o pocas veces al año.
Ocasional	3	Expuesta algunas veces a la semana.
Frecuente	6	Expuesta repetidamente varias veces a la semana.
Continua	10	Continuamente o muchas veces al día.

Tabla 6. Tabla de exposición de acuerdo con el RTC

Para definir el grado de riesgo se tiene la ecuación 1:

*Grado de peligrosidad = Consecuencias * Exposición * Probabilidad* (1)

El mayor valor posible del rango de grados de peligrosidad se obtendrá como producto de los valores máximos y el menor valor se obtendrá como producto de los valores mínimos. En la figura 5, el RTC brinda la clasificación del Riesgo en alto, medio y bajo.

Figura 5. Evaluación de riesgo según RTC

2.4.2. ALARP PARA LA EVALUACION DE RIESGO

La metodología propuesta por el RTC para que las empresas evalúen el riesgo es un soporte fundamental, pero puede ser profundizado por cada empresa dependiendo de sus **objetivos de seguridad.**

Para la aplicación del concepto ALARP [5], es necesario definir las tres regiones de la Figura 6 en términos de la probabilidad y la consecuencia de un accidente.

Para encontrar el riesgo tolerable objetivo, se debe tener cuidado en asegurar que todas las hipótesis están justificadas y documentadas.

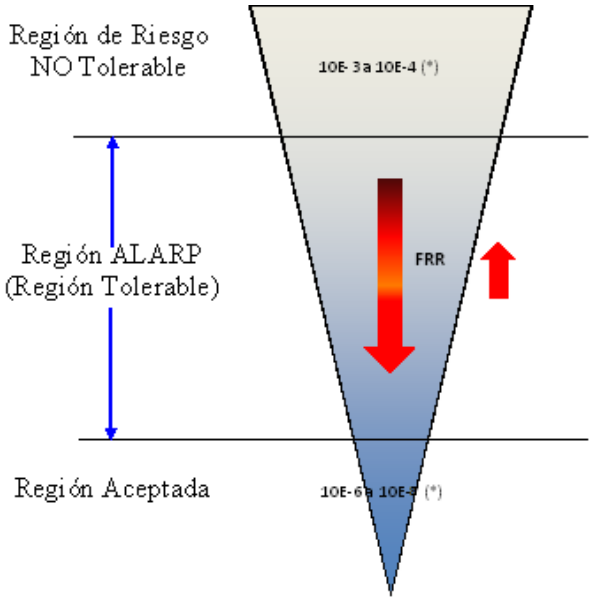

Figura 6. ALARP

La forma triangular indica que a medida que el riesgo aumenta mayor es la inversión necesaria para reducirlo, y para ello es necesario clasificar el riesgo en las siguientes regiones:

- **REGIÓN ACEPTABLE:** el riesgo se encuentra por debajo del aceptable por la empresa. NO se requiere implementación de acciones, es decir no es necesario reducir el riesgo.

  El riesgo individual de muerte por una persona de la población es aceptable si esta entre 10E-06 y 10E-08 anual.

- **REGIÓN TOLERABLE:** el riesgo debe considerarse serio y tomarse las acciones necesarias para bajar el mismo a área ACEPTABLE, siguiendo el criterio ALARP, (tolerable si la reducción es impráctica o si sus costos son desproporcionados con la mejora obtenida)

El riesgo individual de muerte por una persona de la población es tolerable si esta entre 10E-04 y 10E-06 anual.

- **REGION NO TOLERABLE:** el riesgo es altísimo y NO se puede justificar este nivel salvo en circunstancias extraordinarias. Se debe actuar lo más pronto posible, implementando una solución que baje el nivel de riesgo a las áreas A o T."

  El riesgo individual de muerte por una persona es inaceptable si esta entre 10E-03 y 10E-04.

2.5. REDUCCIÓN DEL RIESGO

Es el nivel mínimo de reducción del riesgo que se debe lograr para cumplir con el riesgo tolerable (nivel objetivo de seguridad en los procesos) para una situación específica. La reducción del riesgo consiste en medidas o funciones de ingeniería definidas por un equipo multidisciplinar (ingenieros de procesos, mantenimiento y el operario de la caldera), diseñadas para prevenir los riesgos evaluados, considerando la frecuencia de la exposición al riesgo por personas, la probabilidad y severidad de las consecuencias de la presencia del evento iniciador.

Las **funciones de seguridad** pueden ser implementadas por sistemas basados en equipos eléctricos, electrónicos, electrónicos programables (E/E/PE)o por otras tecnologías relacionadas con la seguridad, como pueden ser equipos hidráulicos, equipos mecánicos, o por dispositivos que reducen el riesgo, como lo pueden ser válvulas de alivio entre otras más, o sencillamente operarios [5].

Para cumplir con el riesgo tolerable garantizado se debe tener en cuenta que las frecuencias de fallo de las funciones de seguridad sean lo suficientemente bajas para prevenir la frecuencia de eventos peligrosos desde el exceso que se requirió para satisfacer el riesgo tolerable, y/o las funciones de seguridad modifiquen las consecuencias de fallo en la medida necesaria para cumplir con el riesgo tolerable.

Para establecerlo es necesario tener en cuenta los siguientes aspectos:

- La percepción y las opiniones de las personas expuestas a los eventos peligrosos.
- Las directrices de las autoridades reguladoras pertinentes.
- Estándares de la industria y directrices.
- La industria, expertos y el asesoramiento científico.
- Requisitos legales y reglamentarios - tanto generales como los que están directamente relacionados con la aplicación específica.

La Figura 7 muestra los conceptos generales de reducción de riesgos [5]:

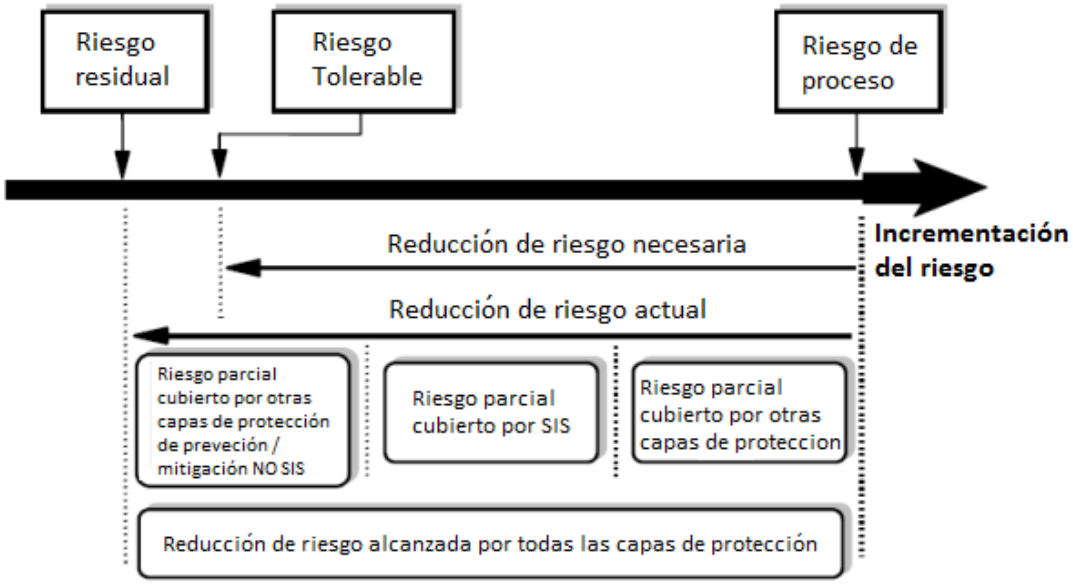

Figura 7. Reducción de Riesgo. Norma ANSI/ISA 84.00.01 Parte 3

- **Riesgo de Proceso:** es el riesgo existente para los eventos peligrosos especificados para el proceso, el sistema de control de procesos básico y las cuestiones relacionadas al factor humano que se consideran en la determinación de este riesgo;

- **Riesgo Tolerable:** es el riesgo que se acepta en un contexto determinado sobre la base de los valores actuales de la sociedad (nivel de objetivo de seguridad de los procesos);

- **El Riesgo Residual:** es el riesgo de eventos peligrosos que ocurren después de la adición de capas de protección.

La reducción del riesgo necesaria para alcanzar el riesgo tolerable especificado, desde el punto de partida del proceso de riesgo, puede ser alcanzada por uno o una combinación de técnicas de reducción de riesgos, como lo son: ALARP.

El concepto ALARP recomienda reducir los riesgos a "la medida de lo razonablemente posible" o hasta un nivel que sea "tan bajo como sea razonablemente práctico". Para que un riesgo sea considerado ALARP debe ser posible demostrar cuantitativamente que el costo de reducir ese riesgo es desproporcionado en comparación con el beneficio que se obtendría. ALARP no es una medida cuantitativa de beneficio contra perjuicio, sino una práctica de juicio para obtener un equilibrio entre riesgo y beneficio a la sociedad.

Si un riesgo está entre los dos extremos (los aceptables e inaceptables) y el principio ALARP se ha aplicado, entonces el riesgo resultante es el riesgo tolerable para la aplicación específica. De acuerdo con este enfoque, se considera

un riesgo caer en una de las tres regiones clasificadas como "inaceptable", "tolerable" o "aceptable, en términos generales" (ver Figura 6).

Para tomar la decisión de reducir el riesgo se debe calcular la relación entre beneficios y costos; si el resultado es superior a uno (1), se debe proponer funciones de seguridad que prevengan los riesgos identificados.

Calcular el costo de daños en la propiedad e interrupción en la producción es en algunos casos más sencillo que determinar el costo de la pérdida de una vida humana.

Para determinar si el riesgo ha sido reducido al nivel tolerable ALARP se debe realizar un estudio de costo- beneficio. Este estudio deberá demostrar mediante una comparativa que el gasto requerido para reducir el riesgo sería proporcional al beneficio obtenido.

La validez de los beneficios de la reducción del riesgo se calcula mediante la ecuación 2 [13]:

$$\frac{Beneficio}{costo} = \frac{F.A.Cp.Ac \times P.Cp.Ac - F.A.Cp.Ad \times P.Cp.Ad.}{C.Cp.Ad + C.Bl.Es} \qquad (2)$$

Dónde:

F.A.Cp.Ac = Frecuencia de accidentes con Capa de protección Actual

F.A.Cp.Ad = Frecuencia accidentes con capas de protección adicional

P.Cp.Ac = Valor total de las pérdidas en caso de suceso sin capa de protección adicional a la instalación.

P.Cp.Ad = Valor total de las pérdidas en caso de suceso con capa de protección adicional a la instalación

C.Cp.Ad = Costo total de la capa de protección adicional

C.Bl.Es = Costo eventual de las intervenciones por bloques espurios de la capa de protección adicional (anual).

Una vez determinado el objetivo de riesgo tolerable, entonces es posible determinarlos niveles de integridad de seguridad a funciones instrumentadas de seguridad.

3. ASIGNACIÓN DE FUNCIONES DE SEGURIDAD A CAPAS DE PROTECCIÓN

El objetivo de esta fase es evaluar qué tipo de capa de protección es adecuada para asignar cada función de seguridad establecida en la reducción del riesgo para lograr los niveles aceptables de riesgo definidos. La reducción del riesgo mediante la selección cuidadosa de los parámetros operacionales básicos del proceso constituye una pieza clave en el diseño de un proceso seguro. Sin embargo, aún después de aplicar esta filosofía de diseño pueden permanecer riesgos potenciales, por lo cual es necesario aplicar medidas de protección adicionales para controlar dichos riesgos. Cada capa de protección (Figura 8) adicional consiste en un conjunto de equipos y/o controles administrativos, los cuales interactúan controlando de esta manera el riesgo.

El proceso básico proporciona el primer nivel de protección. Posteriormente, el sistema de control básico de proceso en conjunción con la supervisión del operador, el sistema de alarmas y las acciones correctivas iniciadas por el operador proporcionan otras capas adicionales de protección. Un operario es una capa de protección no instrumentada, que puede ser parte integral de una función de seguridad.

Es normal en el sector de procesos tener varias capas de seguridad para que el fracaso de una sola capa no provoque o permita una consecuencia nociva y la planta sea inherentemente segura, donde los riesgos residuales puedan ser controlados. Se debe confirmar que las capas de seguridad diseñadas son adecuadas para garantizar la seguridad de la planta; durante este análisis es necesario considerar si las fallas en los sistemas de seguridad introducen nuevos riesgos o demandas.

Las capas de protección seleccionadas deben ser siempre lo más sencillas posible. Sólo en el caso de que no sea suficiente con la aplicación de estas capas, porque el riesgo no puede ser llevado a un nivel aceptable, se debe considerar la necesidad de establecer funciones instrumentadas de seguridad (SIF) para los sistemas instrumentados de seguridad (SIS). Estas funciones con sus correspondientes niveles de rendimiento (SIL) garantizan un proceso seguro.

3.1. ANALISIS DE LAS FUNCIONES DE SEGURIDAD EN LAS CAPAS DE PROTECCIÓN

Para hacer un estudio de la asignación de las funciones de seguridad a las capas de protección es recomendable comprender el funcionamiento de la caldera descrito en el Anexo A de Calderas Piro-tubulares.

Métodos Típicos de reducción de riesgos que se encuentran en las plantas de proceso

Los métodos típicos de reducción de riesgos que se encuentran en las plantas de proceso son mecanismos independientes que reducen el riesgo. La suma de estos proporciona lo que se llama seguridad funcional [1].

Por ello se ha clasificado como capas de prevención a los mecanismos para reducir la probabilidad de que un evento peligroso ocurra y como capas de mitigación a mecanismo para reducir las consecuencias una vez que el evento haya ocurrido.

Layer of Protection Analysis (LOPA) consiste en un análisis objetivo de las distintas capas de protección que se dispone en un proceso, evaluando el riesgo del mismo y comparándolo con el criterio de riesgo tolerable definido por la empresa, para decidir si las capas de protección son adecuadas o por el contrario es necesario mejorar las existentes o introducir nuevas capas adicionales [6]. Esta técnica permite una comparación directa de la contribución de las distintas capas de protección del proceso a la reducción del nivel global del riesgo, LOPA permite además de hacer un análisis de capas, establecer el SIL requerido para cada SIF. Ver anexo C.

En la Figura 8 se muestran las capas de prevención y mitigación que cualquier instalación debería tener para garantizar la seguridad en sus equipos, personal de trabajo, comunidad y medio ambiente [1].

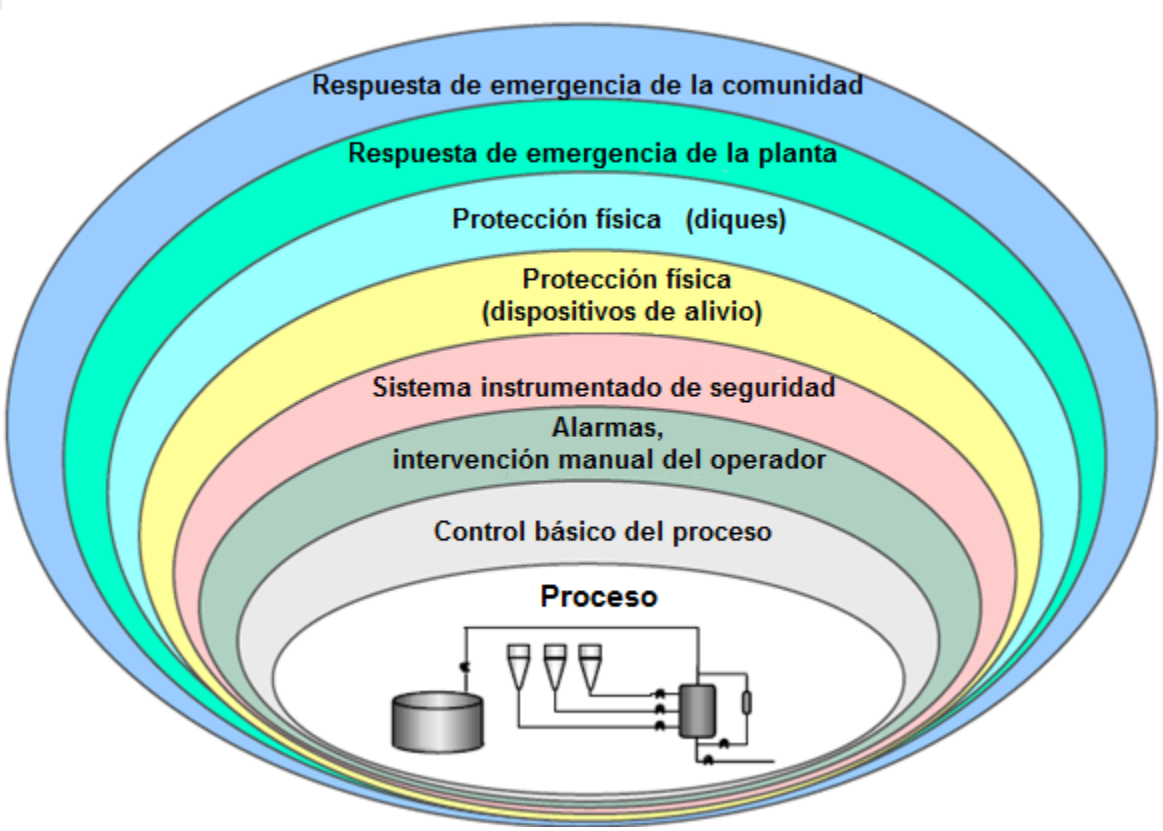

Figura 8. Métodos Típicos de reducción de riesgos que se encuentran en las plantas de proceso

3.1.1. CAPAS DE PREVENCIÓN

Las capas de prevención se implementan para reducir un posible evento peligroso antes de que ocurra.

3.1.1.1. PROCESO

Esta primera capa hace referencia al conjunto de procesos, instalaciones y actividades que pueden generar situaciones de riesgo. Equipos industriales como las calderas cuentan con su propio sistema de seguridad, pero estos dispositivos tienen una probabilidad de falla, siendo una fuente generadora de peligros, como explosiones e implosiones, provocando daños.

3.1.1.2. SISTEMA DE CONTROL BÁSICO DEL PROCESO

Se utilizan para el correcto funcionamiento de la planta dentro de su rango normal de operación; esto incluye la medición, control y/o registro de todas las variables relevantes del proceso. Esta capa está encargada de controlar la producción y la calidad del producto; su principal función es mantener todas las variables dentro de límites seguros, por lo tanto puede ser considerada como una capa adicional de seguridad. Sin embargo, un fallo del sistema de control también puede iniciar un evento peligroso.

La reducción del riesgo de menos de 10 pueden ser realizados por el sistema de control básico BPCS, sin la necesidad de cumplir con IEC 61511-1 ANSI/ISA-84.00.01-2004 Parte 1 (IEC 61511-1 Mod). Cualquier reclamación debe ser justificada por la consideración de la integridad de la BPCS (determinado por el análisis de la fiabilidad o datos de rendimiento) y los procedimientos utilizados para la configuración, modificación y operación y mantenimiento. Para la asignación de la reducción del riesgo a las funciones en el BPCS, es importante asegurarse de que la seguridad de acceso y gestión del cambio se proporcionan. La reducción del riesgo que puede ser reclamado por una función de BPCS también está determinada por el grado de independencia entre las funciones BPCS y la causa de iniciación.

3.1.1.3. SISTEMAS DE ALARMA E INTERVENCIÓN MANUAL DEL OPERADOR

Si el sistema de control de procesos presenta alguna falla, las alarmas se utilizan para la intervención del operador.

Se consideran la capa de seguridad donde las personas se involucran activamente. Los operadores se requieren en las plantas por la simple razón de que no todo puede ser automatizado. Sin embargo, no es posible apoyarse sólo en la acción de los operadores especializados por que se han producido accidentes debidos a

- Los operadores no creían que sucesos peligrosos señalizados por el sistema de alarma fueran realmente ciertos.
- Los operadores, a causa de las muchas señalizaciones de alarma, se equivocaron en las decisiones tomadas posteriormente.

Las alarmas y sistemas de monitoreo deben:

- Detectar problemas tan rápido como sea posible, para asegurar que una acción se puede tomar antes de alcanzar condiciones peligrosas.
- Ser independientes de los dispositivos que van a monitorearse.
- Agregar baja complejidad como sea posible.
- Ser fácil de mantener, comprobar y calibrar.

3.1.1.4. SISTEMAS INSTRUMENTADOS DE SEGURIDAD

Si el sistema de control básico del proceso y los operadores no pueden controlar el riesgo o se equivocan, interviene esta capa de prevención, que siempre debe estar separado de la capa de control, con sensores, controladores y elementos finales. Estos sistemas están diseñados para:

- Permitir que un proceso avance de manera segura cuando condiciones específicas lo permitan.
- Llevar automáticamente un proceso a un estado seguro cuando determinadas condiciones específicas son violadas.

Estos sistemas requieren un mayor grado de seguridad para prevenir cambios accidentales y manipulación, así como un mayor nivel de diagnóstico de fallos.

Los Sistemas Instrumentados de Seguridad (SIS) para alcanzar o mantener el proceso en un estado seguro tienen asociada una o más funciones de seguridad y cada una representa una medida de la reducción del riesgo indicada por su nivel de integridad de seguridad (SIL); las SIF son consideradas lazos de control de seguridad, porque funcionan como bucles de control.

La descripción de las funciones debe ser clara en cuanto a lo que deben hacer para mantener la seguridad. Por ejemplo, "la válvula # XY123 se debe cerrar completamente cuando la presión en el recipiente # ABC456 llega a 100 bar". Toda función de seguridad será llamada función instrumentada de seguridad.

La implementación de una función de seguridad sencilla puede incluir múltiples elementos sensores, módulos acondicionadores de señal, controlador, elementos finales múltiples y servicios utilitarios, como alimentación eléctrica de potencia y/o aire de instrumentos, como lo indica la figura 9.

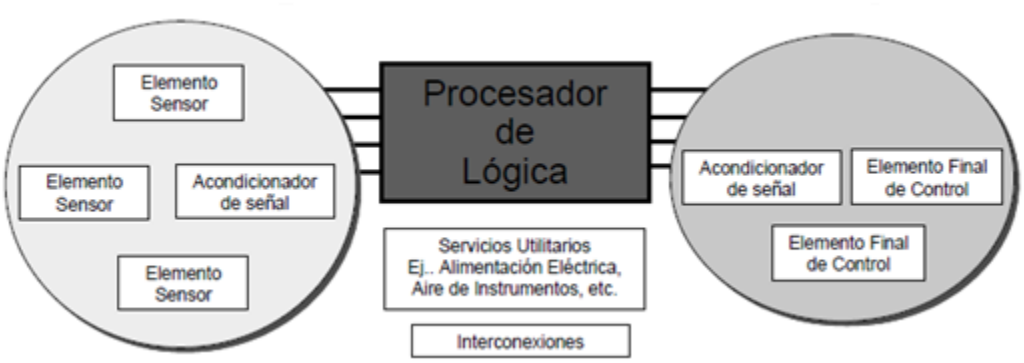

Figura 9. Función Instrumentada de Seguridad

En la Figura 9 se representa esquemáticamente la relación de una función instrumentada de seguridad con otras funciones de seguridad y los sistemas encargados de implementarlas.

3.1.2. CAPAS DE MITIGACIÓN

Las capas de mitigación se implementan para reducir la gravedad o consecuencias de un evento peligroso una vez que han ocurrido. Pueden contener, dispersar o neutralizar la liberación.

3.1.2.1. PROTECCIÓN FÍSICA (DISPOSITIVOS DE ALIVIO Y DIQUES)

Las válvulas de seguridad y discos de ruptura son uno de los medios de protección física que podrían ser utilizados para prevenir una condición de sobrepresión o la liberación de un material tóxico. En esta capa de protección está:

- Los diques (muros de contención) utilizados principalmente en los reactores nucleares.
- Válvulas de alivio de presión y temperatura, actúan para evitar una explosión por exceso de presión o temperatura, liberando un determinado fluido.
- Depuradores y bengalas: diseñados para quemar el exceso de material.
- Sistemas de fuego y gas.

Un sistema de fuego y gas (F&G) se compone de sensores, controladores y elementos finales diseñados para detectar gases combustibles, gases tóxicos o incendios. Estos sistemas no tienen la capacidad de prevenir, éstos solamente actúan cuando hay presencia de gas o fuego.

3.1.2.2. RESPUESTA DE EMERGENCIA DE LA COMUNIDAD

En el caso de una liberación catastrófica, los procedimientos de evacuación pueden ser utilizados para el personal de planta y/o fuera de la comunidad cercana a la zona, si bien estos son los procedimientos y no un sistema físico (aparte de las sirenas), que todavía puede ser considerada como una de las capas de seguridad en general.

3.2. NIVEL INTEGRIDAD DE SEGURIDAD (SIL)

El nivel de integridad de seguridad es el grado de certidumbre de que un sistema de seguridad ejecute de forma satisfactoria las funciones instrumentadas de seguridad requeridas en todas las condiciones en un periodo de tiempo especificado, donde la combinación riesgo, medida de seguridad, medio ambiente son considerados como un todo [1].

El SIL no es directamente una medida de riesgo de proceso, sino una medida del rendimiento del sistema de seguridad necesaria con el fin de controlar los riesgos identificados con anterioridad a un nivel aceptable, es decir, es una forma de indicar la tasa de fallo tolerable de una función de seguridad en particular. El SIL se define numéricamente para poder tener un valor objetivo y así comparar diferentes soluciones y diseños.

El SIL es un valor discreto y la norma ANSI/ISA 84.00.01 especifica cuatro niveles de integridad de seguridad, que indica el grado de disminución de riesgo que está en capacidad de brindar las funciones de seguridad asignadas; el nivel cuarto representa el mayor nivel de integridad y el primero el menos. Las aplicaciones que requieren el uso de una sola función instrumentada de seguridad de nivel cuatro (4) son ocasionales en la industria de procesos. Esta solicitud deberá ser evitada cuando sea razonablemente posible debido a la dificultad de lograr y mantener estos altos niveles de rendimiento a lo largo del ciclo de vida de seguridad. Si los resultados del análisis en un nivel de integridad de seguridad de cuatro (4), se tendrán en cuenta cambios en el diseño del proceso de tal manera que sea más inherentemente seguro.

Cuando una función de seguridad se asigna a una función instrumentada de seguridad, será necesario considerar si la aplicación está en modo demanda o en continuo. La mayoría de las aplicaciones en el sector de proceso operan en modo de demanda, pero las demandas son poco frecuentes. Existen algunas aplicaciones donde las demandas son frecuentes (por ejemplo, más de uno por año) y es más apropiado considerar la operación de la SIF en modo continuo.

FUNCIÓN INSTRUMENTADA DE SEGURIDAD EN MODO DE DEMANDA

Es una acción específica (por ejemplo, el cierre de una válvula) la cual se toma en respuesta a las condiciones de proceso o de otras demandas. En el caso de una falla peligrosa de la función instrumentada de seguridad o del BPCS dado un peligro potencial del proceso, cada SIF recoge y analiza información de los sensores para determinar si se produce una condición peligrosa y consecuentemente, comienza la secuencia de parada para llevar el proceso a un estado seguro. Para la determinación del SIL en este modo de operación se debe recurrir a la tabla 8 [1].

FUNCIÓN INSTRUMENTADA DE SEGURIDAD EN MODO CONTINUO

Cuando en el evento de una falla peligrosa en la función instrumentada de seguridad se puede generar un potencial peligro y éste puede ocurrir sin necesidad de que se presente un fallo a menos que se tomen medidas para

prevenirlo. Se considera en modo de alta demanda o continuo cuando es demandada más de una vez al año y se diseña en función de la probabilidad de falla por hora. Para la determinación del SIL se debe recurrir a la tabla 9 [1].

MODO DE OPERACIÓN EN DEMANDA		
Nivel de integridad de seguridad (SIL)	Objetivo de probabilidad de falla en demanda promedio	Factor de reducción del riesgo
4	$\geq 10^{-5}$ a $< 10^{-4}$	>10000 a ≤100000
3	$\geq 10^{-4}$ a $< 10^{-3}$	>1000 a ≤10000
2	$\geq 10^{-3}$a $< 10^{-2}$	>100 a ≤1000
1	$\geq 10^{-2}$ a $< 10^{-1}$	>10 a ≤100

Tabla 7. Niveles de integridad de seguridad, probabilidad de falla en demanda

MODO DE OPERACIÓN CONTINUA	
Nivel de integridad de seguridad	Objetivo de frecuencia de las fallas peligrosas a ejecutar la función instrumentada de seguridad (por hora)
4	$\geq 10^{-9}$ a $< 10^{-8}$
3	$\geq 10^{-8}$ a $< 10^{-7}$
2	$\geq 10^{-7}$ a $< 10^{-6}$
1	$\geq 10^{-6}$ a $< 10^{-5}$

Tabla 8 Niveles de integridad de seguridad: frecuencia de las fallas peligrosas de la SIF

La probabilidad media de fallo objetivo en demanda o en frecuencia de los fallos peligrosos por hora se aplica a la función instrumentada de seguridad, no a los componentes individuales o subsistemas. Un componente o subsistema (por ejemplo, sensores, controlador, elemento final) no puede tener un SIL asignado fuera de su uso en un determinado SIF.

La asignación de un nivel SIL tiene asociado un valor de PFDavg objetivo, que será determinado por la reducción del riesgo objetivo. La cuantificación del valor de la reducción de riesgo objetivo se puede determinar comparando el riesgo del proceso sin el SIS con el riesgo tolerable como lo indica la ecuación 3 o la ecuación 4, esto se puede llevar acabo de forma cuantitativa o cualitativa aplicando técnicas como LOPA, matriz de capas de seguridad, matriz de riesgo, gráfico de riesgo y gráfico de riesgo calibrado.

$$PFD\ Objetivo = \frac{Frecuencia\ de\ Riesgo\ Aceptable}{Frecuencia\ del\ riesgo\ con\ capas\ de\ proteccion\ actual} \quad (3)$$

La probabilidad de falla en demanda se determina con la ecuación 4:

$$RFF = \frac{1}{PFD\ Objetivo} \qquad (4)$$

Las técnicas empleadas para determinar el SIL objetivo son:

- Matriz de capas de seguridad (técnica cualitativa).
- Matriz de riesgo (técnica cualitativa).
- Gráfico de riesgo (técnica cualitativa).
- Gráfico de riesgo calibrado (técnica cuantitativa).
- LOPA (técnica cuantitativa).

Estas técnicas se basan en un análisis de riesgo previo determinado por las técnicas PHA y normalmente cada empresa tiene determinado el método a utilizar.

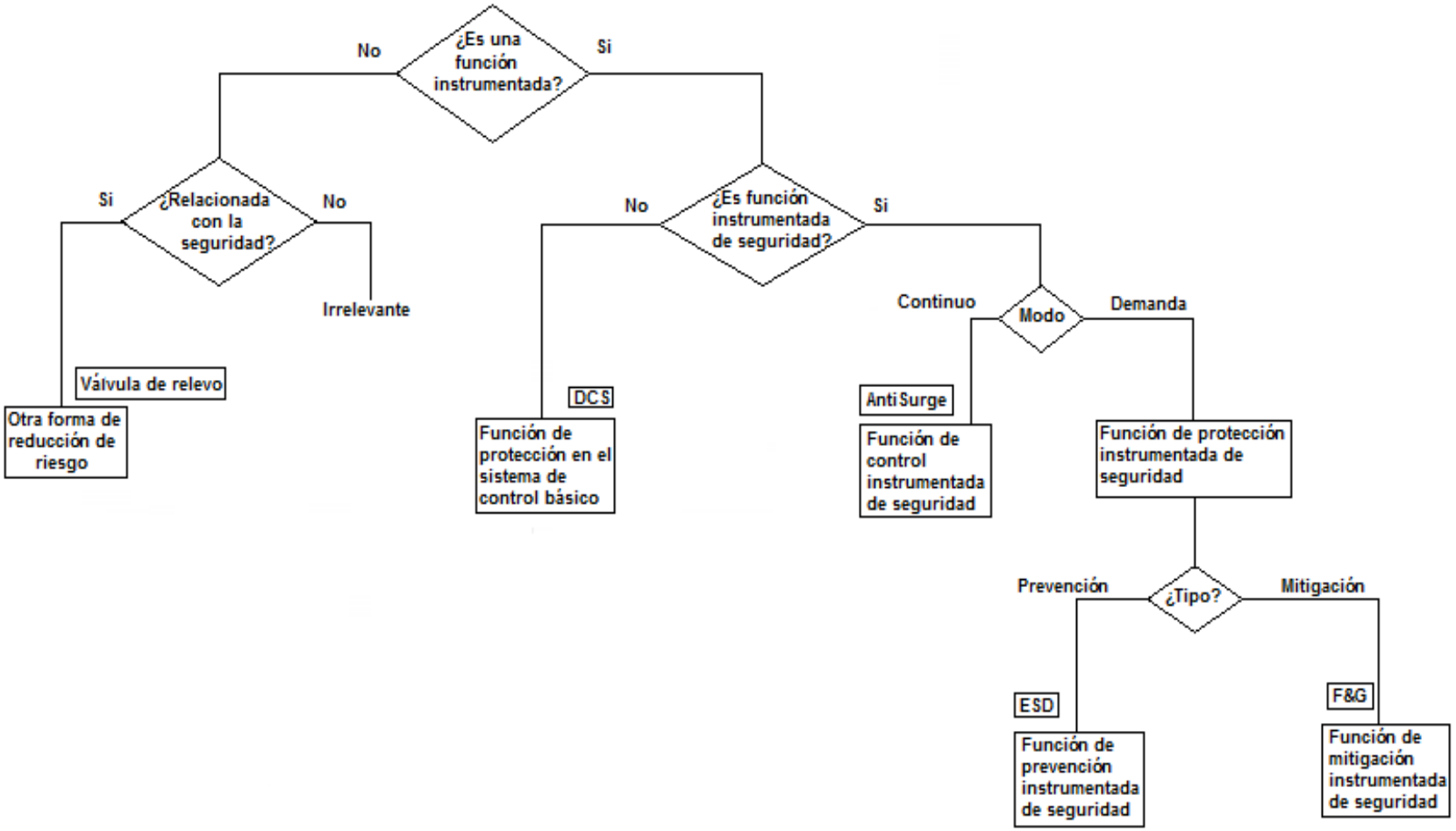

Figura 10. Relación entre las funciones instrumentadas de seguridad y otras funciones.

4. ESPECIFICACIÓN DE LOS REQUERIMIENTOS DE SEGURIDAD (S.R.S.)

Una vez determinado que se requiere un Sistema Instrumentado de Seguridad (SIS) y establecido el Nivel de Integridad de Seguridad (SIL) objetivo para cada función de seguridad, se debe desarrollar las especificaciones de los requerimientos de diseño para el sistema. Los requerimientos del SIS deben ser expresados y estructurados, de tal modo que sean claros, precisos, ejecutables, sostenibles, factibles y escritos de modo que puedan ser comprendidos y aplicados.

El desarrollo y preparación de las especificaciones de los requerimientos de seguridad es un proceso iterativo llevado a cabo por el ingeniero de control e instrumentación en cooperación con el equipo de diseño de plantas y cualquier especialista de seguridad.

4.1. COMPOSICIÓN DE LAS S.R.S

Las especificaciones de seguridad (SRS) enumeran los requisitos para todas las funciones a realizar por el sistema clasificándolas en dos partes principales:

- Las especificaciones de requisitos funcionales.
- Las especificaciones de la integridad de seguridad.

4.1.1. ESPECIFICACIÓN DE REQUISITOS FUNCIONALES.

Los requisitos funcionales describen la lógica del sistema y las características de cada función instrumentada de seguridad (FIS). La especificación funcional debe incluir la definición de los parámetros relevantes como:

a) Rango de operación normal de las variables del proceso y sus límites.

b) El estado seguro del proceso:
   - Esta especificación debe definir el estado de seguridad del proceso para cada función identificada en términos del estado de funcionamiento de cualquier equipo rotativo (bombas, compresores, agitadores). Si el estado seguro consiste en una secuencia de acciones, ésta debe ser descrita e identificada con un código.
   - Los requisitos para ser capaz de llevar manualmente el proceso a un estado de seguridad deben ser definidas. Por ejemplo, si hay un requisito para que el operador sea capaz de apagarlo manualmente un equipo de la sala de control o desde un lugar de campo, entonces esto debe ser especificado. Cualquier requisito de independencia de los interruptores de apagado manual del controlador de la lógica del SIS también tiene que ser definido.

c) Consideraciones para paro manual, acciones a tomar en caso de pérdida de la(s) fuente(s) de energía del SIS, respuesta de acción a cualquier falla detectada y funciones de restablecimiento del SIS después de un paro. La

iniciación manual de funciones protectoras sustituye en muchos casos a la iniciación automática; por esta razón es importante en funciones iniciadas manualmente considerar la confiabilidad humana.

d) Las condiciones ambientales extremas probables a ocurrir durante todo el ciclo de vida de seguridad del SIS. Se deben considerar como mínimo las siguientes variables: temperatura, humedad, contaminantes, interferencia electromagnética/ interferencia de frecuencia, vibración, descarga electrostática, inundación, clasificación eléctrica de áreas.

e) Las entradas y salidas del proceso al SIS y sus acciones.
Describir las acciones de entradas y salidas del SIS y los requisitos para la operación exitosa.

f) Descripción de las interfaces e interacciones con otros sistemas (incluyendo el sistema de control básico de proceso y operadores).

g) Selección de los modos de energizar o des-energizar para disparo. Generalmente las aplicaciones SIS se encuentran normalmente en el modo energizado y son des-energizadas para disparo. Cuando el proceso específico requiera que alguna aplicación SIS sea normalmente des-energizada y energizada para disparo deberá fundamentarse y demostrarse.

   Durante la operación normal, con la planta en condiciones seguras, las entradas de los sensores de planta, el sistema lógico, y salidas a los dispositivos protectores estarán energizados. El sistema interpretará el estado des energizado de una entrada como una demanda y se desenergizarán las salidas apropiadas para iniciar un paro. Este diseño debe asegurar también un paro por pérdida del suministro eléctrico a las entradas del sistema, salidas o lógica del sistema.

h) Considerar la implementación de Bypass, anulación e inhibiciones, incluyendo la forma como se borra. Si existen requisitos específicos para eludir los dispositivos tales como el bloqueo de teclas o contraseñas, éstos también deben ser especificados.

4.1.2. ESPECIFICACIÓN DE INTEGRIDAD DE SEGURIDAD.

Describen el rendimiento o capacidad de cada función instrumentada de seguridad. Estas especificaciones deben ser usadas para establecer una arquitectura aceptable del sistema para lograr el nivel de desempeño, seguridad e integridad requerida para que el SIS ejecute las funciones necesarias. Los requerimientos de integridad de seguridad deben incluir una definición de los siguientes parámetros de integridad:

a) Identificador de la SIF.

b) Una descripción de todas las funciones instrumentadas de seguridad.

c) SIL asociado para cada una de ellas y modo de operación.

d) Las presuntas fuentes de demanda y tasa de demanda supuesta para cada una de las funciones de seguridad.

e) El factor de reducción de riesgo (FRR) para cada función de seguridad.

f) Requerimientos de tiempo de respuesta para llevar el proceso a un estado seguro.

g) Requerimientos de mantenimiento y pruebas para lograr el SIL requerido (intervalo mínimo de prueba).

   La exigencia de un intervalo de prueba deseado debe ser definida para el diseño del SIS. Si las pruebas se van a realizar durante las paradas planificadas (por ejemplo, cada 3 años), el diseño puede requerir más de redundancia que si el intervalo de prueba debe ser anual.

   Actividades importantes:
   - Describir los procedimientos de prueba.
   - Investigar si las medidas adicionales de seguridad como vigilancia o redundancia tienen que ser adaptados durante el intervalo de prueba.
   - Investigar si los aspectos humanos (ignorar el bypass) podría afectar la seguridad durante las pruebas, teniendo en cuenta si las consecuencias podrían ser catastróficas.
   - La actividad de prueba deberá ser documentado.

h) Acciones a tomar en caso de pérdida de energía en el SIS.

4.2. DOCUMENTACIÓN DEL S.R.S.

El SRS puede ser un documento único o una serie de documentos incluyendo los procedimientos, los dibujos o las prácticas corporativas estándar. Estos requisitos pueden ser desarrollados por el equipo de evaluación de peligros y riesgos y/o el equipo del proyecto en sí. La documentación del SRS del SIS, es un factor clave para que los proveedores de la instrumentación SIS propongan las características funcionales que podrían satisfacer la seguridad funcional requerida en la caldera.

Esta documentación puede ser:

- Narrativa.
- Matriz causa efecto.

4.2.1. NARRATIVA

Consiste en documentar la entrada y salida (E/S), la lógica funcional, y el SIL de cada función de seguridad. Esto dependerá de cada sistema. Un ejemplo sencillo podría ser: "Si la temperatura del sensor TT2301 excede 410 grados, entonces las válvulas se cierran XV5301 y XV5302, esta función debe responder dentro de 3 segundos y debe cumplir con SIL 2.

En la tabla 10 están los ítems que se deben tener en cuenta para la documentación del SRS de cada SIF [14].

ITEM	DETALLES DE REQUERIMIENTOS
LAZO:	
ESPECIFICACIÓN DE REQUISITOS FUNCIONALES	
Data sheets del proceso	
Rango de operación normal de las variables del proceso y sus límites de operación.	
Definición de los estados seguros del proceso, para cada uno de los eventos identificados.	
Consideración para paro manual	
Condiciones ambientales extremas	
Entradas del proceso a los SIS y sus puntos de disparo.	
Salidas del proceso del SIS y sus acciones	
Requerimientos de interfaces hombre-maquina	
Selección de des-energizadas para disparar o energizado para disparar.	
Requerimientos para ser re emplazados o bypass incluyendo como ellos deben ser purgados.	
ESPECIFICACIÓN DE INTEGRIDAD DE SEGURIDAD	
Numero ID de la SIF	
Descripción de la SIF	
SIL requerido para la SIF	
Tasa de demanda esperada	
Factor de Reducción de Riesgo RRF	
Tiempo requerido de respuesta para los SIS para llevar el proceso a un estado seguro	
Intervalos de prueba	
Acciones a tomar por la pérdida de energía en los SIS	

Tabla 9. Aspectos relevantes de SRS

4.2.2. MATRIZ CAUSA EFECTO

Es un procedimiento que ha demostrado su efectividad en la descripción funcional de funciones de seguridad y en la definición de condiciones generales y de desconexión. Éste fue especificado por el Instituto Americano del Petróleo (API) en la directiva API RP 14C y en la actualidad se está aplicando a muchos sectores de la industria de procesos [3].

En la Tabla 11 hay un ejemplo de la matriz causa efecto, la causa es la desviación de una variable del proceso se ubica en el eje X, el efecto es la respuesta al proceso en el eje Y y la intersección define la relación entre la causa

y el efecto, es decir el tipo de disparo, N: Disparo no forzado, 2N: Disparo forzado por el operario, si la casilla esta en blanco es porque no existe una relación.

COMPAÑÍA ABC Gráfico de Evaluación de Análisis de Funciones de Seguridad ID Planta Hoja # 1	CAUSA N°	V 101 Abierta	V 201 Abierta	V 301 Cerrado	V 401Abierta	V 501 Abierta	Energizado Maestro
Efecto N°		1	2	3	4	5	6
Temperatura > 120° F	1	N					
Presión > 200 PSI	2			N	N		
Flujo < 56 Gal/m	3		2N				
Flujo < 56 Gal/m	4		2N				
Flujo < 56 Gal/m	5		2N				

Tabla 10. Ejemplo de una Matriz Causa efecto

En la documentación de las causas y los efectos se debe considerar, el identificador del equipo, la descripción y la configuración de los parámetros del proceso.

5. DISEÑO BÁSICO E INGENIERÍA DE UN SIS

Esta etapa consiste en diseñar el sistema instrumentado de seguridad para cumplir los requerimientos de las funciones instrumentadas de seguridad y niveles de integridad asociados.

5.1. INDEPENDENCIA DEL SIS CON OTROS SISTEMAS

La asociación nacional de protección contra fuego NFPA, en los códigos de peligros en calderas industriales y sistemas de combustión, establece la necesidad de independencia de la siguiente manera: “El sistema de control que ejecuta las funciones de seguridad para el manejo de calderas y quemadores no se puede combinar con ninguna otra lógica, se debe proporcionar una separación física y funcional de los sensores, actuadores, controladores, los módulos de entrada y salida del Sistema básico de control del proceso (BPCS) y el SIS”[8]. En otras palabras, se requiere separación física de los componentes porque un fallo de uno no tendrá impacto en el otro. Se debe implementar una lógica diferente, porque si la misma lógica que se realiza en ambos sistemas presenta un error en la especificación funcional, ambos sistemas tendrían el mismo error. Si este requisito no se puede cumplir entonces el sistema de control debe ser diseñado como un sistema relacionado con la seguridad y cumplir con los requisitos establecidos en normas de seguridad funcional.

5.2. FUNCIONES INSTRUMENTADAS DE SEGURIDAD Y DE NO SEGURIDAD

En el SIS se puede implementar funciones de seguridad y de no seguridad, estas funciones pueden compartir los mismos recursos como, CPU, recursos del sistema operativo, memoria y buses [1], [4].

Funciones Instrumentadas que no son de seguridad, como funciones de control o secuencias de arranque o parada, se implementan para asegurar que el apagado sea ordenado o que el arranque sea más rápido pero deben ser independientes de las funciones instrumentadas de seguridad.

Independencia adecuada significa que ni la falla de alguna de las funciones de no seguridad, ni el acceso a la programación del software a estas funciones sea capaz de causar un fallo peligroso a las funciones instrumentadas de seguridad.

5.3. SIS CON DIFERENTES SIL

El estándar ANSI/ISA 84 menciona los requisitos para la selección de los componentes y subsistemas seleccionados para su uso como parte de un sistema instrumentado de seguridad para aplicaciones de SIL 1 a SIL 3 [1], [4]. Los componentes y subsistemas seleccionados para su uso como parte de un sistema instrumentado de seguridad para aplicaciones SIL 4 se hará de conformidad con la norma IEC 61508-2 e IEC 61508-3.

Cuando el SIS es para implementar funciones instrumentadas de seguridad de diferentes niveles de integridad, entonces el hardware puede ser compartido y el software se ajustarán a los niveles de integridad de seguridad más altos al menos

que pueda demostrarse que las funciones de seguridad instrumentadas de menor nivel de integridad de seguridad no puede afectar negativamente a las funciones de seguridad instrumentadas de mayores niveles de integridad de seguridad.

Las funciones instrumentadas de seguridad de diferentes SIL, deben estar claramente separados y etiquetados en la aplicación. Una forma de demostrar la independencia adecuada es cumpliendo con:

a) La identificación de las funciones instrumentadas de seguridad con códigos en la aplicación software.
b) Todas las variables utilizadas en la ejecución de funciones de seguridad instrumentadas podrían estar etiquetados.
c) Todas las aplicaciones de software de seguridad es decir, el código y variables, están protegido contra cualquier cambio.

5.4. DIVERSIDAD

La diversidad se emplea para evitar que ocurran fallas de causa común, ya que el empleo de la misma tecnología en los elementos físicos (hardware) o programas de cómputo (software) puede producir fallas de causa común. En aplicaciones SIS la diversidad se aplica en elementos redundantes, sólo si esta es necesaria para alcanzar los requerimientos de integridad de seguridad.

En el diseño de un SIS se debe considerar la diversidad al momento de seleccionar elementos físicos (hardware), programas de cómputo (software) de aplicación y utilitarios [1].

En el caso de los elementos físicos para implementar diversidad se debe emplear:

a) Tecnología diferente.
b) Dispositivos de fabricantes o vendedores diferentes.

En el caso del hardware incorporado controlador, la diversidad se logra por el uso de tarjetas diferentes del procesador para el controlador y el módulo de supervisión.

En el caso de programas de cómputo (software) la diversidad debe considerar los siguientes puntos:

a) Programación de aplicaciones por diferentes programadores.
b) Empleo de algoritmos diferentes.
c) Empleo de tipos de datos, estructuras de datos y técnicas de almacenamiento de información diferentes.
d) Empleo de subrutinas de manejo de excepciones y/o errores diferentes.
e) El uso de diferentes compiladores, líneas de codificación.

5.5. CERTIFICADO VS USO PREVIO

Una forma para que los usuarios puedan evaluar los sistemas y los proveedores en el mercado de la seguridad es con la certificación de terceros, TÜV de Alemania o FM en los EE.UU, están disponibles para proporcionar una evaluación independiente frente a diferentes estándares, aunque la norma ANSI/ISA 84 no exige el uso de equipos certificados, se considera justificable para los sistemas de lógica compleja y costosa [1].

Los usuarios necesitan que equipos no certificados puedan ser aptos para sus aplicaciones, para ello muchos usuarios tienen listas de instrumentos que han sido aprobados o recomendados para su uso en instalaciones y han sido establecidas por la amplia experiencia que operan con éxito en su BPCS. Esta lista de instrumentos incluye la versión del dispositivo y el apoyo del seguimiento documentado de los rendimientos de campo en el usuario y el fabricante. Además, el fabricante debe tener un proceso de modificación que evalúa el impacto de las fallas reportadas y las modificaciones realizadas.

Existen muy pocos dispositivos de campo que están diseñados según la norma IEC 61508-2 y IEC 61508-3, por lo tanto los usuarios y los diseñadores dependen de los que han sido "probados en uso". Normalmente, los sensores y las válvulas que están en las listas de aprobados o recomendados para el BPCS son considerados como para implementarse en los SIS a través de la evaluación requerida por la IEC 61511-1, ya que disponen de pruebas oportunas para corroborar que los componentes y subsistemas son adecuados para su uso. En el caso de elementos de campo, es posible que la experiencia de funcionamiento prolongado, ya sea en aplicaciones de seguridad o no, pueden ser usados como base para las pruebas.

Si tal lista no existe, entonces los usuarios y los diseñadores necesitan a cabo una evaluación o pruebas en los sensores y válvulas para asegurarse de que el instrumento funcione como se desea. Esto puede requerir discusiones con otros usuarios o diseñadores para ver lo que están utilizando en aplicaciones similares.

El nivel de detalle de las pruebas debe estar de acuerdo con la complejidad del componente o subsistema considerado y con la probabilidad de fallo necesario para alcanzar el nivel de integridad de seguridad requerido para la función instrumentada de seguridad, se debe considerar lo siguiente:

- Gestión y sistemas de gestión de configuración del equipo.
- Adecuada identificación y especificación de los componentes o subsistemas.
- Demostración del funcionamiento de los componentes o subsistemas en los perfiles de funcionamiento similares y ambientes físicos.

En general, los aspectos relevantes del perfil de funcionamiento de los dispositivos de campo son diferentes a las de un controlador.

Para **todos los dispositivos**, los siguientes puntos contribuyen al perfil de funcionamiento:

- EMC;
- Las condiciones ambientales.
- Funcionalidad (por ejemplo, la medición, acción).
- Rango de operación.
- Propiedades del proceso (por ejemplo, las propiedades de las sustancias químicas, temperatura, presión).
- Proceso de conexión.

Para el **controlador**, los siguientes puntos contribuyen al perfil de funcionamiento:

- Versión y la arquitectura de hardware.
- La versión y configuración del software del sistema.
- La aplicación de software.
- Configuración y características de señales de entrada/ salida.
- Tiempo de respuesta.
- Proceso de tasa de demanda.

Las cualidades funcionales que deben ser consideradas para evaluar el cumplimiento de las SRS y así seleccionar la instrumentación idónea del sistema de seguridad por parte de las diversas propuestas ofrecidas por el proveedor son:

5.6. CONFIABILIDAD

La fiabilidad es la probabilidad de que un dispositivo cumpla con una determinada función exitosamente cuando sea solicitada, dentro de los límites y especificaciones del proyecto en un intervalo de tiempo. La fiabilidad está en función del tiempo de funcionamiento y las unidades de medida son en porcentaje por tiempo de funcionamiento.

MTTF es el índice que señala la confiabilidad o el tiempo promedio de falla de un dispositivo y **NO** la vida mínima esperada de éste.

5.7. DISPONIBILIDAD

La fiabilidad indica que el dispositivo o sistema funciona con éxito durante todo el intervalo de tiempo considerado, durante este intervalo no se admite ninguna reparación. Por esta razón este término por si solo es insuficiente para evaluar el éxito medio cuando las reparaciones son posibles. Resulta necesario definir otra medida del éxito para sistemas y dispositivos que se puedan reparar.

MTBF es un término que aplica sólo a sistemas reparables, es un promedio que indica el tiempo promedio entre fallas, esto implica que el dispositivo ha fallado y ha sido reparado. Muchos proveedores de componentes o dispositivos usados en las SIF, facilitan el valor del MTBF en lugar del MTTF.

En los análisis de confiabilidad y disponibilidad, los intervalos de prueba no deben ser menor a tres meses ni mayor a dos años y para el caso del tiempo medio de reparación (MTTR) no debe ser menor a ocho horas.

La disponibilidad en sentido genérico, esta expresada por la relación entre el tiempo en que el sistema ha estado disponible y el tiempo total incluido la reparación, como lo indica la tabla 11:

Tiempo de disponibilidad (horas)	Tiempo de reparación (horas)	Disponibilidad (%)
1000	10	99
10000	10	99.9
100000	10	99.99
1000000	10	99.999

Tabla 11. Disponibilidad

La disponibilidad indica las probabilidades estadísticas de que no haya fallas en un momento dado.

5.8. DIAGNOSTICO

Los diagnósticos son necesarios a fin de detectar los fallos peligrosos que podrían impedir que el sistema responda a la demanda. El diagnóstico asociado a elementos finales de control, especialmente válvulas debe considerar dos condiciones establecidas: operación normal y diagnóstico activo.

El diagnóstico de la válvula durante operación normal debe considerar pruebas en línea, el uso de alarmas en caso de que la válvula cambie de estado sin una señal lógica. Para el diagnóstico activo de la válvula se deben considerar los transmisores de posición o interruptores de límite para retroalimentar al sistema lógico indicando si la válvula operó correcta o incorrectamente, además se debe llevar a cabo la secuencia del paro de emergencia.

El diagnostico involucra los siguientes conceptos:

- **Arquitectura**: Los requisitos de esta parte de la norma están dirigidos a garantizar que las arquitecturas tienen la tolerancia a fallos de hardware necesarios para las fallas aleatorias y algunos errores sistemáticos [15]. Cualquier tipo de falla es tolerado con las arquitecturas redundantes (Ver anexo E para mas detalle).

  En el grado de tolerancia a fallos es necesario que una serie de factores sean considerados:

  En la selección de la arquitectura a utilizar se debe cumplir con requerimientos de integridad del hardware por lo tanto, es importante asegurarse de que es lo suficientemente robusta para los fallos hardware aleatorio y errores sistemáticos.

Para las fallas sistemáticas en modo de falla peligroso, la implementación de canales redundantes no contribuye a la disminución de estas fallas.

Arquitecturas:

- ✓ **1oo1:** Esta arquitectura no es tolerante a fallas ni posee modo de protección de falla. La ventaja de seleccionar esta arquitectura está en que tiene el costo inicial de instalación más bajo de todas las configuraciones.

- ✓ **1oo2:** Los sistemas 1oo2 tienen buena inmunidad en contra de las fallas ocultas, lo que implica una mayor disponibilidad de seguridad que un diseño 1oo1, pero tiene doble probabilidad de bloqueos espurios.

- ✓ **2oo2:** El diseño 2oo2 presenta la mejor inmunidad contra los disparos en falso, es implementado en sistemas de control de producción en el cual el costo de una parada del proceso es alta. En estos sistemas cuando se presenta una falla oculta o no de un elemento puede impedir un disparo valido.

- ✓ **2oo3:** Es una arquitectura robusta en contra de las fallas ocultas y disparos en falso. Un elemento puede fallar, sin iniciar un disparo en falso, y los dos elementos restantes continúan ofreciendo protección contra una condición de disparo valida. Este diseño ofrece la capacidad de colocar un elemento fuera de servicio para prueba o mantenimiento mientras mantiene el resto de la protección activa. El costo inicial es alto, el espacio y las conexiones necesarias para instalar tres elementos son mayores que las demás arquitecturas.

- ✓ **1oo1D:** El diagnostico permite que una falla peligrosa detectada sea convertida en una falla segura.

- ✓ **1oo2D:** En esta configuración si las pruebas de diagnostico en cualquiera de los elementos detectan una falla, entonces la votación de salida es adaptada de forma tal que el estado de salida del sistema sigue lo indicado por el otro sistema. Si las pruebas de diagnostico encuentran fallas en ambos elementos entonces la salida se coloca en el estado de disparo

- ✓ **2oo2D:** Esta arquitectura es igual a la arquitectura 1oo2D, pero con menos líneas de cableado.

La probabilidad de falla segura y peligrosa de las arquitecturas más utilizadas en la industria se encuentra en la figura 11:

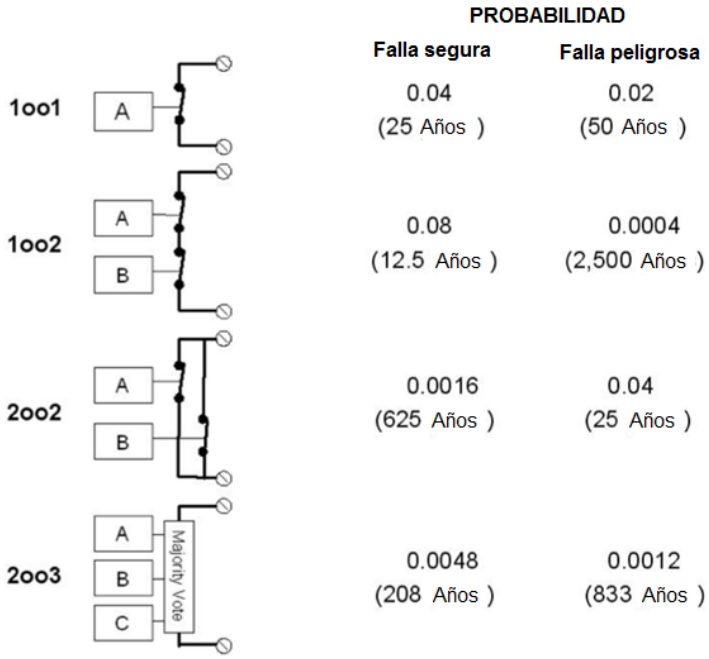

Figura 11. Arquitecturas más usadas en la industria

Además para seleccionar la instrumentación que cumpla con el SIL del SIS debe considerarse la tabla 12:

SIL	Sensores	Controlador	Elemento Final
3	Arquitectura 1oo2 o 2oo3 dependiendo de los requerimientos de activación.	Requerimientos del PLC redundante de seguridad.	Requerimientos de voto 1oo2.
2	La redundancia debe o no ser requerida. Se recomienda arquitectura simple para evitar fallas de causa común. Arquitectura 1oo1.	Requerimientos de PLC de seguridad.	La redundancia puede o no ser requerida.
1	Sensor singular.	Requerimientos de PLC no redundante o lógica relé.	Dispositivo singular.

Tabla 12. Diseño de Instrumentación basado en SIL

- **Fracción de falla segura SFF:** es la fracción de la tasa de falla de hardware de un dispositivo que resulta en una falla segura o falla peligrosa detectada. Ver tabla 13

SIL REQUERIDO				
Arquitectura Tolerancia a fallas	Fracción de falla segura			
	De 0% a 60%	De 60% a 90%	De 90% a 99%	Más de 99%
1oo1	No requerido	SIL 1	SIL 2	SIL 3
1oo1D	No requerido	SIL 1	SIL 2	SIL 3
1oo2	SIL 1	SIL 2	SIL 3	SIL 4
2oo2	No requerido	SIL 1	SIL 2	SIL 3
2oo3	SIL 1	SIL 2	SIL 3	SIL 4
2oo2D	No requerido	SIL1	SIL 2	SIL 3
1oo2D	SIL 1	SIL 2	SIL 3	SIL 4
1oo3	SIL 2	SIL 3	SIL 4	SIL 4

Tabla 13. SIL requerido considerando Arquitectura V/S SFF

- **Tolerancia de falla de hardware HFT:** es el máximo número de fallas en un subsistema, resultante de fallas aleatorias de hardware, que pueden ocurrir sin llevar a la SIF a un estado de falla peligroso.

- **Averías:** los dispositivos industriales presentan dos tipos de averías, seguras y peligrosas. Las averías seguras no conducen a la perdida de la función de seguridad, generan un bloqueo espurio en la instalación que pararía la producción, y las peligrosas, que conducen a la perdida de la función de seguridad. A su vez cada una de estas categorías se divide en averías detectadas y no detectadas.

  $\lambda d = \lambda dd + \lambda du$
  $\lambda s = \lambda sd + \lambda su$
  $\lambda total = \lambda dd + \lambda du + \lambda sd + \lambda su$

  λdd (dangerous detected) = Cuota de averias detectadas peligrosas;
  λdu (dangerous undetected) = Cuota de averias no detectadas peligrosas;
  λsd (safe detected) = Cuota de averias detectadas seguras;
  λsu (safe undetected) = Cuota de averias no detectadas seguras.

  Las cuotas de averías son necesarias para calcular la SFF (Safe Failure Fraction) fracción de fallas seguras, que a su vez son indispensables para verificar el nivel de integridad de seguridad.

- **Cobertura de diagnóstico CD:** El nivel de cobertura de diagnóstico, es decir, el porcentaje de fallas que pueden ser automáticamente detectadas por el sistema, tiene un impacto significativo en el desempeño de seguridad. La cobertura de diagnóstico tiene el propósito de incrementar los intervalos de prueba.

En la tabla 14 se relaciona la redundancia de los sensores, el controlador lógico con la cobertura de diagnóstico, las fallas de causa común y los intervalos de prueba:

Sensores	Controlador lógico	Cobertura de diagnostico	Causa común
Simple	Simple	99.9%	N/A
Dual	Simple	99%	N/A
Triple	Simple	90%	N/A
Simple	Dual	99%	0.1%
Dual	Dual	90%	1%
Triple	Dual	80%	10%
Simple	Triple	99%	0.1%
Dual	Triple	90%	1%
Triple	Triple	80%	10%

Tabla 14. Relacion de redundancia

6. GUIA DE APLICACIÓN DE CRITERIOS

6.1. CONFORMACION DEL EQUIPO DE TRABAJO

El éxito de la aplicación de esta guía, radica en la participación de un equipo multidisciplinario, conformado por ingenieros de proyectos, procesos, producción, seguridad, mantenimiento, instrumentación y personal de seguridad industrial, que aportaran con su conocimiento y experiencia para el desarrollo en cada una de las etapas del diseño de un Sistema Instrumentado de Seguridad. El especialista en riesgos debe orientar sobre la aplicación de las técnicas de análisis de riesgo, determinación del SIL y las demás etapas del ciclo de vida del sistema instrumentado de seguridad.

6.2. ESTUDIO DE CALDERA

Es necesario conocer los componentes y el funcionamiento de la caldera como está especificado en el Anexo A.

6.3. RECOPILACION DE INFORMACION

Para el desarrollo de cada una de las etapas, se requieren la siguiente información:

- Matriz de riesgo.
- Diagrama de flujo del proceso
- Plano de tuberías y de equipos (P&ID).
- Hoja de especificación o placa de identificación de la caldera: consiste en un registro en que se hace constar el nombre del fabricante, tipo de caldera, número de serie y modelo, año de construcción, tipo de combustible empleado, capacidad de generación o flujo de vapor, potencia, superficie de calentamiento, presión de diseño, entre otros.
- Planos de distribución de equipos en la planta, especialmente de los equipos más cercanos a la caldera.
- Libro de operación y mantenimiento de la caldera: en este libro está consignado reparaciones importantes, reportes de calibración, ajustes de dispositivos de control y seguridad, paradas no programadas de la caldera, incidentes, modificaciones de diseño, conversiones de combustible.
- Manual de operación y mantenimiento: libro expedido por el fabricante, en el cual se detallan todos los procedimientos e instrucciones operativas del equipo que debe seguir el operador en condiciones de operación normal o de emergencia, e instrucciones precisas sobre repuestos y procedimientos de reparación.
- Descripción detallada del proceso: incluye la filosofía de operación de los equipos (la relación funcional entre las entradas y salidas del proceso, la lógica de funcionamiento del control operacional y la actuación de los sistemas de bloqueo, el rango de operación normal de las variables del proceso, sus límites de operación), el sistema básico de control y de seguridad (alarmas).

- Registro o listado de las fallas o accidentes en la caldera debido a fallas de mantenimiento como corrosión, taponamiento, recubrimiento, errores humanos, operacionales, entre otros.
- Base de datos de la probabilidad de fiabilidad de equipos, como EXIDA, OREDA, MHIDAS (Mayor Hazard Incident Data System), EIDAS (Explosive Incident Data System), FIRE (Incident data base for chemical ware house fires).
- Información de códigos, estándares y prácticas en calderas industriales.

6.4. ANALISIS DE RIESGO

6.4.1.1. OBJETIVO DE SEGURIDAD

El objetivo de seguridad permite establecer hasta qué punto se puede aceptar que una operación pueda causar eventuales daños y que nivel de gravedad es aceptable para ese daño, considerando las personas, el medio ambiente, el negocio y la frecuencia de ocurrencia objetivo de cada riesgo. Se puede dar el caso que algunas empresas no tengan definida una matriz de riesgo, por lo tanto se debe hacer.

6.4.1.2. SELECCIÓN DE TECNICAS PHA.

Conocer todas las técnicas y su aplicación, como se especifica en el Anexo B, Teniendo en cuenta la etapa del proyecto de acuerdo a la Tabla 3, el conocimiento, información, experiencia, con la autonomía de selección propia del equipo de trabajo.

6.4.1.3. IDENTIFICACIÓN DE PELIGROS

Identificar las causas y consecuencias de los potenciales peligros, basándose en las fallas funcionales y humanas más comunes (Ver Numeral 2.3.1) en el funcionamiento de las calderas industriales piro-tubulares, para ser detalladas en la técnica PHA escogida.

6.4.1.4. EVALUACIÓN DE RIESGOS

Esta etapa evalúa cualitativa o cuantitativamente el riesgo permitiendo la clasificación de acuerdo al RTC o aplicando el concepto ALARP.

Nota: El equipo de trabajo debe tener en cuenta si el RTC, está realmente cubriendo los criterios de aceptación del riesgo aceptados en el proyecto.

6.4.1.5. REDUCCIÓN DEL RIESGO

Debe dar como resultado las posibles funciones de seguridad que permitan prevenir los riesgos identificados, teniendo en cuenta la evaluación de riesgo realizada.

6.5. ASIGNACIÓN DE FUNCIONES DE SEGURIDAD A CAPAS DE PROTECCIÓN

Análisis de las funciones de seguridad en las capas de protección, capas de prevención (proceso, sistema de control básico del proceso, sistemas de alarma e intervención manual del operador, sistemas instrumentados de seguridad), capas de mitigación (protección física (dispositivos de alivio y diques, respuesta de emergencia de la comunidad)

6.5.1. NIVEL INTEGRIDAD DE SEGURIDAD (SIL)

El método para seleccionar el SIL dependerá de muchos factores:

- La complejidad de la solicitud.
- Las directrices de las autoridades reguladoras.
- La naturaleza del riesgo y la reducción del riesgo requerido.
- La experiencia y las habilidades de las personas disponibles para realizar el trabajo.
- La información disponible sobre los parámetros relevantes para el riesgo.
- La severidad de las consecuencias si el sistema de seguridad falla al operar en demanda.
- La probabilidad de que el personal sea expuesto al riesgo.
- Medidas de mitigación para reducir las consecuencias del evento de riesgo.
- La frecuencia con la cual el sistema de seguridad se requiere que actúe.

Una técnica cualitativa se puede utilizar como un primer paso para determinar el SIL requerido de todas las SIF. Si se les asigna un SIL 3 o 4 por este método, entonces se debe considerar con mayor detalle mediante un método cuantitativo.

Para obtener una comprensión más rigurosa del SIL necesario (ver anexo C).

6.6. ESPECIFICACION DE LOS REQUERIMIENTOS DE SEGURIDAD

En esta etapa se debe definir qué y cómo deben actuar las funciones instrumentadas de seguridad, es decir las especificaciones de requisitos funcionales y especificación de integridad de seguridad, respectivamente para lograr el nivel de integridad de seguridad, estas especificaciones permiten documentar todo el proceso de análisis, asignación de funciones de seguridad y requerimientos funcionales de seguridad.

Documentar para narrativa basándose en la tabla 7.

6.7. DISEÑO BÁSICO E INGENIERÍA DE UN SIS

El diseño debe garantizar que se cumplan con las especificaciones de los requerimientos de seguridad (S.R.S), definiendo características funcionales de la instrumentación de cada SIF definidas en el capitulo 5.

7. RESULTADO DE LA GUÍA APLICADA EN EL CASO DE ESTUDIO

7.1. CONFORMACION DEL EQUIPO DE TRABAJO

El equipo multidisciplinario, para el desarrollo del proyecto fue conformado por siete (7) personas:

- Jefe de mantenimiento
- Jefe de producción
- Jefe de seguridad
- Dos (2) operarios de calderas
- Dos (2) Especialistas en riesgos.

7.2. ESTUDIO DE CALDERA

Con el equipo de trabajo se estudiaron los componentes y el funcionamiento de la caldera caso de estudio, apoyados en el Anexo A, con el fin de corroborar que se cuenta con la instrumentación básica para el correcto funcionamiento de la caldera, además para iniciar la documentación del procedimiento de operación y mantenimiento de la caldera, ya que no se cuenta con esto.

7.3. RECOPILACION DE INFORMACION.

- **MATRIZ DE RIESGO:** En la empresa caso de estudio no se cuenta con una matriz de riesgo, solo existe un documento donde clasifica a la caldera como un equipo crítico, porque su inadecuada ubicación dentro de la empresa y cercanía al tanque de almacenamiento de A.C.P.M y disolvente podría generar una explosión e incendio, con consecuencias graves que aún no se han estimado.

  El único accidente grave que se ha presentado en la empresa fue un incendio ocasionado por un disolvente inflamable, utilizado para la fabricación de bandas.

- **INFORMACION TECNICA SOBRE LA CALDERA**
  Esta información permite identificar en la etapa de asignación de funciones de seguridad, si con la instrumentación actual es suficiente para prevenir los peligros identificados.

PLACA DE IDENTIFICACIÓN DE LA CALDERA

Caldera modelo:	E63C40C-2
Serie:	CC0745
Combustible:	ACPM
Presión de diseño:	150 PSI
Presión de operación máxima:	85 PSI
Presión de operación mínima:	75 PSI
Voltaje controles:	110v
Voltajes motores:	220v
Calibración válvula de seguridad:	Abre 150 PSI Cierra 146 PSI
Control de llama marca:	FIREYE
Modelo:	P/N 61-5042
CHASIS:	MC120
MOD PROGRAMADOR:	MP230
AMPLIFICADOR DE LLAMA:	MAUV1
TARJETA DE PURGA:	N.A
DETECTOR DE LLAMA:	UV2
DISPLAY:	N.A

Tabla 15. Placa de identificación de la caldera

HOJA DE ESPECIFICACIÓN DE LA CALDERA

TABLERO DE CONTROL	MARCA	SERIE	MODELO
Base alambrado	FIREYE	NO	P/N 61-5042
Temporizador	FIREYE	010	MC120
Relevo	FIREYE	0544-04	MP230
Amplificador de llama	FIREYE	0541-01	MAUV1
Tarjeta de purga	N.A		
Detector de llama	FIREYE	NO	UV2

Tabla 16. Especificación del tablero de control

CONTROL NIVEL DE AGUA	MARCA	SERIE	MODELO
Columna de agua	Mac DONELL MILLER	03H	157S
Control eléctrico	Warrick	NO	1G1DO

Tabla 17. Especificación del control de nivel de agua

CONTACTORES	MARCA	SERIE	MODELO
Bomba de agua	Telemecanique	NO	LC1D09
Bomba de combustible	Telemecanique	NO	LC1D09
Bomba de piloto	NO		
Compresor de aire	NO		
Precalentador eléctrico	NO		
Soplador	Telemecanique	NO	LC1D09

Tabla 18. Especificación contactores

TERMICOS DISYUNTORES	MARCA	SERIE	MODELO
Bomba de agua	Telemecanique	NO	GV2ME14/6-10AMP
Bomba de combustible	Telemecanique	NO	GV2Me07/1,6-2,5AMP
Bomba piloto	NO		
Compresor de aire	No		
Soplador	Telemecanique	NO	GV2ME14/6-10AMP

Tabla 19. Especificación de térmicos disyuntores

PROTECTOR OPTIMAL BREAKER	MARCA	SERIE	MODELO
Bomba de agua	NO		
Bomba de piloto	NO		
Bomba de combustible	NO		
Compresor	NO		
Precalentador	NO		
Panel de control	Telemecanique		GV2LE10 de 6,3 AMP
Soplador	NO		

Tabla 20. Especificación de protectores

MOTORES ELECTRICOS	MARCA	SERIE	MODELO
Bomba de agua	SIEMENS	884381	3 HP 1708 RPM
Bomba de piloto	NO		
Bomba de combustible	SIEMENS	838226	0,6HP 1680 RPM
Compresor soplador	NO		
Soplador	SIEMENS	888455	3,0 HP 3490 RPM

Tabla 21. Especificación de motores eléctricos

CONTROLES DE OPERACIÓN Y EQUIPO MANEJO DE COMBUSTIBLE	MARCA	SERIE	MODELO
Mudutrol	NO		
Pressuretrol O.P	HONEYWELL	NO	L404A
Pressuretrol AUX.	HONEYWELL	NO	L404A
Columna de agua	Mac. DONELL MILLER	03H	157S
Válvula de flujo	NO		
Válvula de alivio(ACPM)	NO		
Bomba de agua	HIDROMAC	060769	F5T
Bomba de agua	No		
Compresor	No		
Bomba combustible (ACPM)	SUNTEC		J6PB100
Bomba de piloto	NO		
Boquilla principal	Monarch	F-80	5 GPS
Boquilla piloto	Monarch	F-80	4 GPS
Pre calentador eléctrico	NO		
Termostato pre calentador eléctrico	NO		
Termostato interlock	NO		
Solenoide piloto (ACPM)	ASCO	T476041	8262G22V
Solenoide principal (ACPM)	ASCO	T476041	8262G22V
Solenoide purga de aire	NO		
Switch de flujo de aire	NO		
Switch aire de atomización	NO		
Válvula reguladora presión	NO		
Solenoide retorno	NO		
Solenoide atomización vapor	NO		
Válvula de seguridad	Kunkle	6010EDO-AM	¾” 1651 LB/HR
Termómetro chimenea	NO		
Transformador de ignición	ALLISON	NO	10-10000V
Bujía de nivel	Warrick	NO	3/8”
Microswitch limite bajo	NO		
Potenciómetro	NO		
Manómetro ACPM PPAL	Winters	NO	0-200 psi caratula 2 ½”
Manómetro ACPM retorno	NO		
Manómetro vapor	Winters	NO	0-300 psi
Actuador Damper	HONEYWELL	NO	M436

Tabla 22. Especificación de Control de operación y manejo de combustible

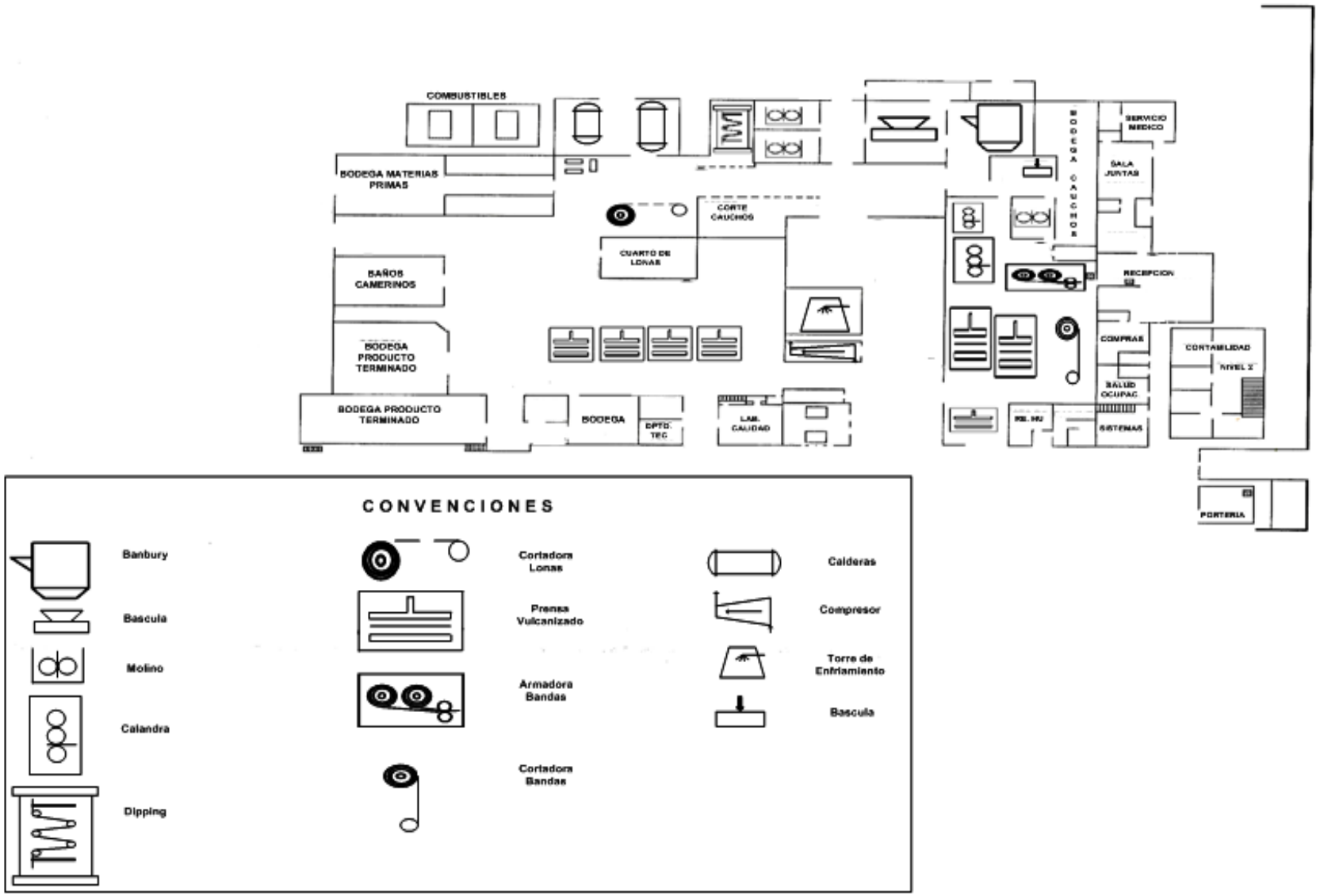

Figura 12. Plano de distribución de la planta

CONTROL DE NIVEL DE AGUA

- Bomba inicia: 5.9 cms en nivel visible.
- Bomba apaga: 6.8 cms en nivel visible.
- Caldera apagada (Mac DONELL): 4.5 cms en nivel visible.

CONTROL DE MOTOR VENTILADOR:

- Carga motor ventilador 9 AMP
- Carga motor ventilador: Operación Mínima: 4.8 AMP
  Operación Máxima: 6.5 AMP

COMBUSTIBLE ACPM:

- Presión de combustible bomba: 110psi.

ANALISIS DE GASES:

- Temperatura de chimenea: 225°C
- Presión de vapor: 150 PSI
- Contenido de CO2: 12.1%
- Contenido de O2: 4.5%
- Eficiencia de combustión: 92.1%

PARTE INTERNA:

- 2 Electrodos de ignición: 9/16 x 16°.
- 1 Boquilla hago de 5 galones x 30°.
- 1 Boquilla hago de 4 galones x 45°.
- 2 Codos de baquelita.
- 1 Fotoceldas fireye UV2.
- 1 Transformador de ignición 110vts-10.000vlts. Marca ALLANSON.
- 1.20 Metros de ignición.
- 2 Terminales de 35 amperios.
- 1 Ventilador rotor: 15 ½ x 7 ½ x 1 ¾.
- Vidrio transparente templado de 13".

PARTE EXTERNA:

- 1 Motor Siemens 3 HPx 3490 serie N° 894114.
- 1 Motor Damper Honeywell M 436.
- 1 Microswitch Telemecanique XCKM115.
- 1 Manómetro Winters 0 a 300psi. Caratula 4".
- 1 Pressuretrol Honeywell L404A1396.
- 1 Columna de agua Mac Donnell Miller 157S.
- 3 grifos de purga en ½".
- 1 Juego de nivel en ½".
- 1 Tubo vidrio Pirex de 5/8 x 10 ¼"
- 1 Válvula de globo de 1"x 150 libras.
- 1 Bujía Warrick
- 1 Válvula globo 1 ¼ x 150 Libras.
- 1 Cheque globo de 1 ¼ x 200 libras.

- 1 Juego mirilla.
- 1 Vidrio pirex mirilla.
- 6 Chapetas SP461.
- 1 Termómetro Winters 100-500°C, Caratula 3”.
- 2 Válvulas solenoide ASCO 8262G22V de ¼”.
- 1 Válvulas bola de ¼”.
- 1 Manómetro Winters 0-200 psi. Caratula 2 ½”
- 1 Motor Siemens 0.6 HP x 1860 RPM, serie 838386
- 1 Acople L-75.
- 1 Bomba Suntec JEPB -100.
- 1 Filtro ACPM Westwood de 3/8”.
- 1 Válvula de seguridad Kunkle de ¾ x 1851 lbs/hora.
- 2 Tornillos escualizables de 5/16.
- 1 Dámper chimenea de 10” x 16”

CAJA PANEL:

- 3 Portaluces VCP Telemecanique.
- 1 Switch de 6 pines – 3 posiciones.
- 1 Base Fireye 61-5042.
- 1 Relé Warrick 1G1DO.
- 1 Switch de 2 pines – 2 posiciones.
- 1 ½ Regleta eléctrica de 12 pares.
- 1 Optimal Telemecanique GV2LE10 – 6,3 amperios.
- 1 Disyuntor Telemecanique GV2ME07 – 1.6 – 2.5 amperios.
- 2 Disyuntores Telemecanique GV2M14 – 6 -10 amperios
- 3 Contactores Telemecanique LC1D09 – 110Vts.

UN TANQUE DE CONDENSADOS DE 60 GALONES DE CAPACIDAD:

- 1 Motor Siemens 3HP x1708 RPM. Serie 884381.
- 1 Acople L-100.
- 1 Bomba Hidromac F5T, serie 060769.
- 1 Filtro en “Y” de 1 ½” x 150 Lbs.
- 1 Válvula cortina de 1 ¼”x 150 Lbs.
- 1 Juego flotador con bola cobre en ½”.
- 1 Tubo pirex vidrio de 5/8 x 13”.
- 1 Termómetro Winters 0 – 200 °C, carátula 3”.
- A la mano: Un juego de llaves para el panel de controles

AGUA DE ALIMENTACIÓN:

En muchos casos el agua de alimentación de las calderas es impropia para la operación, porque tienen minerales, gases en solución y en suspensión. Si el agua de alimentación es apta para el consumo humano, no es un indicador de que sea adecuada para su uso. Es responsabilidad del propietario de la caldera hacer un tratamiento o acondicionamiento para que no se presente corrosión e incrustaciones.

PRESIÓN DE TRABAJO PSI	ALCALINIDAD P.P.M	SÓLIDOS EN SUSPENSIÓN P.P.M
0-50	500	150
50-300	700	300

Tabla 23. Especificación de agua para caldera

Las cantidades de aceite, grasas y otras materias orgánicas dentro de la caldera no deben exceder de 10 p.p.m (partículas por millón)
Puede haber corrosión cuando:

1. El agua no es suficientemente alcalina.
2. Por oxígeno disuelto, bióxido de carbono disuelto u otros gases presentes.

Una medida preventiva contra la corrosión consiste en mantener suficiente alcalinidad en el agua de la caldera para conservar un PH entre un 11 y un 11,5. Los valores de PH se indican con números entre 0 y 14 y denotan grados de acides o alcalinidad. Valores de 7 hacia 14 indican alcalinidad creciente.

En algunas ocasiones el agua de alimentación se puede ver afectada por productos químicos como detergentes, formando espuma en la caldera. La forma de remover estas impurezas es con agentes antiespumantes.

CONTROL DE NIVEL BAJO DE AGUA.
Si el nivel del agua baja, la caldera para automáticamente. La caldera podrá volver a operar solamente después de que el nivel normal de agua se restablezca. En esta caldera se usa un control de nivel de agua baja por medio de un flotador en conjunción con los electrodos de nivel bajo de agua. El flotador en la columna de agua esta acondicionado para operar aproximadamente por encima del nivel de operación del electrodo de la caldera. Si el nivel de agua baja a un nivel anormal, inferior a 4.5 cms sobre los tubos los contactos de la columna operados por el flotador se abrirán. La apertura del circuito por el flotador causara los mismos efectos que el relevo de nivel de agua baja.

Si el nivel de agua baja a un nivel inseguro (aproximadamente 4.5 cms sobre los tubos) los contactos operados por el flotador se abre y la caldera se apaga. Al mismo tiempo los contactos de la alarma se cierran complementando el circuito para la alarma. Cuando el nivel normal de agua es restablecida en la caldera se reactiva.

En el evento de que el control de nivel bajo de agua operado por flotador falle, el circuito de control se abrirá al descender el nivel de agua por debajo del extremo del contactor del electrodo, interrumpiendo la marcha de la caldera por apertura del circuito de control.

SECUENCIA DE OPERACIÓN AUTOMÁTICA ACPM ENCENDIDO ON-OFF CONTROL FIREYE UV2

1. Verificar condiciones normales de trabajo.

2. Colocar el conmutador selector de limite en posición ON (hacia arriba) se energiza el circuito de arranque de la unidad de control de combustión y el transformador de ignición, siempre y cuando el control del límite no está interrumpiendo el circuito. El relevo de carga cambiara de posición y entonces, el motor del soplador y el programador empiezan a operar, efectuando el barrido de gases (pre-purga).

3. Después de un barrido de gases (pre-purga) durante treinta o cuarenta segundos, la operación automática debe empezar.

   La válvula solenoide de aceite primario (piloto) se energiza a los 30 segundos aproximadamente. El relevo de llama abierta cierra sus contactos energizando la válvula de aceite secundario, siempre y cuando la llama primaria haya sido establecida y reconocida por la fotocelda.

   El transformador de ignición se des energiza a los treinta (30) segundos. La unidad continuara operando hasta que se eleve la presión de la caldera a la graduación del control de límite.

4. Se puede detener el encendido manualmente en cualquier momento colocando el conmutador selector de posición OFF.

   Cualquier falla o interrupción en la llama principal se detecta inmediatamente por la fotocelda ocasionando que el relevo de llama salte inmediatamente cerrando la válvula principal de combustible y desenergizando el programador del motor. El motor del soplador continuara operando hasta que el control de combustión se bloquee en el punto de seguridad. En algunos casos se requerirá de rearme manual de control de combustión oprimiendo el botón “reset” respectivo.

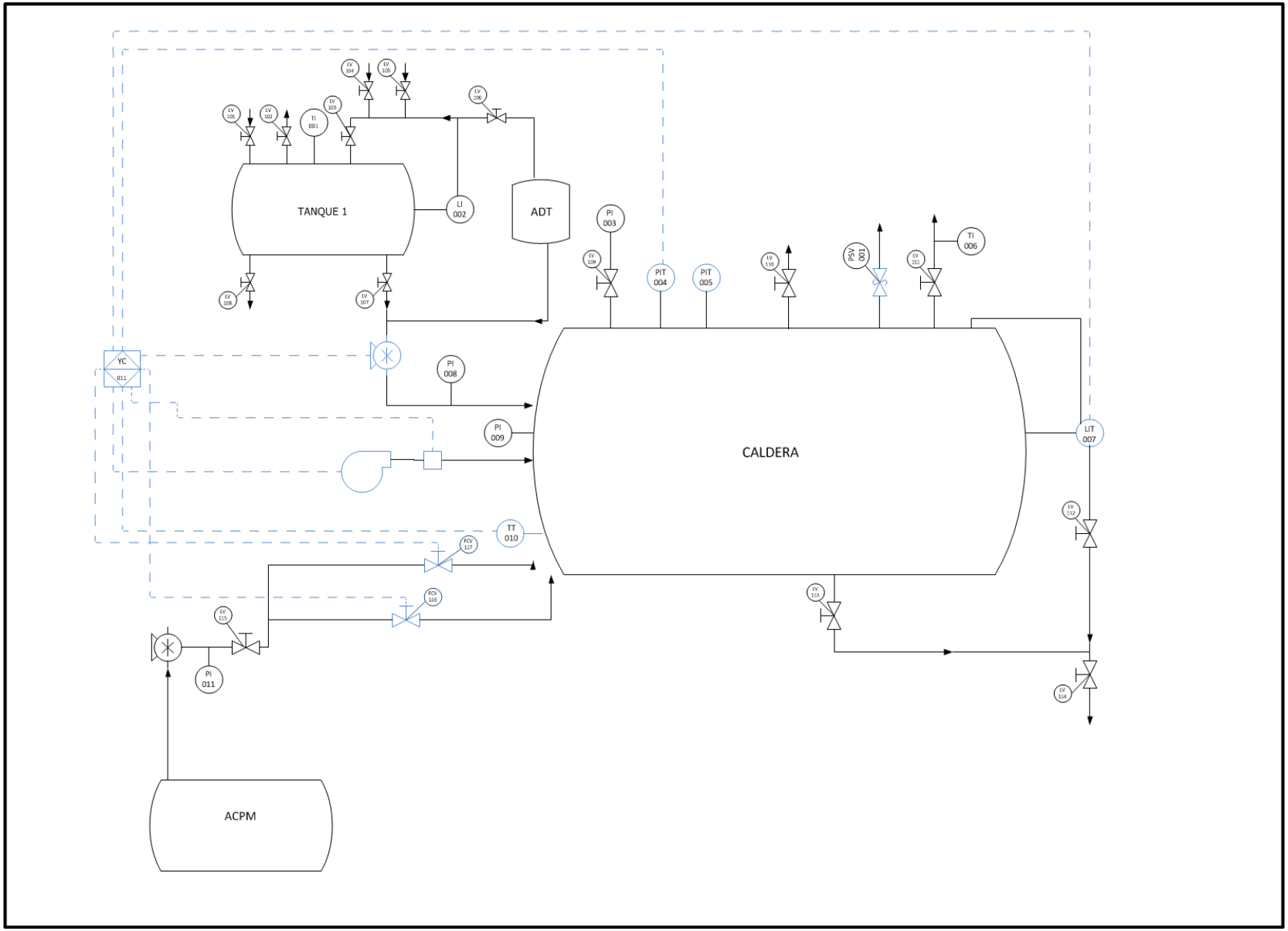

Figura 13. P&ID de la caldera

MANTENIMIENTO SEMANAL

- Hacer mantenimiento al quemador limpiando la fotocelda teniendo cuidado de no rayarla.
- Limpiar las boquillas y si es necesario remplazarlas.
- Limpiar y verificar la separación de los electrodos de 1/8” y la separación de la boquilla de 3/4".
- Purgar el control de nivel McDonnell con las 3 válvulas de purga.
- Revisar estado de las correas y verificar su tensión.
- Limpiar el filtro de combustible.

MANTENIMIENTO BIMESTRAL

- Descarbonar y limpiar ductos de combustión
- Revisar cámara de combustión y refractario
- Revisar y limpiar tubería de entrada de agua a la caldera
- Desarmar, limpiar y revisar el control de nivel McDonnell, revisar los bulbos de mercurio
- Revisar asientos de la válvula, rectificando los vástagos.
- Limpiar la malla de entrada de aire y las aletas del ventilador.
- Revisar los empaques de las bombas de alimentación.
- Revisar alineación y anclaje de bombas y motores.
- Revisar y limpiar controles eléctricos, tablero y contactos arrancadores.
- Limpiar y verificar el estabilizador eléctrico.
- Verificar empaques de alimentación de la caldera.
- Limpiar filtro de agua de alimentación
- Disparar manualmente válvula de seguridad.

MANTENIMIENTO SEMESTRAL

- Deshollinar la chimenea
- Lavar la caldera
- Revisar y vaciar tanque de condensado, quitar la válvula flotadora y lavarlo bien.
- Limpiar el lado de fuego de los tubos de la caldera
- Revisar el lado de agua de la caldera
- Limpiar y revisar el sensor de nivel interno de agua
- Limpiar y revisar el switch de presión del aire
- Después de lavar la caldera, examinar con cuidado las superficies de evaporización para ver si hay indicios de corrosión, picaduras, etc.
- Llenar agua hasta el nivel, revisar, sellar fugas encender caldera y verificar funcionamiento.

CONTROL DE AGUAS

- PH de purga de fondo
- TDS purga de fondo
- PH condensados
- PH agua de alimentación de caldera
- PH torre enfriamiento
- TDS Torre enfriamiento
- PH acueducto
- TDS acueducto

7.4. ANALISIS DE RIESGO

7.4.1.1. OBJETIVO DE SEGURIDAD

CLASES DE RIESGOS							
CONSECUENCIA				PROBABILIDAD			
	Personas	Medio ambiente	Negocio	Frecuente	Poco Frecuente	Remoto	Improbable
				Más de una Vez por año 10E-02	Entre 1 y 10 Años 10E-03	Entre 10 y 100 Años 10E-04	Entre 100 y 1000 años 10E-05
Catastrófica	Accidentes fatales (más de una persona)	Grandes descargas Toxicas más alto Que el volumen permitido. Nube de vapor, fireball, pool fire, jet fire, flash fire	Perjuicios superiores A $200 millones	NT	NT	NT	T
Critico	Lesiones graves (Amputación, quemaduras De 2 y 3 grado Incapacidad de mas De Un mes)	Descargas toxicas Igual que el volumen Permitido	Perjuicios entre $50 Y $200 millones	NT	NT	T	A
Marginal	Lesiones leves (Cortaduras, raspones Quemaduras de 1 grado, Incapacidad en días)	Descargas toxicas Menores al volumen Permitido	Perjuicios entre $10 Y $50 millones	NT	T	T	A
Insignificante	Personal sin lesiones	Sin descargas toxicas	Perjuicios menores a $10 millones	T	T	A	A

Tabla 24. Matriz de Riesgos caso de estudio

7.4.1.2. SELECCIÓN DE TECNICAS PHA.

Los especialistas en riesgo realizaron una explicación sobre todas las técnicas PHA, su aplicación, ventajas y desventajas, con el equipo de trabajo se seleccionó la técnica **HAZOP** (Hazard Operability Analysis - Análisis de peligros y operatividad), porque es la herramienta más completa, de fácil manejo y se cuenta con la información necesaria para desarrollar el estudio, además se encuentra en **operación rutinaria**, de acuerdo con lo mencionado en la Tabla 3.

7.4.1.3. IDENTIFICACIÓN DE PELIGROS

En la tabla 25, se encuentra el desarrollo de la técnica HAZOP en la caldera caso de estudio, identificando los potenciales riesgos causados por fallas funcionales y humanas.

ANÁLISIS DE OPERABILIDAD EN PLANTA 1							
LÍNEA O SISTEMA: Caldera 1							
Ref	**Palabra guía**	**Variable**	**Causas**	**Consecuencias**	**Gravedad de Consecuencias**	**Salvaguardas Existentes**	**Recomendación de nuevas Salvaguardas**
1	Mas	Nivel de la caldera	Falla en bomba de alimentación a la caldera por mala lectura del sensor.	Pérdida económica anual, por mala calidad de vapor afectando el funcionamiento de algunas maquinas	I	Apertura manual de válvula de purga.	Gestión de alarmas para control de nivel
			Falla en el control de nivel.				
			Mala limpieza del sensor de nivel.	Daños leves en maquinaria e instrumentación	I		
			Falla por operario que deja activa la bomba de alimentación				
2	Menos	Nivel de la caldera	Falla en el sensor de nivel que registra un falso nivel en la caldera por burbujas dentro de la caldera.	Explosión	Ca	Control de nivel de la caldera. Alarma por bajo nivel.	Sistema adicional de seguridad (SIS)
				Incendio.	Ca		
				Implosión	Cr		
			Falla del operario por dejar válvula de purga abierta.	Daño en el hogar	M		
				Perdidas económicas por año, por el apagado automático de la caldera.	Cr		
3	No	Nivel de la caldera	Insuficiente agua en el tanque de alimentación.	Explosión	Ca	Control de nivel de la caldera.	Gerenciamiento de alarmas para control de nivel. Sistema adicional de seguridad (SIS)
				Incendio	Ca		
				Implosión	Cr		
			Falla del operario por dejar válvula de purga abierta.	Daño en el hogar	M		
				Pérdida económica anual, por el apagado automático de la caldera.	I		
4	Inverso	Nivel de la caldera	Menor presión de bomba de alimentación	Daños leves en maquinaria e instrumentación	I	No hay	Gerenciamiento de alarmas para control de nivel.
				Explosión	Ca		
				Incendio	Ca		
				Daño en el hogar	M		

5	Mas	Presión de la caldera	Falla del control de presión.	Explosión	Ca	Control de presión. Alarma por alta presión. Válvula de alivio	Sistema adicional de seguridad (SIS)
			Mala lectura por parte del operario del manómetro				
			Mala calibración de manómetro.				
			Falla en la válvula de alivio	Incendio	Ca		
			Falla por operario al dejar cerrada la válvula de salida de vapor	Daño en el quemador	M		
6	Menos	Presión de la caldera	No suministro de agua en caldera.	Pérdida económica anual, por mala calidad del vapor afectando el funcionamiento de algunas maquinas	I	Control de presión.	Gerenciamiento de alarmas para control de presión.
			No hay combustión adecuada				
			Malas condiciones del agua				
7	Alto	Flujo de Vapor de la caldera	Sobredemanda de vapor	Daños en el hogar	M	Válvula de salida del vapor	Control de flujo del vapor
8	Bajo	Flujo de Vapor de la caldera	Poca demanda de vapor.	Daños en el hogar	M		
			Agua no precalentada				
			Fugas en la caldera.				
9	Alta	Temperatura de vapor	Mala combustión.	Daños en el quemador	M	Medidor de temperatura	Control de temperatura
				Dilataciones térmicas	M		
			Malas condiciones del agua	Erosión	M		
10	Baja	Temperatura de vapor	Mala combustión.	Pérdida económica anual por mala calidad del vapor afectando el funcionamiento en las maquinas.	I		
			Malas condiciones del agua				

11	Exceso	Combustión (Llama)	Mala calibración en boquillas de suministro de ACPM.	Excesivas temperaturas de gases.	M	Control de combustión	Sistema de Gestión de quemado
			Falla en el manómetro.				
			Mala calibración en presión de atomización.	Pérdida económica anual por desperdicio de combustible.	I		
			Falla de la fotocelda	Incendios.	Ca		
12	Poca	Combustión (Llama)	Mala calibración en boquillas de suministro de A.C.P.M.	Pérdida económica anual por desperdicio de combustible.	I		
			Taponamiento en boquillas por suciedad del A.C.P.M.	Implosión	Cr		
			Fallo en la fotocelda.				
			Falla en el manómetro	Explosión.	Ca		
13	No	Combustión (Llama)	Falsa llama.	Explosión.	Ca		
			Falla en el control de quemado.				
			Suciedad en la fotocelda				
			Cortocircuito.	Implosión	Cr		
			Taponamiento de boquillas por suciedad en el ACPM	Incendio.	Ca		

Tabla 25. HAZOP caso de estudio

7.4.1.4. EVALUACIÓN DE RIESGOS

De acuerdo con el equipo de trabajo se tomó en cuenta el Reglamento Técnico Colombiano (RTC), teniendo en cuenta la Tabla 4 de consecuencias, la tabla 5 de probabilidades, la tabla 6 de exposición del personal y la clasificación del Riesgo en alto, medio y bajo de la figura 5.

Consecuencias	Ponderación			Riesgo
	Consecuencia (C)	Probabilidad (P)	Exposición (E)	R = C x P x E
Explosión	10	8	10	800
Implosión	9	4	9	324
Incendio	10	7	10	700
Dilataciones térmicas	9	5	8	360
Erosión	8	4	10	320
Daño en los tubos de humo	7	5	10	350
Daño en el quemador	9	4	9	324
Daño en el hogar	9	4	10	360
Daños leves en maquinaria e instrumentación	8	5	8	320
Daño de la bomba de alimentación.	8	7	10	560
Excesivas temperaturas de gases.	5	6	8	240
Pérdida económica anual, por mala calidad de vapor afectando el funcionamiento de algunas maquinas	1	8	1	8
Pérdida económica anual, por desperdicio de combustible.	1	9	1	9
Pérdida económica anual, por el apagado automático de la caldera	1	7	1	7

Tabla 26. Evaluación de riesgo con el RTC caso de estudio

De acuerdo a la tabla anterior, se observa que los riesgos más altos son la explosión e incendio de la caldera. Algunos de los riesgos clasificados en medios y bajos como lo fueron la implosión, daños internos en la caldera y pérdidas económicas; para la empresa caso de estudio no fue satisfactoria esta clasificación porque estos deberían pertenecer a una categoría de riesgos más alta por lo tanto se prosigue a hacer el método ALARP.

7.4.2. ALARP

En la tabla 27 se encuentra la clasificación definitiva de riesgos por parte de la empresa caso de estudio, con base a la información de costo de riesgos de cada evento y la frecuencia registrada en los libros de mantenimiento y base de datos de frecuencia de accidentes en otras empresas. Sobre esta tabla se trabajara para la posterior etapa.

Consecuencias	Frecuencia	Consecuencia	Evaluación
Explosión	Remoto	Catastrófica	NT
Implosión	Remoto	Critica	NT
Incendio	Poco frecuente	Catastrofico	NT
Dilataciones térmicas	Poco frecuente	Marginal	T
Erosión	Remoto	Marginal	T
Daño en el quemador	Poco frecuente	Marginal	T
Daño en el hogar	Poco frecuente	Marginal	T
Daños leves en maquinaria e instrumentación	Poco frecuente	Insignificante	T
Excesivas temperaturas de gases.	Remoto	Insignificante	A
Pérdida económica anual, por mala Calidad de vapor afectando el funcionamiento de algunas maquinas	Frecuente	Insignificante	T
Pérdida económica anual, por Desperdicio de combustible.	Frecuente	Insignificante	T
Pérdida económica anual, por el apagado automático de la caldera	Frecuente	Insignificante	T

Tabla 27. Evaluación de riesgos mediante ALARP caso de estudio

7.4.2.1. REDUCCIÓN DEL RIESGO

Teniendo en cuenta las consecuencias, salvaguardas existentes, y recomendaciones de nuevas salvaguardas de la Tabla 25, se procede a calcular la relación entre beneficios y costos a las consecuencias que son tolerables solamente, ya que de acuerdo al concepto ALARP, las consecuencias que se encuentran en la región de No tolerable requieren acciones inmediatas y la relación costo-beneficio es mayor que 1, y la consecuencia aceptable no representa riesgo para la empresa, por lo tanto se omite.

La validez de los beneficios de la reducción del riesgo se observa en la tabla 28, donde se calcula mediante la ecuación 2, teniendo en cuenta las frecuencias establecidas por la empresa en la tabla 24.

Ref	Consecuencias	Salvaguardas Existentes	Recomendación de nuevas salvaguardas	F.A.Cp.Ac	F.A.Cp.Ad	P.Cp.Ac	P.Cp.Ad	C.Cp.Ad	C.Bl.Es	Resultado
1	Pérdida económica anual, por mala Calidad de vapor afectando el funcionamiento de algunas maquinas	Apertura manual de válvula de purga.	Gestión de alarmas para control de nivel*	2 veces al año	1 cada 6 años.	500.000	80.000	800.000	0	1.23
	Daños leves en maquinaria e instrumentación			1 vez al año	1 vez cada 10 años	1 millón	100.000			1.237
2	Daño en el hogar	Alarma por bajo nivel.	Sistema adicional de seguridad (SIS)**	1 cada 10 años	1 cada 100 años	12 millones	1millón	3 millones	500.000	0.34
3	Perdidas económicas por hora, por el apagado automático de la caldera	Control de nivel de la caldera.	Gestión de alarma para control de nivel.*	2 veces por año	1 cada10 años	400.000	40.000	800.000	0	0.995
4	Daños leves en maquinaria e instrumentación.	No hay	Gerenciamiento de alarmas para control de nivel.*	1 vez cada 2 años	1 vez cada 10 años	1 millón	100.000	800.000	0	0.61
	Daño en el hogar.			1 vez cada 10 años	1 vez cada 100 años	12 millones	1 millón			1.48
5	Daño en el quemador	Control de presión. Alarma por alta presión. Válvula de alivio	Sistema adicional de seguridad (SIS)**	1 cada 10 años	1 cada 100 años	5 millones	500.000	3 millones	500.000	0.14
6	Perdidas económicas por hora, por mala	Control de presión	Gestión de alarmas para control de presión	1 cada 10 años	1 cada 100 años	500.000	50.000	800.000	0	0.06
	Calidad de vapor afectando el funcionamiento de algunas máquinas.									
7	Daños en el hogar	Válvula manual de salida del vapor	Control de flujo del vapor***	1 cada 10 años	1 cada 100 años	12 millones	1 millón	300.000	0	3.96
8	Daño en el hogar	Válvula de salida del vapor	Control de flujo del vapor***	1 cada 10 años	1 cada 100 años	12 millones	1 millón	300.000	0	3.96

9	Daños en el calentador.	Medidor de temperatura	Control de temperatura***	1 cada 5 años	1 cada 10 años	5 millones	2.5 millones	400.000	0	1.87
	Dilataciones térmicas.			1 cada 5 años	1 cada 10 años	2 millones	1 millón			0.75
	Erosión			1 cada 10 años	1 cada 100 años	10 millones	100.000			2.49
10	Perdidas económicas por hora por mala calidad del vapor afectando el funcionamiento en algunas maquinas			3 veces por año	1 cada 10 años	500.000	150.000			3.71
11	Pérdida económica anual por desperdicio de combustible	Control de combustión	Sistema de gestión de quemado. **	2 veces cada año	1 vez cada 10 años	100.000	10.000	3 millones	500.000	0.056
12	Pérdida económica anuales por desperdicio de combustible	Control de combustión	Sistema de gestión de quemado. **	2 veces al año	1 vez cada 10 años	100.000	10.000	3 millones	500.000	0.056

Tabla 28. ALARP Caso de estudio

Notas:

*El sistema de alarmas para un lazo de control, tiene un costo total de 5 millones que se amortiza en 10 años, tiempo estimado del ciclo de vida del sistema de alarmas. En mantenimiento y reparaciones se estima anualmente 300.000, no se consideran costos por bloqueos espurios del sistema de alarmas.

** Un lazo de seguridad de un sistema instrumentado de seguridad, tiene un costo total de 30 millones que se amortiza a 10 años, la vida útil estimada para un SIS es de 20 años. Pero en mantenimiento, pruebas reparaciones y bloqueos espurios se estima anualmente un costo de 500.000.

*** Un lazo de control de flujo de vapor y de temperatura tiene un costo de 3 millones que se amortiza en 10 años, la vida útil estimada es de 10 años.

7.5. ASIGNACIÓN DE FUNCIONES DE SEGURIDAD A CAPAS DE PROTECCIÓN

7.5.1. ANALISIS DE LAS FUNCIONES DE SEGURIDAD EN LAS CAPAS DE PROTECCIÓN

De acuerdo a los conceptos de Capas de protección se debe clasificar las salvaguardas actuales y recomendadas.

SALVAGUARDAS EXISTENTES	CAPA DE PROTECCION	RECOMENDACIÓN DE NUEVAS SALVAGUARDAS	CAPA DE PROTECCION
Apertura manual de válvula de purga.	PROCESO	Gestión de alarmas para control de nivel	ALARMA
Control de nivel de la caldera.	BPCS		
Alarma por bajo nivel.	ALARMA	Sistema adicional de seguridad (SIS) para nivel	SIS
Válvula de alivio	PROCESO	Gerenciamiento de alarmas para control de presión.	ALARMA
Control de presión.	BPCS		
Alarma por alta presión.	ALARMA	Sistema adicional de seguridad (SIS) para presión	SIS
Válvula de salida del vapor	PROCESO	Control de flujo del vapor	BPCS
Medidor de temperatura	PROCESO	Control de temperatura	BPCS
Control de combustión	BPCS	Sistema de Gestión de quemado	SIS
	RESPUESTA DE EMERGENCIA DE LA COMUNIDAD		

Tabla 29. Identificación de capas de protección del caso de estudio

En la tabla 29, se identificaron a que capas de protección pertenecen las salvaguardas existentes y recomendadas. Observando que la caldera cuenta con buenas medidas para el correcto funcionamiento, pero es escaso en buenas medidas de prevención y mitigación del riesgo.

En el análisis de capas de protección se debe considerar la frecuencia de accidentes de cada capa de protección para cada una de las desviaciones a reducir.

Ref	1	2	3	4	5			6	7	8	9	10
#	Descripción del evento inicial	Nivel de gravedad	Causa de iniciación	Probabilidad de la causa	Capas de Protección			Acceso restringido a mitigaciones adicionales	Adicional IPL de Mitigación, Diques Alivio de Presión	Probabilidad de evento intermedio	SIF, IL & PFD	Probabilidad de evento mitigado
					Diseño de proceso	BPCS	ALARMAS					
1	Perdidas económicas por año, por mala calidad de vapor afectando el funcionamiento de algunas maquinas	I	Falla en bomba de alimentación a la caldera por mala lectura del sensor.	0,01	1	0,1	1	1	-	1,0E-03	1,0E-02	1,0E-05
			Falla en el control de nivel.	0,1	1	0,1	1	1	-	1,0E-02	1,0E-03	1,0E-05
	Daños leves en maquinaria e instrumentación	I	Mala limpieza del sensor de nivel.	0,1	1	0,1	1	1	-	1,0E-02	1,0E-01	1,0E-03
			Falla por operario que deja activa la bomba de alimentación	0,1	1	0,1	1	1	-	1,0E-02	1,0E-01	1,0E-03
2	Explosión	Ca	Falla en el sensor de nivel que registra un falso nivel en la caldera por burbujas dentro de la caldera.	0,1	1	0,1	0,1	1	-	1,0E-03	1,0E-02	1,0E-05
	Incendio.	Ca			1	0,1	0,1	1	-	1,0E-03	1,0E-02	1,0E-05
	Implosión	Cr			1	0,1	0,1	1	-	1,0E-03	1,0E-02	1,0E-05
	Daño en el hogar	M	Falla del operario por dejar válvula de purga abierta	0,1	1	0,1	0,1	1	-	1,0E-03	1,0E-01	1,0E-04
	Perdidas económicas por año, por el apagado automático de la caldera.	Cr			1	0,1	0,1	1	-	1,0E-03	1,0E-02	1,0E-05

3	Explosión	Ca	Insuficiente agua en el tanque de alimentación.	0,01	1	0,1	1	1	-	1,0E-03	1,0E-02	1,0E-05
	Incendio	Ca			1	0,1	1	1	-	1,0E-03	1,0E-02	1,0E-05
	Implosión	Cr			1	0,1	1	1	-	1,0E-03	1,0E-02	1,0E-05
	Daño en el hogar	M	Falla del operario por dejar válvula de purga abierta	0,1	1	0,1	1	1	-	1,0E-02	1,0E-02	1,0E-04
	Perdidas económicas por año, por el apagado automático de la caldera.	I			1	0,1	1	1	-	1,0E-02	1,0E-03	1,0E-05
4	Daños leves en maquinaria e instrumentación	I	Menor presión de bomba de alimentación	0,01	1	0,1	1	1	-	1,0E-03	1,0E-01	1,0E-04
	Explosión	Ca			1	0,1	1	1	-	1,0E-03	1,0E-02	1,0E-05
	Incendio	Ca			1	0,1	1	1	-	1,0E-03	1,0E-02	1,0E-05
	Daño en el hogar	M			1	0,1	1	1	-	1,0E-03	1,0E-01	1,0E-04
5	Explosión	Ca	Falla del control de presión.	0,1	1	0,1	0,1	0,1	PSV	1,0E-04	1,0E-01	1,0E-05
			Mala lectura por parte del operario del manómetro	0,1						1,0E-04	1,0E-01	1,0E-05
			Mala calibración de manómetro.	0,1						1,0E-04	1,0E-01	1,0E-05
	Incendio	Ca	Falla en la válvula de alivio	0,01	1	0,1	0,1			1,0E-05	1,0E+00	1,0E-05
	Daño en el quemador	M	Falla por operario al dejar cerrada la válvula de salida de vapor	0,1	1	0,1	0,1			1,0E-04	1,0E+00	1,0E-04

6	Perdidas económicas por año, por mala calidad del vapor afectando el funcionamiento de algunas maquinas	I	No suministro de agua en caldera.	0,01	1	0,1	1	1	-	1,0E-03	1,0E-02	1,0E-05
			No hay combustión adecuada	0,1	1	0,1	1	1	-	1,0E-02	1,0E-03	1,0E-05
			Malas condiciones del agua	0,01	1	0,1	1	1	-	1,0E-03	1,0E-02	1,0E-05
7	Daños en el hogar	M	Sobredemanda de vapor	0,01	1	1	1	1	-	1,0E-02	1,0E+00	1,0E-02
8	Daños en el hogar	M	Poca demanda de vapor.	0,01	1	1	1	1	-	1,0E-02	1,0E+00	1,0E-02
			Agua no precalentada	0,01	1	1	1	1	-	1,0E-02	1,0E+00	1,0E-02
			Fugas en la caldera.	0,01	1	1	1	1	-	1,0E-02	1,0E+00	1,0E-02
9	Daños en el calentador	M	Mala combustión	0,1	1	1	1	1	-	1,0E-01	1,0E-01	1,0E-02
	Dilataciones térmicas	M			1	1	1	1	-	1,0E-01	1,0E-01	1,0E-02
	Erosión	M	Malas condiciones del agua	0,01	1	1	1	1	-	1,0E-02	1,0E-01	1,0E-03
10	Perdidas económicas por hora por mala calidad del vapor afectando el funcionamiento en las maquinas.	I	Mala combustión.	0,1	1	1	1	1	-	1,0E-01	1,0E-04	1,0E-05
			Malas condiciones del agua	0,01	1	1	1	1	-	1,0E-02	1,0E-03	1,0E-05

11	Excesivas temperaturas de gases.	M	Mala calibración en boquillas de suministro de ACPM.	0,1	1	0,1	1	1	-	1,0E-02	1,0E-02	1,0E-04
			Falla en el manómetro.	0,01	1	0,1	1	1	-	1,0E-03	1,0E-02	1,0E-05
	Perdidas económicas por año por desperdicio de combustible.	I	Mala calibración en presión de atomización.	0,1	1	0,1	1	1	-	1,0E-02	1,0E-03	1,0E-05
	Incendios.	Ca	Falla de la fotocelda	0,01	1	0,1	1	1	-	1,0E-03	1,0E-02	1,0E-05
12	Perdidas económicas por año por desperdicio de combustible.	I	Mala calibración en boquillas de suministro de A.C.P.M.	0,1	1	0,1	1	1	-	1,0E-02	1,0E-02	1,0E-04
	Implosión	Cr	Taponamiento en boquillas por suciedad del A.C.P.M.	0,01	1	0,1	1	1	-	1,0E-03	1,0E-02	1,0E-05
			Fallo en la fotocelda.	0,01	1	0,1	1	1	-	1,0E-03	1,0E-02	1,0E-05
	Explosión.	Ca	Falla en el manómetro	0,01	1	0,1	1	1	-	1,0E-03	1,0E-02	1,0E-05
13	Explosión.	Ca	Falsa llama.	0,01	1	0,1	1	1	-	1,0E-03	1,0E-02	1,0E-05
			Falla en el control de quemado.	0,1	1	0,1	1	1	-	1,0E-02	1,0E-03	1,0E-05
			Suciedad en la fotocelda	0,01	1	0,1	1	1	-	1,0E-03	1,0E-02	1,0E-05
	Implosión	Cr	Cortocircuito.	0,1	1	0,1	1	1	-	1,0E-02	1,0E-03	1,0E-05
	Incendio.	Ca	Taponamiento de boquillas por suciedad en el ACPM	0,1	1	0,1	1	1	-	1,0E-02	1,0E-03	1,0E-05

Tabla 30. LOPA caso de estudio

7.5.2. NIVEL INTEGRIDAD DE SEGURIDAD (SIL)

Para le empresa caso de estudio, se aplicó matriz de riesgo como técnica cualitativa para determinar el SIL requerido de todas las SIF como se observa en la tabla 31.

	PROBABILIDAD			
CONSECUENCIAS	Frecuente	Poco Frecuente	Remoto	Improbable
Catastrófica	3	3	3	2
Critico	3	3	2	1
Marginal	3	2	2	1
Insignificante	2	2	1	A

Tabla 31. Determinación SIL con matriz de riesgo caso de estudio

Ref	Descripción del evento inicial		Consecuencia	Frecuencia	SIL
1	Perdidas económicas por año, por mala calidad de vapor afectando el funcionamiento de algunas maquinas	Falla en bomba de alimentación a la caldera por mala lectura del sensor.	Insignificante	Frecuente	2
		Falla en el control de nivel.	Insignificante	Poco frecuente	2
	Daños leves en maquinaria e instrumentación	Mala limpieza del sensor de nivel.	Insignificante	Remoto	1
		Falla por operario que deja activa la bomba de alimentación	Insignificante	Remoto	1
2	Explosión	Falla en el sensor de nivel que registra un falso nivel en la caldera por burbujas dentro de la caldera.	Catastrófico	Frecuente	3
	Incendio.		Catastrófico	Frecuente	3
	Implosión		Critico	Frecuente	3
	Daño en el hogar	Falla del operario por dejar válvula de purga abierta	Marginal	Remoto	2
	Perdidas económicas por año, por el apagado automático de la caldera.		Insignificante	Remoto	1
3	Explosión	Insuficiente agua en el tanque de alimentación.	Catastrófico	Frecuente	3
	Incendio		Catastrófico	Frecuente	3
	Implosión		Critico	Frecuente	3
	Daño en el hogar	Falla del operario por dejar válvula de purga abierta	Marginal	Remoto	2
	Perdidas económicas por año, por el apagado automático de la caldera.		Insignificante	Remoto	1

4	Daños leves en maquinaria e instrumentación	Menor presión de bomba de alimentación	Insignificante	Frecuente	2
	Explosión		Catastrófico	Frecuente	3
	Incendio		Catastrófico	Frecuente	3
	Daño en el hogar		Marginal	Frecuente	3
5	Explosión	Falla del control de presión.	Catastrófico	Poco frecuente	3
		Mala lectura por parte del operario del manómetro	Catastrófico	Remoto	3
		Mala calibración de manómetro.	Catastrófico	Remoto	3
	Incendio	Falla en la válvula de alivio	Catastrófico	Poco frecuente	3
	Daño en el quemador	Falla por operario al dejar cerrada la válvula de salida de vapor	Marginal	Remoto	2
6	Perdidas económicas por año, por mala calidad del vapor afectando el funcionamiento de algunas maquinas	No suministro de agua en caldera.	Insignificante	Poco frecuente	2
		No hay combustión adecuada	Insignificante	Frecuente	2
		Malas condiciones del agua	Insignificante	Poco frecuente	2
7	Daños en el hogar	Sobredemanda de vapor	Marginal	Poco frecuente	2
8	Daños en el hogar	Poca demanda de vapor.	Marginal	Poco frecuente	2
		Agua no precalentada	Marginal	Remoto	2
		Fugas en la caldera.	Marginal	Remoto	2
9	Daños en el calentador	Mala combustión	Marginal	Frecuente	3
	Dilataciones térmicas		Marginal	Frecuente	3
	Erosión	Malas condiciones del agua	Marginal	Poco frecuente	2
10	Perdidas económicas por hora por mala calidad del vapor afectando el funcionamiento en las maquinas.	Mala combustión.	Insignificante	Frecuente	2
		Malas condiciones del agua	Insignificante	Poco frecuente	2

11	Excesivas temperaturas de gases.	Mala calibración en boquillas de suministro de ACPM.	Insignificante	Remoto	1
		Falla en el manómetro.	Insignificante	Frecuente	2
	Perdidas económicas por año por desperdicio de combustible.	Mala calibración en presión de atomización.	Insignificante	Remoto	1
	Incendios.	Falla de la fotocelda	Catastrófico	Frecuente	3
12	Perdidas económicas por año por desperdicio de combustible.	Mala calibración en boquillas de suministro de A.C.P.M.	Insignificante	Remoto	1
	Implosión	Taponamiento en boquillas por suciedad del A.C.P.M.	Critico	Remoto	2
		Fallo en la fotocelda.	Critico	Frecuente	3
	Explosión.	Falla en el manómetro	Catastrófico	Frecuente	3
13	Explosión.	Falsa llama.	Catastrófico	Frecuente	3
		Falla en el control de quemado.	Catastrófico	Poco frecuente	3
		Suciedad en la fotocelda	Catastrófico	Remoto	3
	Implosión	Cortocircuito.	Critico	Poco frecuente	3
	Incendio.	Taponamiento de boquillas por suciedad en el ACPM	Catastrófico	Remoto	3

Tabla 32. SIL requerido Matriz de riesgo

Debido a que se asignaría un SIL 3 por este método, entonces se debe considerar con mayor detalle mediante un método cuantitativo para determinación del SIL. Para ello el equipo de trabajo, decidió implementar la gráfica de riesgos calibrado porque permite la determinación del SIL de manera cuantitativa, asignando valores a parámetros tan relevantes como la vulnerabilidad. Las demás técnicas son subjetivas y no se cuenta con la experiencia suficiente para desarrollarlas.

#	Descripción del evento inicial		Consecuencia	Ocupación	Posibilidad de evitar el accidente	Probabilidad de que ocurra el evento	SIL
1	Perdidas económicas por año, por mala calidad de vapor afectando el funcionamiento de algunas maquinas	Falla en bomba de alimentación a la caldera por mala lectura del sensor.	Ca	-	-	W2	N.R
		Falla en el control de nivel.	Ca	-	-	W2	N.R
	Daños leves en maquinaria e instrumentación	Mala limpieza del sensor de nivel.	Ca	-	-	W2	N.R
		Falla por operario que deja activa la bomba de alimentación	Ca	-	-	W2	N.R
2	Explosión	Falla en el sensor de nivel que registra un falso nivel en la caldera por burbujas dentro de la caldera.	Cd	Fa	Pa	W2	2
	Incendio.		Cd	Fa	Pa	W2	2
	Implosión		Cc	Fa	Pa	W2	1
	Daño en el hogar	Falla del operario por dejar válvula de purga abierta	Cb	Fa	Pa	W2	N.R
	Perdidas económicas por año, por el apagado automático de la caldera.		Ca	-	-	W2	N.R
3	Explosión	Insuficiente agua en el tanque de alimentación.	Cd	Fa	Pa	W2	2
	Incendio		Cd	Fa	Pa	W2	2
	Implosión		Cc	Fa	Pa	W2	1
	Daño en el hogar	Falla del operario por dejar válvula de purga abierta	Cb	Fa	Pa	W2	N.R
	Perdidas económicas por año, por el apagado automático de la caldera.		Ca	-	-	W2	N.R
4	Daños leves en maquinaria e instrumentación	Menor presión de bomba de alimentación	Ca	-	-	W2	N.R
	Explosión		Cd	Fa	Pa	W2	2
	Incendio		Cd	Fa	Pa	W2	2
	Daño en el hogar		Cb	Fa	Pa	W2	N.R.
5	Explosión	Falla del control de presión.	Cd	Fa	Pa	W1	1
		Mala lectura por parte del operario del manómetro	Cd	Fa	Pa	W1	1
		Mala calibración de manómetro.	Cd	Fa	Pa	W1	1
	Incendio	Falla en la válvula de alivio	Cd	Fa	Pa	W1	1

	Daño en el quemador	Falla por operario al dejar cerrada la válvula de salida de vapor	Cb	Fa	Pa	W1	N.R.
6	Perdidas económicas por año, por mala calidad del vapor afectando el funcionamiento de algunas maquinas	No suministro de agua en caldera.	Ca	-	-	W2	N.R
		No hay combustión adecuada	Ca	-	-	W2	N.R
		Malas condiciones del agua	Ca	-	-	W2	N.R
7	Daños en el hogar	Sobredemanda de vapor	Cb	Fa	Pa	W2	N.R.
8	Daños en el hogar	Poca demanda de vapor.	Cb	Fa	Pa	W2	N.R.
		Agua no precalentada	Cb	Fa	Pa	W2	N.R.
		Fugas en la caldera.	Cb	Fa	Pa	W2	N.R.
9	Daños en el calentador	Mala combustión	Ca	-	-	W3	N.R
	Dilataciones térmicas		Ca	-	-	W3	N.R
	Erosión	Malas condiciones del agua	Ca	-	-	W2	N.R
10	Perdidas económicas por hora por mala calidad del vapor afectando el funcionamiento en las maquinas.	Mala combustión.	Ca	-	-	W3	N.R
		Malas condiciones del agua	Ca	-	-	W2	N.R
11	Excesivas temperaturas de gases.	Mala calibración en boquillas de suministro de ACPM.	Ca	-	-	W2	N.R
		Falla en el manómetro.	Ca	-	-	W2	N.R
	Perdidas económicas por año por desperdicio de combustible.	Mala calibración en presión de atomización.	Ca	-	-	W2	N.R
	Incendios.	Falla de la fotocelda	Cd	Fa	Pa	W2	2
12	Desperdicio de combustible.	Mala calibración en boquillas de suministro de A.C.P.M.	Ca	-	-	W2	N.R
	Implosión	Taponamiento en boquillas por suciedad del A.C.P.M.	Cc	Fa	Pa	W2	1
		Fallo en la fotocelda.	Cc	Fa	Pa	W2	1

	Explosión.	Falla en el manómetro	Cd	Fa	Pa	W2	2
13	Explosión.	Falsa llama.	Cd	Fa	Pa	W2	2
		Falla en el control de quemado.	Cd	Fa	Pa	W2	2
		Suciedad en la fotocelda	Cd	Fa	Pa	W2	2
	Implosión	Cortocircuito.	Cc	Fa	Pa	W2	1
	Incendio.	Taponamiento de boquillas por suciedad en el ACPM	Cd	Fa	Pa	W2	2

Tabla 33. Matriz de Riesgo Calibrada Caso de estudio.

COMPARACIÓN SIL

Ref	Desviación de la Variable	Descripción del evento inicial		SIL Matriz de Riesgo	SIL Grafico de Riesgo Calibrada	SIL LOPA	ALARP	Medidas de reducción de riesgo
1	Mas Nivel de la caldera	Perdidas económicas por año, por mala calidad de vapor afectando el funcionamiento de algunas maquinas	Falla en bomba de alimentación a la caldera por mala lectura del sensor.	2	N.R	1,0E-02	1.23	Gestión de Alarmas
			Falla en el control de nivel.	2	N.R	1,0E-03	1.23	
		Daños leves en maquinaria e instrumentación	Mala limpieza del sensor de nivel.	1	N.R	1,0E-01	1.237	
			Falla por operario que deja activa la bomba de alimentación	1	N.R	1,0E-01	1.237	
2	Menos Nivel de la caldera	Explosión	Falla en el sensor de nivel que registra un falso nivel por burbujas dentro de la caldera.	3	2	1,0E-02	> 1	SIF con SIL 2
		Incendio.		3	2	1,0E-02	> 1	
		Implosión		3	1	1,0E-02	> 1	
		Daño en el hogar	Falla del operario por dejar válvula de purga abierta	2	N.R	1,0E-01	0.34	-
		Perdidas económicas por año, por el apagado automático de la caldera.		1	N.R	1,0E-02	0.995	-

3	No Nivel de la caldera	Explosión	Insuficiente agua en el tanque de alimentación.	3	2	1,0E-02	> 1	SIF con SIL 2
		Incendio		3	2	1,0E-02	> 1	
		Implosión		3	1	1,0E-02	> 1	
		Daño en el hogar	Falla del operario por dejar válvula de purga abierta	2	N.R	1,0E-02	1.48	Gestión de alarmas
		Perdidas económicas por año, por el apagado automático de la caldera.		1	N.R	1,0E-03	0.995	-
4	Inverso Nivel de la caldera	Daños leves en maquinaria e instrumentación	Menor presión de bomba de alimentación	2	N.R	1,0E-01	0.61	-
		Explosión		3	2	1,0E-02	> 1	SIF con SIL 2
		Incendio		3	2	1,0E-02	> 1	
		Daño en el hogar		3	N.R.	1,0E-01	1.48	Gestión de alarmas
5	Mas Presión de la caldera	Explosión	Falla del control de presión.	3	1	1,0E-01	> 1	SIF con SIL 1
			Mala lectura por parte del operario del manómetro	3	1	1,0E-01	> 1	
			Mala calibración de manómetro.	3	1	1,0E-01	> 1	
		Incendio	Falla en la válvula de alivio	3	1	1,0E+00	> 1	
		Daño en el quemador	Falla por operario al dejar cerrada la válvula de salida de vapor	2	N.R.	1,0E+00	0,14	-
6	Menos Presión de la caldera	Perdidas económicas por año, por mala calidad del vapor afectando el funcionamiento de algunas maquinas	No suministro de agua en caldera.	2	N.R	1,0E-02	0,06	-
			No hay combustión adecuada	2	N.R	1,0E-03	0,06	-
			Malas condiciones del agua	2	N.R	1,0E-02	0,06	-
7	Alto Flujo de Vapor de la caldera	Daños en el hogar	Sobredemanda de vapor	2	N.R.	1,0E+00	3,96	Control de flujo de vapor
8	Bajo Flujo de Vapor de la caldera	Daños en el hogar	Poca demanda de vapor.	2	N.R.	1,0E+00	3,96	
			Agua no precalentada	2	N.R.	1,0E+00	3,96	
			Fugas en la caldera.	2	N.R.	1,0E+00	3,96	

9	Alta Temperatura de vapor	Daños en el calentador	Mala combustión	3	N.R	1,0E-01	1,87	Gestión de alarmas
		Dilataciones térmicas		3	N.R	1,0E-01	0,75	-
		Erosión	Malas condiciones del agua	2	N.R	1,0E-01	2,49	Gestión de alarmas
10	Baja Temperatura de vapor	Perdidas económicas por hora por mala calidad del vapor afectando el funcionamiento en las maquinas.	Mala combustión.	2	N.R	1,0E-04	3,71	
			Malas condiciones del agua	2	N.R	1,0E-03	3,71	
11	Exceso Combustión (Llama)	Excesivas temperaturas de gases.	Mala calibración en boquillas de suministro de ACPM.	1	N.R	1,0E-02	-	-
			Falla en el manómetro.	2	N.R	1,0E-02	-	-
		Perdidas económicas por año por desperdicio de combustible.	Mala calibración en presión de atomización.	1	N.R	1,0E-03	0.056	-
		Incendios.	Falla de la fotocelda	3	2	1,0E-02	> 1	SIF con SIL 2
12	Poca Combustión (Llama)	Perdidas económicas por año por desperdicio de combustible.	Mala calibración en boquillas de suministro de A.C.P.M.	1	N.R	1,0E-02	0,056	-
		Implosión	Taponamiento en boquillas por suciedad del A.C.P.M.	2	1	1,0E-02	> 1	SIF con SIL 2
			Fallo en la fotocelda.	3	1	1,0E-02	> 1	
		Explosión.	Falla en el manómetro	3	2	1,0E-02	> 1	
13	No Combustión (Llama)	Explosión.	Falsa llama.	3	2	1,0E-02	> 1	SIF con SIL 2
			Falla en el control de quemado.	3	2	1,0E-03	> 1	
			Suciedad en la fotocelda	3	2	1,0E-02	> 1	
		Implosión	Cortocircuito.	3	1	1,0E-03	> 1	
		Incendio.	Taponamiento de boquillas por suciedad en el ACPM	3	2	1,0E-03	> 1	

Tabla 34. Comparación de SIL's Caso de estudio

7.6. ESPECIFICACION DE LOS REQUERIMIENTOS DE SEGURIDAD

De acuerdo con la tabla 34 donde se comparo los SIL's asociados, se procede a realizar la especificación de requerimientos de seguridad de las SIF necesarias para el proceso como se puede ver en la tabla 35.

REF	Lazo	Desviación de la Variable	SIL
1	Nivel	Menos Nivel de la caldera	2
		No Nivel de la caldera	2
2	Presión	Mas Presión de la caldera	1
3	Combustión	Exceso Combustión (Llama)	2
		Poca Combustión (Llama)	2
		No Combustión (Llama)	2

Tabla 35. SIF requeridas con su SIL asociado Caso de estudio

En el lazo de nivel se integran las desviaciones menos y no nivel, porque se trata de la misma variable con causas y consecuencias similares, además al evitarse un menor nivel, no se presentara la desviación de No nivel. Igualmente se hace cuando no hay combustión con una poca combustión. Quedando de la siguiente manera como se observa en la tabla 36.

REF	Lazo	Desviación de la Variable	SIL
1	Nivel	Menos Nivel de la caldera	2
2	Presión	Mas Presión de la caldera	1
3	Combustión	Exceso Combustión (Llama)	2
		Poca Combustión (Llama)	2

Tabla 36. Integracion de SIF requeridas con su SIL asociado Caso de estudio

La especificación de los requerimientos de seguridad para cada SIF, seria la siguiente:

ITEM	DETALLES DE REQUERIMIENTOS
LAZO:	1 - NIVEL
ESPECIFICACIÓN DE REQUISITOS FUNCIONALES	
Data sheets del proceso	Sensor de Nivel, Bomba de alimentación, válvulas solenoides.
Rango de operación normal de las variables del proceso y sus límites de operación.	Bomba inicia: 5.9 cms en nivel visible. Bomba apaga: 6.8 cms en nivel visible. Caldera apagada: 4.5 cms en nivel visible.
Definición de los estados seguros del proceso, para cada uno de los eventos identificados.	Si el nivel del agua baja a 4.5 cm, la caldera para automáticamente y se genera una alarma. La caldera podrá volver a operar solamente después de que el nivel normal de agua se restablezca.
Consideración para paro manual	Un interruptor de parada independiente del sistema programable.
Condiciones ambientales extremas	Instrumentación especial para manejo de agua.
Entradas del proceso a los SIS y sus puntos de disparo.	El SIS se dispara cuando: Mínimo nivel de agua en la caldera: 10% de la capacidad de la caldera.
Salidas del proceso del SIS y sus acciones	Señal eléctrica al motor de suministro de agua y cierre a las válvulas de suministro de combustible y motor del ventilador.
Requerimientos de interfaces hombre-maquina	Dar alarmas cableadas en el principal cuarto de control son requeridas por alguna falla del sistema de seguridad o condición de energizado.
Selección de des-energizadas para disparar o energizado para disparar.	El completo sistema de seguridad podría ser des-energizado para disparo
Requerimientos para ser re emplazados o bypass incluyendo como ellos deben ser purgados.	Requerido.
ESPECIFICACIÓN DE INTEGRIDAD DE SEGURIDAD	
Numero ID de la SIF	SIF 1
Descripción de la SIF	Poco nivel en la caldera
SIL requerido para la SIF	SIL 2 Modo Demanda
Tasa de demanda esperada	Una vez por año
Factor de Reducción de Riesgo RRF	100
Tiempo requerido de respuesta para los SIS para llevar el proceso a un estado seguro	5 Segundos
Intervalos de prueba	6 meses
Acciones a tomar por la perdida de energía en los SIS	Cierre de todas las válvulas

Tabla 37. S.R.S. SIF Menos nivel

ITEM	DETALLES DE REQUERIMIENTOS
LAZO:	2 -PRESION
ESPECIFICACIÓN DE REQUISITOS FUNCIONALES	
Data sheets del proceso	Sensor de Presión, Control de Presión.
Rango de operación normal de las variables del proceso y sus límites de operación.	Presión de diseño: 150 PSI Presión Máxima: 85 PSI. Presión mínima: 75 PSI. Presión de la válvula de alivio: 100 PSI
Definición de los estados seguros del proceso, para cada uno de los eventos identificados.	Si la presión sube a más de 85 PSI el quemador se apaga, y se apaga el motor que suministra agua a la caldera. Se genera una alarma por presión alta y si la presión incrementa a 100 psi la válvula de alivio se dispara.
Consideración para paro manual	-
Condiciones ambientales extremas	No aplica.
Entradas del proceso a los SIS y sus puntos de disparo.	El SIS actúa cuando: La presión en la caldera es 110 PSI.
Salidas del proceso del SIS y sus acciones	Una válvula de alivio de presión independiente de la válvula de alivio actual. Señal eléctrica al motor de suministro de agua y cierre a las válvulas de suministro de combustible y motor del ventilador.
Requerimientos de interfaces hombre-maquina	Dar alarmas cableadas en el principal cuarto de control son requeridas por alguna falla del sistema de seguridad o condición de energizado.
Selección de des-energizadas para disparar o energizado para disparar.	El completo sistema de seguridad podría ser des-energizado para disparo
Requerimientos para ser re emplazados o bypass incluyendo como ellos deben ser purgados.	Requerido.
ESPECIFICACIÓN DE INTEGRIDAD DE SEGURIDAD	
Numero ID de la SIF	SIF 2
Descripción de la SIF	Más presión en la caldera.
SIL requerido para la SIF	SIL 1 Modo demanda.
Tasa de demanda esperada	1 vez cada 5 años.
Factor de Reducción de Riesgo RRF	10.
Tiempo requerido de respuesta para los SIS para llevar el proceso a un estado seguro	5 Segundos.
Intervalos de prueba	1 año.
Acciones a tomar por la pérdida de energía en los SIS	Cierre de todas las válvulas

Tabla 38. S.R.S. SIF más presión

ITEM	DETALLES DE REQUERIMIENTOS
LAZO:	2 –COMBUSTION – EXCESIVA.
ESPECIFICACIÓN DE REQUISITOS FUNCIONALES	
Data sheets del proceso	Sensor de Llama, Controlador de llama, amplificador de llama, motor soplador, 2 válvulas solenoides, transformador
Rango de operación normal de las variables del proceso y sus límites de operación.	Fotocelda: 0 -230 voltios. Máximo: 180 voltios Mínimo: 80 voltios.
Definición de los estados seguros del proceso, para cada uno de los eventos identificados.	Se puede detener el encendido manualmente en cualquier momento, colocando el interruptor selector en OFF. Cualquier falla o interrupción en la llama principal se detecta inmediatamente por la fotocelda, cerrando la válvula principal de combustible y desenergizando el programa del motor. El motor de soplador continuara operando hasta que el control de combustión se bloquee en el punto de seguridad. Rearme manual control de combustión oprimiendo el botón reset.
Consideración para paro manual	Interrupción por falla en la llama por el visor de llama.
Condiciones ambientales extremas	La fotocelda soporta hasta 200°F.
Entradas del proceso a los SIS y sus puntos de disparo.	El SIS actúa cuando: La fotocelda esta en 200 voltios.
Salidas del proceso del SIS y sus acciones	Señal eléctrica al motor de suministro de agua y cierre a las válvulas de suministro de combustible y motor del ventilador.
Requerimientos de interfaces hombre-maquina	Dar alarmas cableadas en el principal cuarto de control son requeridas por alguna falla del sistema de seguridad o condición de energizado.
Selección de des-energizadas para disparar o energizado para disparar.	El completo sistema de seguridad podría ser des-energizado para disparo
Requerimientos para ser re emplazados o bypass incluyendo como ellos deben ser purgados.	Requerido.
ESPECIFICACIÓN DE INTEGRIDAD DE SEGURIDAD	
Numero ID de la SIF	SIF 3
Descripción de la SIF	Exceso de combustión.
SIL requerido para la SIF	SIL 2 Modo demanda.
Tasa de demanda esperada	1 vez por año.
Factor de Reducción de Riesgo RRF	100
Tiempo requerido de respuesta para los SIS para llevar el proceso a un estado seguro	5 Segundos
Intervalos de prueba	6 meses
Acciones a tomar por la pérdida de energía en los SIS	Cierre de todas las válvulas

Tabla 39. S.R.S. SIF Exceso de Combustión

ITEM	DETALLES DE REQUERIMIENTOS
LAZO:	2 –COMBUSTION – POCO.
ESPECIFICACIÓN DE REQUISITOS FUNCIONALES	
Data sheets del proceso	Sensor de Llama, Controlador de llama, amplificador de llama, motor soplador, 2 válvula solenoides, transformador.
Rango de operación normal de las variables del proceso y sus límites de operación.	Fotocelda: 0 -230 voltios. Máximo: 180 voltios Mínimo: 80 voltios.
Definición de los estados seguros del proceso, para cada uno de los eventos identificados.	Se puede detener el encendido manualmente en cualquier momento, colocando el interruptor selector en OFF. Cualquier falla o interrupción en la llama principal se detecta inmediatamente por la fotocelda, cerrando la válvula principal de combustible y desenergizando el programa del motor. El motor de soplador continuara operando hasta que el control de combustión se bloquee en el punto de seguridad. Rearme manual control de combustión oprimiendo el botón reset.
Consideración para paro manual	Interrupción por falla en la llama por el visor de llama.
Condiciones ambientales extremas	La fotocelda soporta hasta 200°F.
Entradas del proceso a los SIS y sus puntos de disparo.	El SIS actúa cuando: La fotocelda esta en 60 voltios.
Salidas del proceso del SIS y sus acciones	Señal eléctrica al motor de suministro de agua y cierre a las válvulas de suministro de combustible y motor del ventilador.
Requerimientos de interfaces hombre-maquina	Dar alarmas cableadas en el principal cuarto de control son requeridas por alguna falla del sistema de seguridad o condición de energizado.
Selección de des-energizadas para disparar o energizado para disparar.	El completo sistema de seguridad podría ser des-energizado para disparo
Requerimientos para ser re emplazados o bypass incluyendo como ellos deben ser purgados.	Requerido.
ESPECIFICACIÓN DE INTEGRIDAD DE SEGURIDAD	
Numero ID de la SIF	SIF 4
Descripción de la SIF	Poca combustión.
SIL requerido para la SIF	SIL 2 Modo demanda.
Tasa de demanda esperada	1 vez por año.
Factor de Reducción de Riesgo RRF	100
Tiempo requerido de respuesta para los SIS para llevar el proceso a un estado seguro	5 Segundos
Intervalos de prueba	6 meses
Acciones a tomar por la pérdida de energía en los SIS	Cierre de todas las válvulas

Tabla 40. S.R.S Menos combustión

La siguiente matriz que se observa en la tabla relaciona todas las entradas de las SIF's con las salidas. La intersección indica que alguna de estas relaciones puede ser forzada por el operario (2N) y solo una no requiere la intervención del operario (N).

MATRIZ CAUSA EFECTO

Tag #	SIL	Rango de Instrumento	Unidades de ingeniería	Cerrar Válvula ventilador	Cerrar válvula combustible	Abrir válvula de presión
SIF 1	2	0 -10	cms	2N	2N	
SIF 2	1	60-200	PSI	2N	2N	N
SIF 3	2	0-300	Voltios	2N	2N	
SIF 4	2	0-300	Voltios	2N	2N	

Tabla 41. Matriz Causa efecto de la empresa caso de estudio

7.7. DISEÑO BÁSICO E INGENIERÍA DE UN SIS

INDEPENDENCIA ENTRE EL SIS Y EL SISTEMA DE CONTROL BÁSICO DEL PROCESO:
Para la caldera caso de estudio se consideró diseñar el sistema instrumentado de seguridad con sensores, elementos finales y controlador lógico independiente con el fin de cumplir con lo establecido por la NFPA 85, además de esta manera se evitan fallas de causa común.

FUNCIONES INSTRUMENTADAS DE SEGURIDAD Y DE NO SEGURIDAD
Se utilizan una función de no seguridad para garantizar una secuencia de apagado correcto en la caldera. Esta única función que está en el sistema instrumentado de seguridad y que no tiene un SIL asociado, actúa cuando al recibir una señal de menos nivel, más presión, excesiva o poca combustión envía una señal primero a las válvulas para cortar el flujo de combustible, luego debe apagar el motor de bombeo de agua y debe activar el motor del ventilador para purgar la caldera.

SIS CON DIFERENTES SIL
El sistema instrumentado de seguridad cuenta con 4 funciones instrumentadas de seguridad y solo la SIF de más presión tiene un SIL menor a las demás funciones por lo tanto el SIL para el controlador lógico debe ser SIL 2, el más alto.
Los sensores de las SIF no se relacionan porque miden diferentes variables, pero los elementos finales si son compartidos, porque las acciones de salida de cada SIF, garantizan el apagado automático de la caldera. Las válvulas de corte de combustible, deben tener asociado el SIL más alto de todas las SIF, es decir 2.

DIVERSIDAD
Para evitar las fallas de causa común se considera utilizar tecnología diferente y proveedores de instrumentación de diferentes fabricantes, para cada una de las funciones instrumentadas de seguridad.
El controlador lógico debe emplear algoritmos diferentes al del sistema de control básico del proceso.

CERTIFICADO VS USO PREVIO
Para las funciones instrumentadas de seguridad que tienen asociado SIL 2, se debe considerar que la instrumentación sea certificada, porque este SIL implica un alto grado de certidumbre para que el SIS ejecute dichas funciones. Esta certificación en la instrumentación puede ser TUV o FM.

Para la función instrumentada de seguridad, mas presión se puede recurrir a las listas de uso previo, para seleccionar la instrumentación.

CARACTERISTICAS FUNCIONALES

- **Confiabilidad:** MTTF Mean Time To Failure, tiempo medio para fallar. Este valor no es brindado por la mayoría de los fabricantes, porque no considera la reparación en los equipos. Idealmente este valor debe dar 100%, es decir

que no se van a presentar averías. Por lo tanto no se considera en el diseño del SIS.

- **Disponibilidad:** MTTR Mean Time To Repair, tiempo medio de reparación. Generalmente es de 8 horas a 10 horas.
  MTBF Mean Time Between Failure, tiempo medio entre fallas, este valor debe ser dado por el fabricante. Este valor es dado en porcentaje, el valor más alto es 99,99%.

- **Diagnóstico:**
  Los siguientes términos se calcularon utilizando las tablas
  - Arquitectura
  - Fracción de falla segura SFF Safe Failure Fraction. Fracción de falla segura.
  - Tolerancia de falla de hardware HFT, Hardware Fault Tolerance, Tolerancia a fallas hardware.
  - Averías:
    - λdd (dangerous detected) = Cuota de averías detectadas peligrosas.
    - λdu (dangerous undetected) = Cuota de averías no detectadas peligrosas.
    - λsd (safe detected) = Cuota de averías detectadas seguras.
    - λsu (safe undetected) = Cuota de averías no detectadas seguras.

  - Cobertura de diagnóstico CD.

ITEM	SIF 1			SIF 2			SIF 3			SIF 4		
	Sensor	Controlador	EF	Sensor	Controlador	EF	Sensor	Controlador	EF	Sensor	Controlador	EF
MTTR	8 horas			8 horas			8 horas			8 horas		
Arquitectura	1oo1			1oo1			1oo1			1oo1		
	No se considera redundancia	Debe seleccionarse un PLC	No se considera redundancia	Sensor singular	Debe seleccionarse un PLC porque el controlador del SIS es SIL 2	Dispositivo singular	No se considera redundancia	Debe seleccionarse un PLC	No se considera redundancia	No se considera redundancia	Debe seleccionarse un PLC	No se considera redundancia
SFF	De 90 a 99%			De 60 a 90%			De 90 a 99%			De 90 a 99%		
HFT	0			0			0			0		
Averías segura	0.04 Se presenta cada 25 años.											
Averías peligrosas	0.02 Se presenta cada 50 años.											
CD	99.9 %											
Causa común	N.A											

Tabla 42. Características Funcionales del SIS Caso de estudio

Consideraciones de funcionamiento del SIS:

Fuente de alimentación: 110v, 60Hz.

Sistema de puesta en tierra: Se debe cumplir con los estándares para garantizar la puesta en tierra de la instrumentación.

BYPASS: las válvulas bypass deben estar instaladas cerca a las válvulas SIS de suministro de combustible. Además deben ser conectadas a un sistema de alarma que alerten al operario que la válvula bypass está abierta.

SOFTWARE DE APLICACIÓN: Se considera el uso de la lógica “ladder” para la programación del controlador SIS.

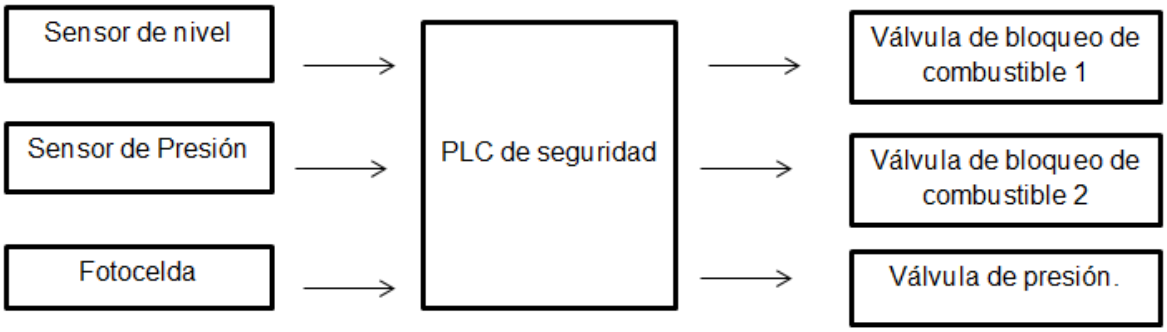

Tabla 43. Propuesta de un proyecto del SIS Caso de estudio

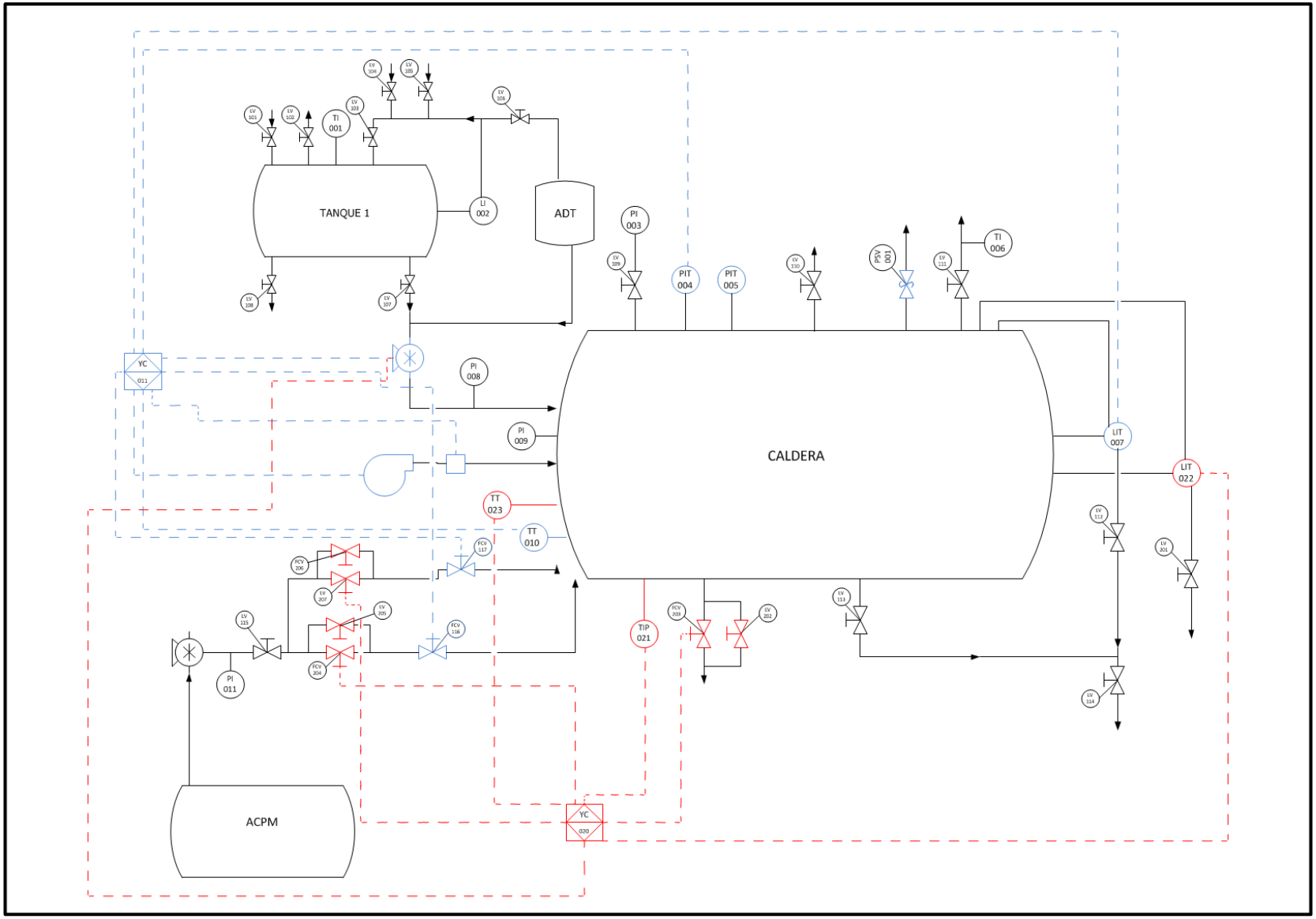

Figura 14. P&ID Caldera Con SIS

8. CONCLUSIONES

- El estándar ANSI/ISA 84 sugiere una metodología para abordar el ciclo de vida de un sistema instrumentado de seguridad a través de la descripción y orientación de etapas que inician en un análisis de riesgo hasta la desinstalación de un sistema instrumentado de seguridad; es así como el proyecto de grado define criterios de cómo desarrollar desde la etapa análisis de riesgo hasta el diseño de un sistema instrumentado de seguridad.

- La guía de aplicación permite asesorar la creación de medidas de seguridad a fin de prevenir los riesgos y llevar la caldera caso de estudio a un nivel aceptable de seguridad y de igual manera como instaurar las políticas de seguridad para lograr mantener y mejorar el nivel de seguridad.

- Es fundamental contar con un equipo de trabajo multidisciplinar, que permita la diversidad de conocimientos y experiencias, para hacer más detallada el desarrollo de cada etapa del SIS.

- En la etapa análisis de riesgo, la técnica HAZOP permitió realizar una amplia identificación de los peligros de una manera dinámica con el equipo de trabajo.

- EL reglamento técnico Colombiano RTC, para la evaluación de los riesgos brinda una orientación básica para la clasificación del riesgo, porque no tiene en cuenta el objetivo de seguridad de la empresa. A diferencia del concepto ALARP que permitió clasificar mejor los riesgos y relacionar costo-beneficio.

- Para la evaluación de las capas de protección de una caldera, LOPA es una técnica completa y de fácil compresión para su aplicación.

- Para determinar el SIL asociado a cada SIF, la técnica cualitativa matriz de riesgo dio SIL muy altos, a diferencia de las técnicas cuantitativas que dan SIL más exactos.

- La documentación de que y como debe actuar el sistema instrumentado de seguridad deben ser redactados de forma clara y completa, porque es fundamental para el diseño del sistema instrumentado de seguridad.

- Las consideraciónes de diseño y las características funcionales de la instrumentación deben estar detallados para que en la etapa de instalación del SIS, se realice una buena selección de la instrumentación y así validar que el SIS cumple con los requerimientos de seguridad definidos.

- Las calderas son máquinas que implican un alto riesgo de operación, porque tiene asociada varias funciones instrumentadas de seguridad con niveles de integridad altos.

- Con este proyecto queda abierta la posibilidad de seguir desarrollando temáticas en base al estándar ANSI/ISA 84, es así como sería posible trabajar en las fases siguientes instalación, validación del SIS, operación y mantenimiento del SIS para un sistema de seguridad funcional

9. BIBLIOGRAFIA

[1]. ANSI/ISA-84.00.01-2004. “Functional Safety: Safety Instrumented Systems for the Process Industry Sector Part 1 Framework, Definitions, System, Hardware and Software Requirements”. International Society of Automation. Disponible en www.ISA.org. [Acceso en Noviembre 15, 2010].

[2]. Vergara Paulo, “Impacto de la implementación de un sistema de gestión de seguridad funcional en los SIS” II Jornada de Automatización de la industrial petrolera JAIP/Colombia 2011 [Acceso en Septiembre 8 de 2011].

[3]. García L. M. CFSE, “Automatización del Ciclo de Vida de un SIS, para cumplir con los requerimientos de la IEC 61511 y/o ANSI/ISA 84.00.01. Herramienta de automatización”, Siemens Energy & Automation, Sumneytown Pike, Spring House, [Acceso en Septiembre 14 de 2011].

[4]. ANSI/ISA-84.00.01-2004. “Functional Safety: Safety Instrumented Systems for the Process Industry Sector - Part 2: Guidelines for the Application of ANSI/ISA-84.00.01-2004 Part 1”. International Society of Automation. Disponible en www.ISA.org. [Acceso en Noviembre 15, 2010].

[5]. ANSI/ISA-84.00.01-2004. “Functional Safety: Safety Instrumented Systems for the Process Industry Sector - Part 3: Guidance for the Determination of the Required Safety Integrity Levels – Informative. Disponible en www.ISA.org. [Acceso en Noviembre 15, 2010]

[6]. United States Deparment of labor, Occupational Safety & Health Administration. Disponible en http://www.osha.gov. [Acceso en Octubre 27 de 2011].

[7]. Cortes, Federico Julio. “Sistemas Instrumentados de Seguridad”. GN La revista del gas natural. Disponible en: http://larevistadelgasnatural.osinerg.gob.pe/presentaciones/files/112_2.pdf [Acceso 20 de Febrero de 2012].

[8]. Puerta, Fernando Alonso de la, “Guía para la selección y aplicación de las técnicas de PHA (análisis de peligros de procesos)”, Universitat Politècnica de Catalunya. Disponible en http://upcommons.upc.edu/pfc/handle/2099.1/4187. [Acceso en Octubre 21 de 2011].

[9]. NFPA 8501-1997. “Standard for single burner boiler operation”. [Acceso en Octubre 10 de 2011].

[10]. Spirax Sarco Engienieering. “Interior de una caldera”. España. [Acceso en Enero 8 de 2012]

[11]. The babcock & Wilcox Company. “Boilers”. Charlotte, E.E.U.U. [Acceso 10 de Febrero de 2012]

[12]. Ministerios de Protección Social y de Minas y Energía. “Reglamento Técnico de Calderas Para Colombia”. Disponible en: http://responsabilidadintegral.org/administracion/circulares/archivos/reglamento%20tecnico%20calderas.pdf. [Acceso 18 de Febrero de 2012].

[13]. GM International Technology for Safety. “Manual SIL - Safety Instrumented Systems”. [Acceso 22 de Febrero de 2012].

[14]. Gruhn Paul. “Safety instrumented systems. Design, analysis, and justification - (2005). (2nd ed., ISA)”. [Acceso en Abril 23 de 2012]

[15]. Alvarado Rosa. Determinación de un sistema instrumentado de seguridad (SIS) y su nivel de integridad de seguridad (SIL). Universidad Central de Venezuela. Disponible en: http://saber.ucv.ve/jspui/handle/123456789/692. [Acceso en Mayo 1 de 2012].