UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

EVALUACIÓN DE LA INSTRUMENTACIÓN ELECTRÓNICA PARA PROCESOS PELIGROSOS DE UNA REFINERÍA DE PETRÓLEO

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRÓNICO

PRESENTADO POR:

BRIAN THOMAS SALAZAR MORALES

PROMOCIÓN
2007- I

LIMA – PERÚ
2011

EVALUACIÓN DE LA INSTRUMENTACIÓN ELECTRÓNICA PARA PROCESOS PELIGROSOS DE UNA REFINERÍA DE PETRÓLEO

A mi familia, por el incondicional apoyo que siempre me ha brindado.

SUMARIO

El presente informe de suficiencia trata de la evaluación de las características de los instrumentos electrónicos utilizados en sistemas de seguridad aplicados a procesos industriales peligrosos. Es de mucha importancia este tema, pues ayuda a comprender de que manera se debe utilizar la instrumentación para reducir el nivel de riesgo de los procesos. Las características tanto funcionales como de desempeño son normadas por organismos internacionales, principalmente por la Comisión Electrotécnica Internacional IEC. El IEC ha dispuesto dos estándares de uso mandatorio por fabricantes y usuarios de instrumentación: IEC 61508 e IEC 61511, ambos estándares son consultados para la elaboración del presente informe.

Se presentan conceptos modernos referidos a instrumentación de seguridad, tales como: **Función Instrumentada de Seguridad**, **Sistema Instrumentado de Seguridad y Nivel de Integridad Segura,** este último para referirse a cuan confiable es un sistema de seguridad. Estas definiciones deben ser tomadas en cuenta por los ingenieros en las nuevas plantas industriales o para la implementación de sistemas que ayuden a prevenir accidentes no deseados en plantas existentes.

Por último, la aplicación de esta instrumentación es expuesta en un sistema de seguridad que se implementa en los proceso de Destilación del crudo de una Refinería de Petróleo.

ÍNDICE

INTRODUCCIÓN

A lo largo de los seis capítulos que integran este informe, se aborda el tema de la instrumentación electrónica utilizada en procesos industriales peligrosos con el propósito de evaluar y exponer sus características desde el punto de vista de los estándares internacionales IEC para luego poder aplicarla a los procesos de una refinería de petróleo.

Asimismo, con este informe se pretende destacar la importancia de la utilización de estos instrumentos con características especiales en los procesos industriales para reducir su nivel de riesgo y así prevenir accidentes con consecuencias lamentables. Además, se presenta una propuesta para implementar un sistema de seguridad en los procesos de Destilación de crudo de una refinería.

El Capítulo I contiene una introducción con los objetivos y alcances del informe realizado. En el Capítulo II se presenta un resumen de los procesos más importantes de una Refinería de Petróleo, destacando los pertenecientes a la Destilación del crudo. El Capítulo III muestra un resumen de los instrumentos electrónicos más comunes que se utilizan en los procesos de una refinería de petróleo. El Capítulo IV y Capítulo V toman como referencia a los estándares IEC 61508 e IEC 61511 para la evaluación que se hace a los procesos industriales y a los instrumentos electrónicos de seguridad. Luego de una presentación de los procesos de una refinería, de los instrumentos electrónicos industriales, de las normas IEC 61505 e IEC 61511, el Capítulo VI expone la implementación de un Sistema de Seguridad en los procesos peligrosos de la Destilación del crudo de una Refinería tomando como base los capítulos anteriores.

Finalmente, los anexos complementan el desarrollo del presente informe y ayudan a comprender mejor los estándares IEC.

CAPÍTULO I
ANTECEDENTES

1.1 Objetivo

La Evaluación de la Instrumentación Electrónica para Procesos Peligrosos de una Refinería de Petróleo tiene los siguientes objetivos:

a) Evaluar las características de funcionalidad de los instrumentos electrónicos de seguridad basados en las normas IEC 61508 e IEC 61511.

b) Evaluar las características de desempeño de de los instrumentos electrónicos de seguridad basados en las normas IEC 61508 e IEC 61511.

c) Explicar la importancia de la implementación de un sistema de seguridad en los procesos industriales.

d) Explicar el uso del Nivel de Integridad Segura (SIL) para especificar el grado de seguridad que se desea en un sistema.

e) Describir la implementación de un Sistema Instrumentado de Seguridad (SIS) en los procesos de la Destilación del crudo dentro de una Refinería de Petróleo.

1.2 Alcances

Los alcances del presente trabajo son los siguientes:

a) Definir los conceptos relacionados a la seguridad de los procesos industriales.

b) Describir los principales instrumentos electrónicos utilizados en una Refinería de Petróleo.

c) Describir los estándares internacionales referidos a la seguridad de los procesos industriales.

d) Evaluar los requerimientos que exigen las normas IEC 61508 e IEC 61511.

e) Describir los Niveles de Integridad Segura para operaciones en demanda y operaciones continuas.

f) Identificar las diversas arquitecturas que se pueden implementar para mejorar el nivel de seguridad de un proceso.

g) Aplicar el concepto de PFD en un ejemplo de un Sistema Instrumentado de Seguridad.

h) Describir el Sistema Básico de Control que gobierna inicialmente los procesos de la Destilación del crudo de una Refinería.

i) Describir la implementación de un Sistema Instrumentado de Seguridad realizado a los procesos de la Destilación del crudo.

1.3 Antecedentes históricos

La seguridad en las plantas industriales es hoy en día uno de los temas de mayor preocupación en la industria a nivel mundial, debido a que una inadecuada valoración de los riesgos asociados a los procesos involucrados, ha producido en algunas organizaciones, accidentes fatales y grandes pérdidas económicas como consecuencia de los costos de tratamiento, compensación y rehabilitación de los afectados, reparación y reposición de equipos dañados, pérdida de producción, etc.

Por citar algunos ejemplos tenemos:

Fuga de sustancia tóxica en Bophal, India 1984 (Union Carbide India Ltd.).- El escape del isocianato de metilo (MIC) produjo la muerte de 3500 personas. Los informes destacaron una serie de factores que contribuyeron al accidente: la inexistencia de sistemas de corte en las tuberías para evitar la entrada de agua del lavado, la presencia del MIC en el depósito a una temperatura demasiado elevada, el sistema de lavado de gases no funcionaba adecuadamente [1].

Incendio por derrame de petróleo en Cubatao, Brasil 1984 (PETROBRAS).- El derrame y posterior incendio produjo la muerte de 500 personas. La investigación indica que la posible causa del derrame se debió a que no existía ningún sistema de medida de presión en el oleoducto [2].

Explosión en planta de petróleo en San Juan, México 1984 (PEMEX).- El incendio produjo la muerte de más de 500 personas. Los informes revelan que se produjo una ruptura en la tubería de suministro de GLP de la refinería a la planta de almacenamiento debida a la sobrepresión en la tubería por sobrellenado de uno de los depósitos. Las válvulas de alivio y corte no funcionaron [3].

Estos casos nos dan una referencia de las consecuencias producidas por no contar con un sistema de seguridad en sus procesos peligrosos.

El uso de sistemas de control industrial, basados en DCS (Sistemas de Control Distribuido) o simples PLC (Controladores Lógicos Programables), garantizan la continuidad operativa del proceso pero estos sistemas no protegen convenientemente el equipo bajo control ni el entorno sencillamente porque no fueron concebidos para "no fallar". Es por ello que en la década del 80´, importantes comisiones internacionales se formaron para elaborar un estándar que facilite a fabricantes y plantas adecuarse a esta necesidad [4].

CAPÍTULO II
DESCRIPCIÓN DEL PROCESO DE DESTILACIÓN EN UNA REFINERÍA DE PETRÓLEO

En este Capítulo describiremos las etapas existentes en una Refinería de Petróleo. Además describiremos con más detalle el proceso de destilación, el cual será base para el desarrollo del Capítulo 6.

2.1 Definición de crudo

El crudo o petróleo crudo es una mezcla compleja de hidrocarburos con pequeñas cantidades de sulfuros, nitrógeno, sales y metales como el Níquel (Ni), Vanadio (V) y Cobre (Cu). Es oleoso y más ligero que el agua, de color oscuro y olor fuerte; se encuentra nativo en el interior de la Tierra y a veces forma grandes yacimientos de donde se extrae y traslada a las refinerías [5].

2.2 Procesos de destilación

Los procesos de refinación del crudo pueden clasificarse en tres grupos mayores: Separación, Conversión y Tratamiento [6].

La Destilación es el proceso más común del grupo de Separación. Dentro del grupo de Conversión se incluye: craqueo, hidroproceso, isomerización, alquilación, reformación. Y el Tratamiento es el proceso final donde se dan los últimos retoques a los productos obtenidos en los procesos anteriores [6]. En la Figura 2.1 se observan los procesos más importantes de una refinería.

El proceso de destilación, también conocido como fraccionamiento, es la primera etapa del procesamiento del crudo. En este proceso el crudo atraviesa los hornos de calentamiento para elevar su temperatura hasta la ebullición y luego en las columnas de destilación se recondensa en componentes basados en los rangos de sus puntos de ebullición [7].

2.2.1 Hornos de calentamiento

Estos son equipos industriales en los que se entrega el calor generado por la combustión de un elemento combustible (por ejemplo residual, gas natural) a una carga de crudo que circula por dentro de unos tubos en forma de serpentín. En la Figura 2.2 se

ilustran los dos hornos de calentamiento con los que cuenta una refinería.

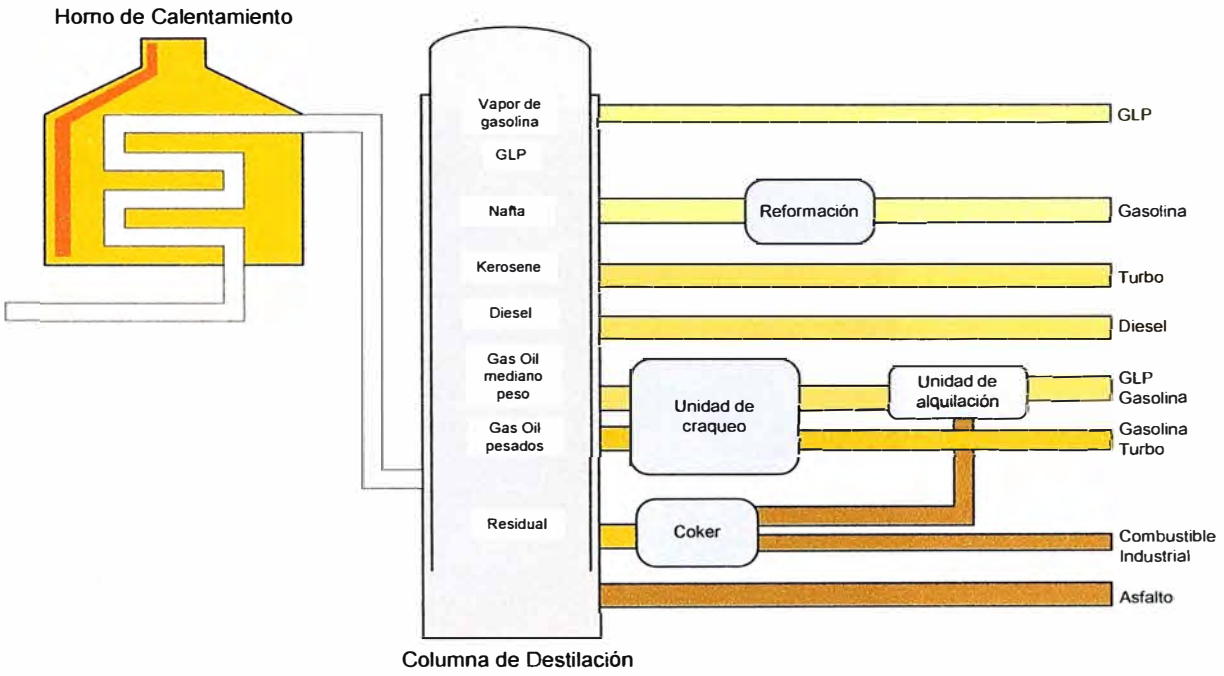


Fig. 2.1 Procesos más importantes de una refinería de petróleo

Fig. 2.2 Hornos de calentamiento

2.2.2 Columnas de destilación

Las columnas de destilación permiten separar el crudo en diversas fracciones. Para este propósito, una de las columnas opera a presión atmosférica y la otra en condiciones de vacío, que aprovechando la diferente volatilidad de los componentes, se logra su separación, siendo los pesados (fuel oil, asfalto) recolectados en la parte inferior de la

columna y los livianos (gasolina, GLP, diesel) recolectados en la parte superior. La Figura 2.3 muestra una de las dos columnas de destilación con las que cuenta una refinería.

Fig. 2.3 Columna de destilación

CAPÍTULO III
INSTRUMENTACIÓN ELECTRÓNICA INDUSTRIAL

Dentro de las variables más importantes que se miden y controlan en los procesos industriales se encuentran el flujo, presión y temperatura. La Figura 3.1 muestra un esquema de la Instrumentación Electrónica que describiremos en este Capítulo y que son parte de los utilizados en los diversos procesos de una refinería para medir y controlar las variables antes mencionadas.

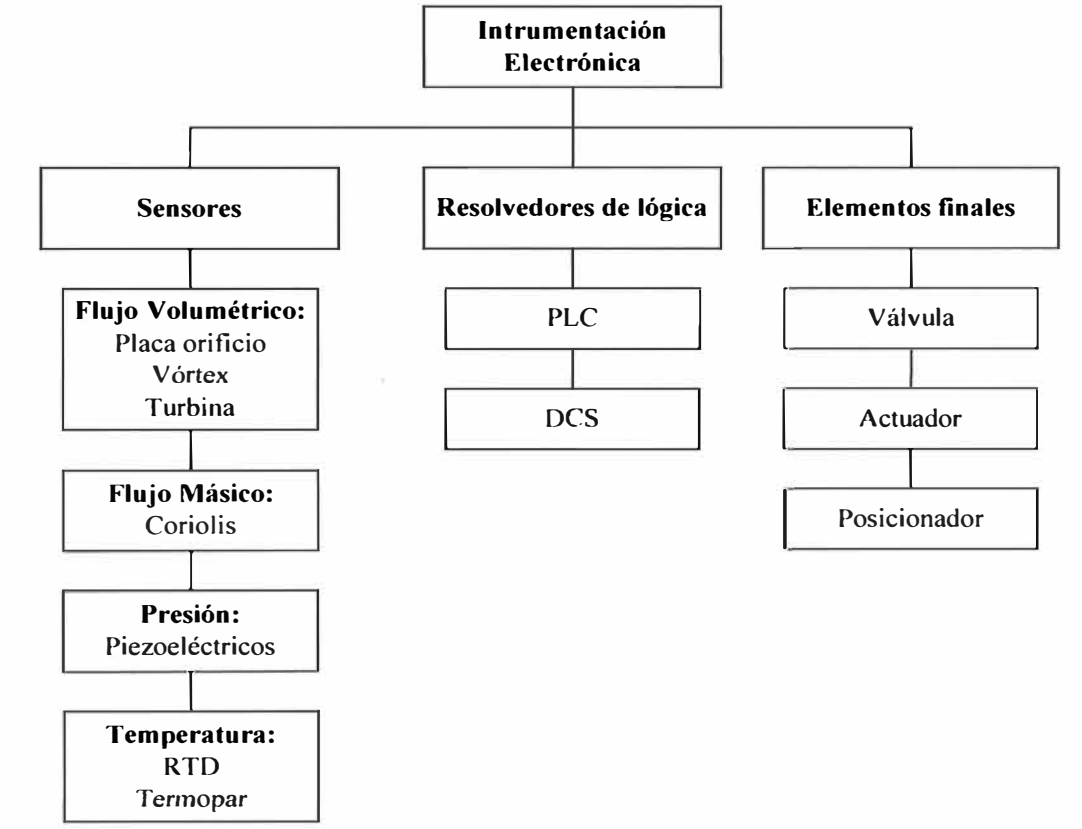


Fig. 3.1 Esquema de la instrumentación electrónica utilizada en los proceso de una refinería de petróleo

3.1 Medición de flujo volumétrico

3.1.1 Medidor de placa orifico

Consiste en una placa perforada instalada en la tubería. Dos tomas conectadas en la parte anterior y posterior de la placa, captan esta presión diferencial la cual es proporcional

al cuadrado del caudal [8]. Utilizado en tuberías de proceso superiores a 1", y poseen una rangeabilidad (valores máximos y mínimos capaces de medir) de 3:1.

La Figura 3.2 muestra su símbolo según la norma ANSI/ISA-S5, y la Figura 3.3 muestra una placa orificio montada con un transmisor de presión diferencial.

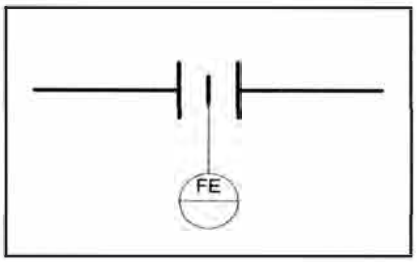


Fig. 3.2 Símbolo ANSI/ISA-S5 para la placa orificio

Fig. 3.3 Placa orificio con transmisor de presión diferencial

3.1.2 Medidor tipo Vórtex

Un cuerpo en forma de cono en el interior del tubo genera alternativamente vórtices (aéreas de baja presión) desfasados en 180º, cuya frecuencia es directamente proporcional a la velocidad y por lo tanto, al caudal [8]. Utilizados en tuberías de proceso desde ½" a 12", y poseen una rangeabilidad (valores máximos y mínimos capaces de medir) de 10:1.

La Figura 3.4 muestra su símbolo según la norma ANSI/ISA-S5, y la Figura 3.5 muestra un medidor tipo Vórtex.

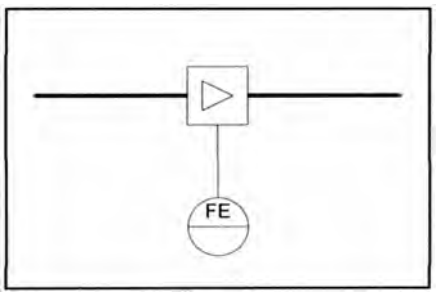


Fig. 3.4 Símbolo ANSI/ISA-S5 para el medidor Vórtex

Fig. 3.5 Medidor de caudal tipo Vórtex

3.1.3 Medidor tipo turbina

Se basa en la determinación de la frecuencia del remolino producido por una hélice estática situada dentro de la tubería que atraviesa el fluido. La frecuencia del remolino es proporcional a la velocidad del fluido y, por lo tanto, al caudal [8]. Utilizados en tuberías de proceso desde ¼" a 12", y poseen una rangeabilidad (valores máximos y mínimos capaces de medir) de 10:1.

La Figura 3.6 muestra su símbolo según la norma ANSI/ISA-S5, y la Figura 3.7 muestra un medidor tipo turbina.

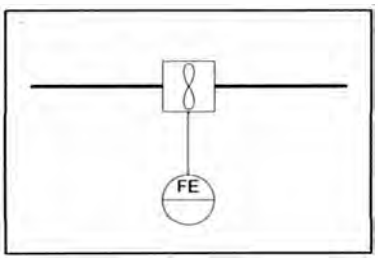


Fig. 3.6 Símbolo ANSI/ISA-S5 para el medidor de turbina

Fig. 3.7 Medidor de caudal tipo turbina

En la Tabla 3.1 se muestra una comparación entre las características de los medidores de flujo volumétrico.

TABLA Nº 3.1 Características de los medidores de flujo volumétrico

	Caudal máx/mín	**Escala**	**Servicio**	**Coste relativo**	**Ventajas**	**Desventajas**
Placa orificio	3:1	cuadrática	Liq. / vapor	Bajo	Simple, económico	Solo fluidos limpios, baja precisión
Vórtex	10:1	lineal	Liq. / gas	Medio	Soporta vibraciones	Solo fluidos no viscosos
Turbina	10:1	lineal	Liq. / gas	Alto	Precisión	Caro, solo fluidos limpios

3.2 Medición de flujo másico

3.2.1 Medidor de Coriolis

Basados en el teorema de Coriolis, calculan directamente el flujo másico del fluido que los atraviesa. Poseen buena precisión: +/- 0.5% [8]. Utilizados en tuberías de proceso desde 1/8" a 12", y poseen una rangeabilidad (valores máximos y mínimos capaces de medir) de 20:1.

La Figura 3.8 muestra un medidor de flujo másico tipo Coriolis.

Fig. 3.8 Medidor de flujo tipo Coriolis

En la Tabla 3.2 se muestra un resumen de las características del medidor de flujo másico tipo Coriolis.

TABLA Nº 3.2 Características de los medidores de flujo másico

	Caudal máx/min	Escala	Servicio	Coste relativo	Ventajas	Desventajas
Coriolis	20:1	lineal	Liq. / gas	Alto	Preciso, independiente de presión, temperatura, densidad	Caro

3.3 Medición de presión

La presión puede medirse en valores absolutos, manométricos o diferenciales. En la Figura 3.9 se indican las clases de presión que los instrumentos miden comúnmente en la industria.

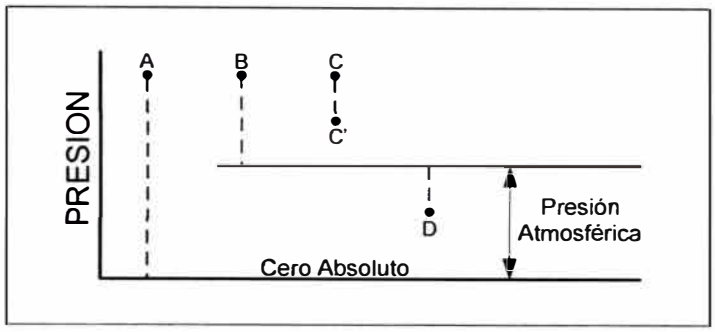


Fig. 3.9 Clases de presión

La **presión absoluta** se mide con relación al cero absoluto de presión (punto A). La **presión relativa** o **manométrica** es la determinada por un elemento que mide la diferencia entre la presión absoluta y la atmosférica del lugar donde se efectúa la medición (punto B). La **presión diferencial** es la diferencia entre dos presiones (puntos C y C'). El **vacío** es la diferencia de presiones entre la presión atmosférica existente y la presión absoluta, es decir, es la presión medida por debajo de la atmosférica (punto D) [8].

3.3.1 Sensores con elementos piezoeléctricos

Formados por elementos cristalinos que, al deformarse físicamente por la acción de una presión, generan una señal eléctrica [8]. Los instrumentos con estos elementos cuentan con doble diafragma que sirven para medir presión absoluta, manométrica, diferencial y de vacío.

La Figura 3.10 muestra el símbolo según la norma ANSI/ISA-S5 para los medidores de presión (a) manométrica, de vacío, (b) diferencial, la Figura 3.11 muestra un transmisor de presión manométrica y la Figura 3.12 muestra un transmisor de presión diferencial.

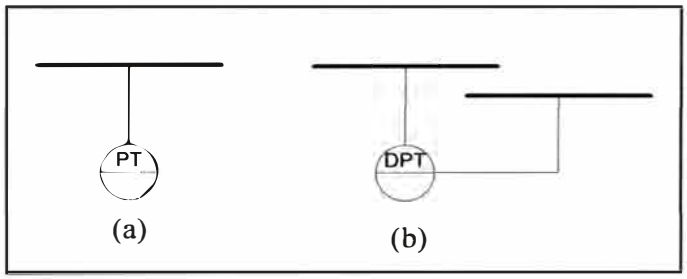


Fig. 3.10 Símbolo ANSI/ISA-S5 para instrumentos de presión

Fig. 3.11 Medidor de presión manométrica

Fig. 3.12 Medidor de presión diferencial

En la Tabla 3.3 se muestra un resumen de las características de los medidores de presión con elementos piezoeléctricos.

TABLA Nº 3.3 Características de los medidores de presión

	Margen (bar)	**Precisión**	**Estabilidad en el tiempo**	**Sensibilidad a vibraciones**
Piezoeléctricos	0,1 - 600	1%	mala	baja

3.4 Medición de temperatura

Existen diversos fenómenos físicos que son influidos por la temperatura y que son utilizados para medirla. En la industria de procesos, son dos fenómenos los más importantes: variación de resistencia de un conductor y f.e.m. creada en la unión de dos metales distintos. Estos son la base de los medidores RTD y termopares respectivamente [8].

La Figura 3.13 muestra el símbolo según la norma ANSI/ISA-S5 para los medidores de temperatura.

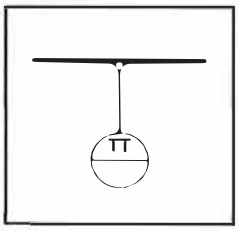


Fig. 3.13 Símbolo ANSI/ISA-S5 para instrumentos de temperatura

3.4.1 Elementos con variación de resistencia (RTD)

La medida de temperatura depende de las características de resistencia en función de la temperatura que son propias del elemento de detección. El material que forma el conductor se caracteriza por su coeficiente de temperatura. Los materiales más usados por su amplia linealidad son el Platino (Pt) y el Níquel (Ni) [8].

3.4.2 Termopar

Formado por la unión de dos metales diferentes los cuales desarrollan una pequeña tensión continua proporcional a la temperatura de la unión de medida. Dependiendo del rango de temperatura a medir se selecciona el tipo de termopar con los metales adecuados. Los tipos más comunes de termopares son el J (hierro – constantán) y el K (cromel – alumel) [8].

La Figura 3.14 muestra un termopar con termopozo de protección.

Fig. 3.14 Medidor de temperatura tipo termopar

En la Tabla 3.4 se muestra una comparación entre las características de los medidores de temperatura.

TABLA Nº 3.4 Características de los medidores de temperatura

	Precisión relativa	**Rango**	**Costo relativo**	**Velocidad de respuesta**	**Estabilidad en el tiempo**
RTD	mayor	-200 a +850 ºC	mayor	lenta	excelente
Termopar	menor	-200 a +2000 ºC	menor	rápida	mala

3.5 Resolvedores de lógica / Controladores

3.5.1 Controladores Lógicos Programables (PLC)

El PLC es un dispositivo electrónico digital con memoria programable para almacenar instrucciones que implementan funciones como: lógica secuencial, de tiempo y de cuenta, cálculos aritméticos, etc. Usado para el control de máquinas y procesos [8].

Los PLC's fueron concebidos inicialmente como una alternativa más eficiente a la lógica de control en sistemas discretos; es decir, aquellos en los que las variables son variables discretas binarias (on/off); inclusive, de allí el origen del nombre "controlador lógico". Sin embargo, actualmente su campo de acción abarca el procesamiento, totalización o regulación de variables continuas y analógicas.

Versiones especiales de PLC's son utilizados en sistemas de seguridad debido a la implementación de características solicitadas por los organismos internacionales.

3.5.2 Sistemas de Control Distribuido (DCS)

El control distribuido es un sistema jerarquizado en varios niveles con uno o varios microprocesadores controlando las variables que están repartidas por la planta, conectando por un lado a las señales de los transmisores de las variables y por el otro a las válvulas de control. La filosofía de este control es distribuir el riesgo de fallo para asegurar una continuidad operativa de la planta [8].

La Figura 3.15 muestra el símbolo según la norma ANSI/ISA-S5 para los (a) PLC, (b) DCS.

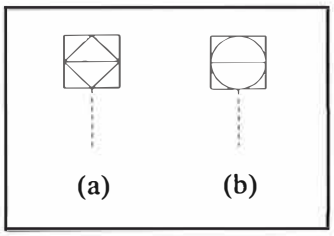


Fig. 3.15 Símbolo ANSI/ISA-S5 de resolvedores de lógica

3.6 Elementos finales de control

3.6.1 Válvula tipo globo

Son válvulas de movimiento lineal en las que el obturador se mueve en la dirección de su propio eje. Usadas para regulación modulante y fina [8].

La Figura 3.16 muestra su símbolo según la norma ANSI/ISA-S5, y la Figura 3.17 muestra una válvula globo montada con un actuador.

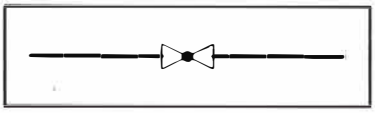


Fig. 3.16 Símbolo ANSI/ISA-S5 para válvulas globo.

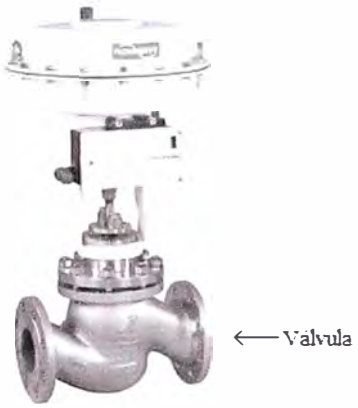


Fig. 3.17 Válvula tipo globo

3.6.2 Válvula tipo bola (esférica)

Son válvulas de movimiento circular en donde el obturador en forma de bola tiene un corte adecuado y gira transversalmente 90°. Usado para efectuar una apertura y corte rápida [8].

La Figura 3.18 muestra su símbolo según la norma ANSI/ISA-S5, y la Figura 3.19 muestra el cuerpo de una válvula bola.

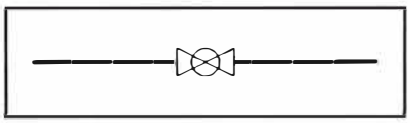


Fig. 3.18 Símbolo ANSI/ISA-S5 para válvulas bola.

Fig. 3.19 Válvula tipo bola

3.6.3 Actuador

El actuador neumático consiste en un diafragma con resorte que trabaja regularmente entre 3 – 15 psi. Al aplicar cierta presión de aire sobre el diafragma, el resorte se comprime

de tal manera que el mecanismo empieza a moverse abriendo o cerrando la válvula [8].

La Figura 3.20 muestra el símbolo según la norma ANSI/ISA-S5 para los actuadores (a) de diafragma, (b) de cilindros, y la Figura 3.21 muestra un actuador de diafragma montado sobre una válvula.

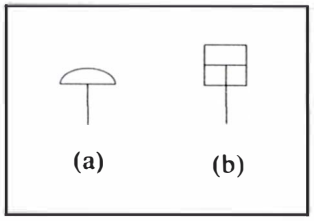


Fig. 3.20 Símbolo ANSI/ISA-S5 para actuadores

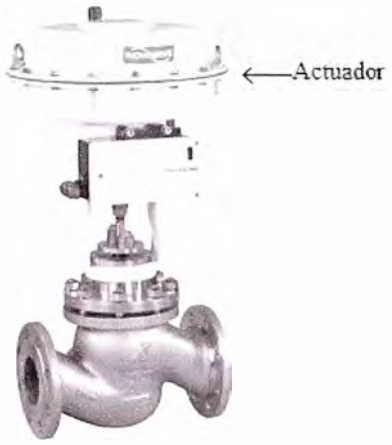


Fig. 3.21 Actuador de diafragma

3.6.4 Posicionador eléctrico

Esencialmente es un controlador proporcional de posición con punto de consigna procedente del controlador externo (PLC, DCS) en 4 – 20 mA. El Posicionador compara la señal de entrada con la posición del vástago y si esta no es correcta, envía aire al actuador o bien lo elimina en el grado necesario para que la posición del vástago corresponda exactamente a la señal de entrada [8].

La Figura 3.22 muestra el símbolo según la norma ANSI/ISA-S5 para los posicionadores eléctricos y la Figura 3.23 muestra un posicionador eléctrico de simple efecto.

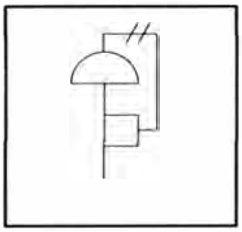


Fig. 3.22 Símbolo ANSI/ISA-S5 para posicionadores

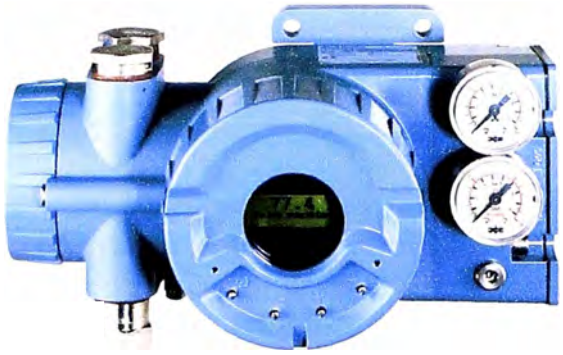


Fig. 3.23 Posicionador eléctrico

CAPÍTULO IV
SEGURIDAD EN PROCESOS INDUSTRIALES

La seguridad en los procesos industriales involucra varios temas que son expuestos por diversos estándares internacionales. En el presente Capítulo presentaremos los estándares referidos a esta área principalmente según la IEC. Estos estándares son importantes porque establecen un modelo a seguir para la fabricación e implementación de los instrumentos electrónicos industriales para sistemas de seguridad. Además, nos basaremos en los estándares IEC 61508 e IEC 61511 para exponer los conceptos fundamentales de esta área.

Para una mejor comprensión de los términos y abreviaturas se ha elaborado un Glosario que se encuentra en el Anexo E.

4.1 Estándares Internacionales

4.1.1 Estándares IEC

La Comisión Electrotécnica Internacional (IEC, por sus siglas en inglés) ha dispuesto 2 estándares orientados a la seguridad en la industria de procesos. Estos estándares imponen rigurosas condiciones, de uso mandatario, en la integración de equipos y sistemas de protección.

IEC 61508: "Seguridad Funcional de los sistemas de seguridad eléctricos / electrónicos / electrónicos programables" (7 partes)

Publicado en 1996. Este estándar establece un enfoque genérico para todas las actividades del ciclo de vida de los sistemas de seguridad compuestos por componentes E/E/PE utilizados para llevar a cabo funciones de seguridad [9].

Es aplicable a todos los sistemas de seguridad, independiente de la aplicación.

IEC 61511: "Seguridad Funcional - Sistemas Instrumentados de Seguridad para la industria de procesos" (3 partes)

Publicado en 2003. Este estándar está desarrollado como aplicación del estándar IEC 61508 y orientado para la industria de procesos. Establece recomendaciones para la especificación, diseño, instalación, operación y mantenimientos de un sistema instrumentado de seguridad (SIS) [10]. Establece la relación con el estándar IEC 61508

como se observa en la Figura 4.1.

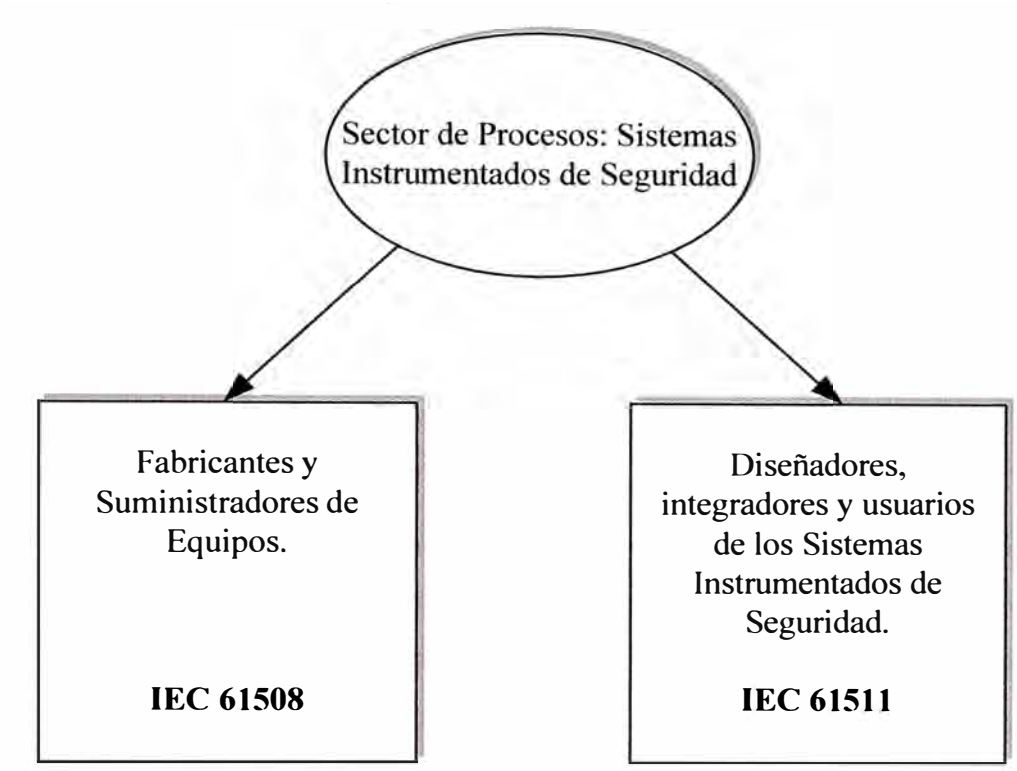


Fig. 4.1 Relación entre el estándar IEC 61508 e IEC 61511

Las estructuras completas de estos 2 estándares se encuentran en el Anexo A.

4.1.2 Estándares ISA

ANSI/ISA-S84.01-1996: "Aplicación de Sistemas Instrumentados de Seguridad para la industria de procesos".

Publicado en 1996. Este estándar es específico para la industria de proceso y orientado la aplicación de sistemas instrumentados de seguridad. No cubre el modelo completo del ciclo de vida de seguridad como lo establecido por IEC [11].

Reemplazado por la S84.00.01.

ANSI/ISA-84.00.01-2004 "Seguridad Funcional: Sistemas Instrumentados de Seguridad para la industria de procesos". (3 partes)

Publicado en 2004. Basado en el estándar IEC-61511. Da recomendaciones para la especificación, diseño, instalación, operación y mantenimientos de un SIS [12].

4.2 Peligros y Riesgos

Todo proceso industrial posee cierto peligro que puede desencadenar un acontecimiento no deseado, ya sea una lesión física, un daño menor a la propiedad o un impacto mayor al medio ambiente.

Considerando que el riesgo de un peligro es la combinación de la probabilidad de ocurrencia del daño y la severidad o consecuencia del daño, podemos citar algunos ejemplos de procesos peligrosos con diferentes niveles de riesgo:

a) Reacción química en un tanque reactor que opera a elevada temperatura.

b) Transporte de sustancias tóxicas a un tanque de almacenamiento.

c) Bombeo de combustible a través de un poliducto que atraviesa un rio.

d) Ingreso de combustible a los quemadores de un horno de refinería para su encendido.

e) Circulación de crudo de petróleo a través de un horno de refinería para su calentamiento.

De esta manera, para un mejor análisis y una mejor evaluación, los riesgos se clasifican según 6 niveles de probabilidad y 4 niveles de consecuencias. La combinación obtenida es una matriz como la mostrada en la Tabla 4.1 donde los riesgos resultantes se agrupan en 3 clases de riesgo: Clase I, Clase II y Clase III.

TABLA Nº 4.1Clasificación de Riesgos

Probabilidad	**Clase de Riesgo**			
	Consecuencia Catastrófica	**Consecuencia Crítica**	**Consecuencia Marginal**	**Consecuencia Insignificante**
Frecuente	I	I	I	II
Probable	I	I	II	II
Ocasional	I	II	II	II
Remoto	II	II	II	III
Improbable	II	III	III	III
Increible	II	III	III	III

La clase de riesgo que presente un proceso servirá para definir qué medidas se deben tomar para garantizar la realización de un proceso seguro. La interpretación de las clases de riesgo se encuentra en la Tabla 4.2.

TABLA Nº 4.2 Interpretación de clases de riesgo

Clase de riesgo	**Interpretación**
Clase I	Riesgo intolerable. Se requiere tomar medidas de control inmediatas.
Clase II	Riesgo indeseable, y tolerable solamente si la reducción del riesgo no es práctica o si los costos de la reducción son mayores al beneficio obtenido.
Clase III	Riesgo despreciable. Considerado como insignificante.

Es criterio de cada organización u empresa la identificación y calificación de los riesgos que poseen sus procesos.

Por ejemplo una empresa puede definir sus niveles de probabilidad y consecuencia como:

Probabilidad

Frecuente: Accidente que puede esperarse más de dos veces al año

Probable: Accidente que puede esperarse una vez al año.

Ocasional: Accidente que puede esperarse en 5 años.

Remoto: Accidente que puede esperarse durante la vida útil de la planta.

Improbable: Accidente raramente escuchado en la industria.

Increíble: Accidente nunca escuchado en la industria.

Consecuencia

Catastrófica: Múltiples muertes dentro y fuera de la planta.

Crítica: Lesión incapacitante o muerte del trabajador.

Marginal: Lesión menor con tratamientos médicos.

Insignificante: Sin lesión de trabajadores.

4.3 ALARP (As Low As Reasonably Practicable)

El modelo ALARP o "Tan bajo como sea razonablemente práctico" según su traducción al español, es un modelo que indica que los riesgos deben ser reducidos lo mayor posible de acuerdo a su practicidad. Debe haber una desproporción entre el riesgo existente y el sacrificio involucrado (tiempo, dinero, dificultad) en reducirlo más para considerarlo como ALARP [13]. La Figura 4.2 muestra este modelo presentado por el HSE Health and Safety Executive y que se ha hecho extensivo a todos los sectores de la industria.

4.4 Sistemas Instrumentados de Seguridad (SIS)

Los Sistemas Instrumentados de Seguridad (SIS) son métodos más convenientes que se utilizan para reducir los riesgos de los procesos peligrosos y mantenerlos en un nivel de riesgo tolerable [14].

Están formados por una combinación de sensores, resolvedores de lógica (controladores) y elementos finales de control (válvulas y actuadores), tal como muestra la

Figura 4.3, que detectan condiciones anormales de funcionamiento y automáticamente llevan el proceso a condiciones seguras de operación [15].

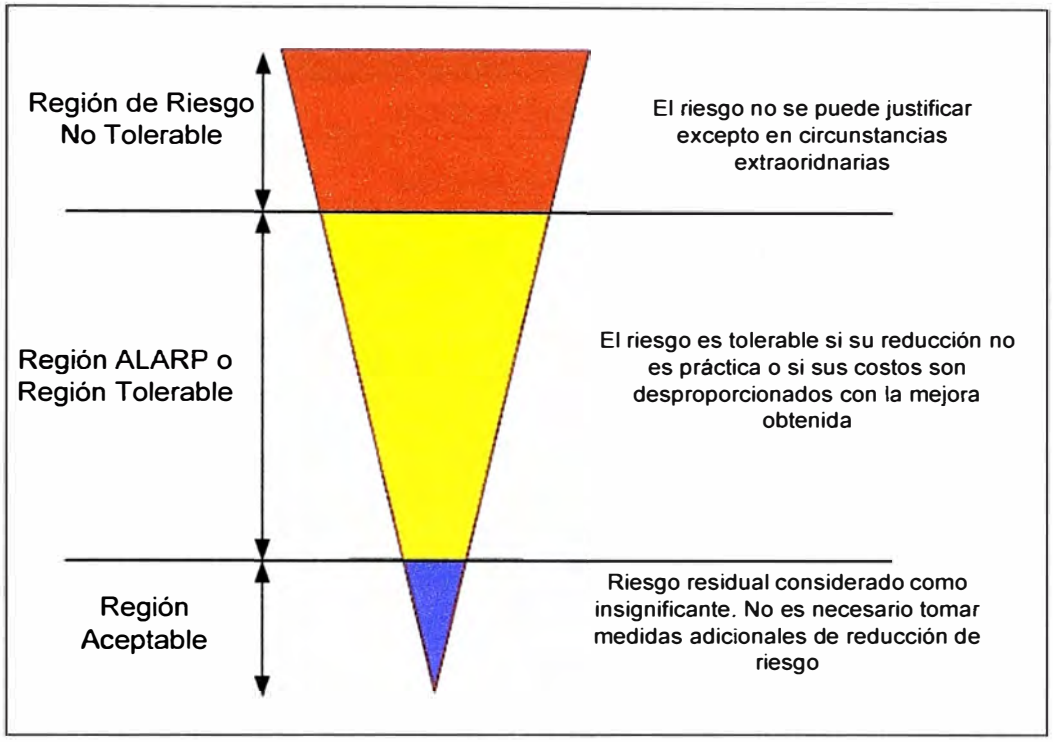


Fig. 4.2 Modelo ALARP según The Health and Safety Executive (HSE)

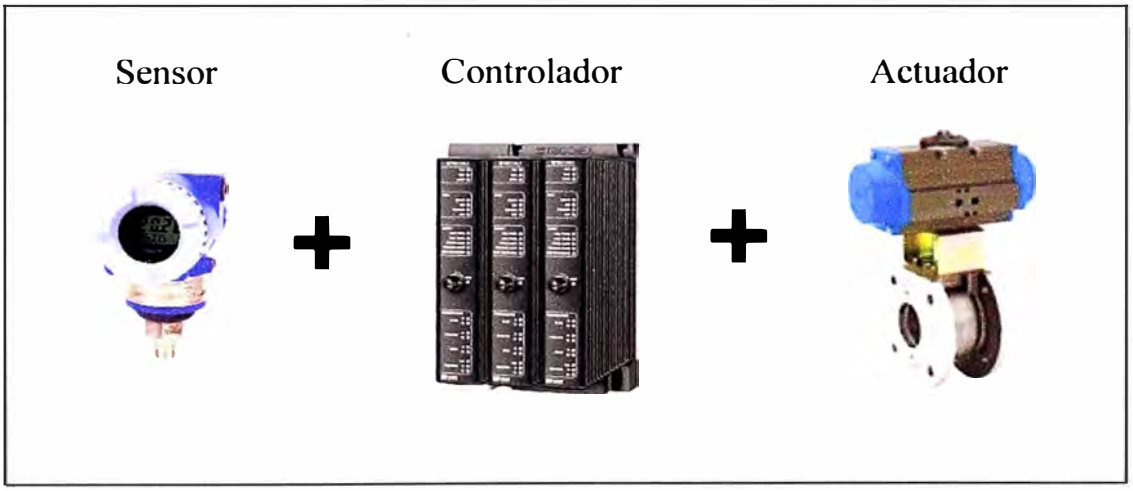


Fig. 4.3 Componentes de un SIS

La Figura 4.4 muestra el concepto general de reducción de riesgo. El riesgo existente del proceso sin seguridad alguna, debe ser reducido utilizando un SIS.

El Sistema Instrumentado de Seguridad (SIS) ejecutará una función de seguridad específica por cada proceso peligroso identificado con la finalidad de reducir su riesgo y mantenerlo en un estado seguro. Esta función de seguridad se denomina **Función Instrumentada de Seguridad** (SIF) [15].

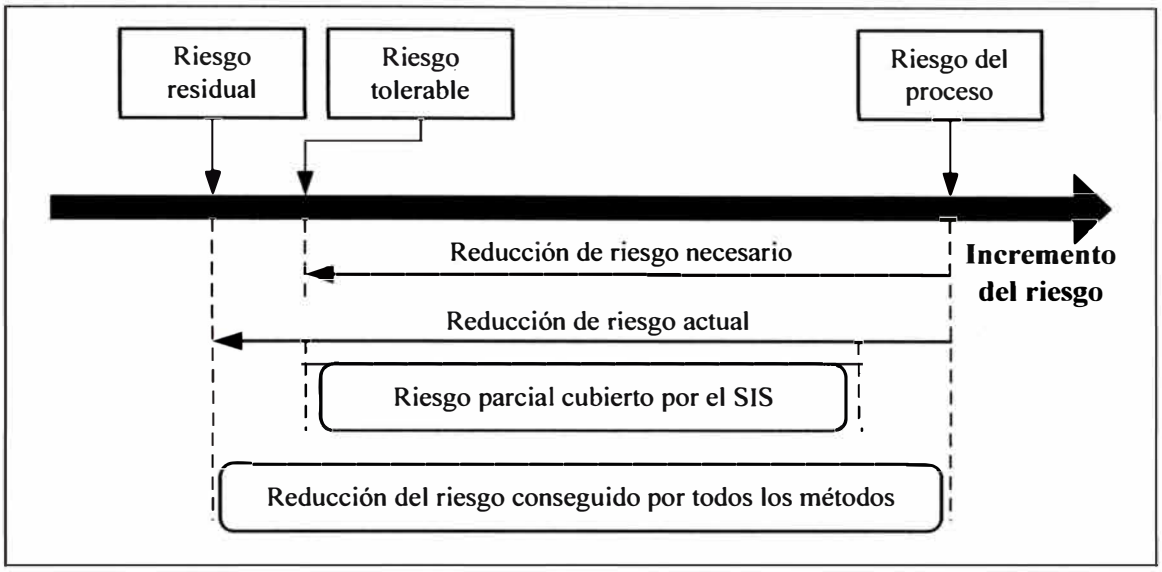


Fig. 4.4 Reducción de riesgos

Entre los demás métodos utilizados para la reducción de riesgos se tiene: Sistemas Básicos de Control de Procesos (BPCS), Sistema de Alarmas, Sistema de Supervisión, Respuesta ante una emergencia, Capacitación del personal, etc. [16]. Muchas veces, un SIS no basta para llevar el riesgo a un nivel tolerable.

Estos Sistemas de Seguridad están físicamente separados de los Sistemas Básicos de Control de Procesos (DCS, PLC) que se usan regularmente en las plantas. El objetivo de los BPCS es asegurar la continuidad operativa y productiva de los procesos, mientras que los SIS pueden iniciar una secuencia de parada de emergencia (ESD) si se detecta alguna condición insegura en el proceso [17].

Se permiten ciertas comunicaciones entre el BPCS y el SIS solo para información del operador, como lo ilustrado en la Figura 4.5.

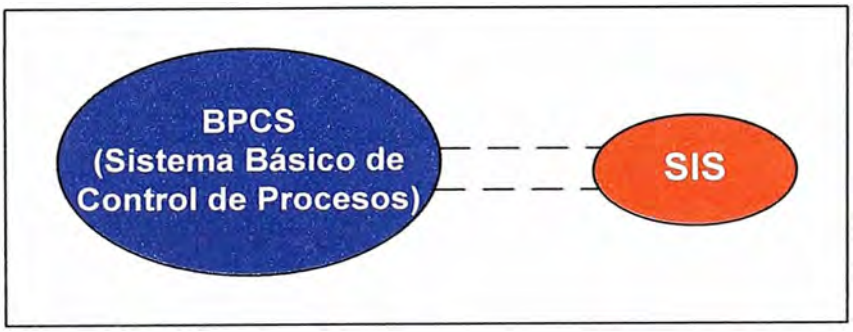


Fig. 4.5 Independencia entre BPCS y SIS

4.5 Ejemplos de Funciones Instrumentadas de Seguridad

De acuerdo a los ejemplos vistos en la sección 4.2, en la Tabla 4.3 podemos mencionar las funciones instrumentadas de seguridad que corresponden a dichos procesos peligrosos.

TABLA Nº 4.3 Ejemplos de Funciones Instrumentadas de Seguridad

Peligros	Funciones Instrumentadas de Seguridad
Reacción química en un tanque reactor que opera a elevada temperatura.	Apertura de fluido refrigerante para prevenir rupturas por alta temperatura.
Transporte de sustancias tóxicas a un tanque de almacenamiento.	Cierre de válvula de entrada a tanques para prevenir rebosamientos de capacidad que pueden resultar en contaminación del medio ambiente.
Bombeo de combustible a través de un poliducto que atraviesa un rio.	Cierre de válvula de bloqueo en poliducto al detectar sobre presión y prevenir que la tubería reviente.
Ingreso de combustible a los quemadores de un horno de refinería para su encendido.	Corte de combustible en un horno industrial cuando la presión de combustible es demasiado baja para mantener la combustión, pudiendo resultar en fuga y posible explosión en la cámara de combustión.
Circulación de crudo de petróleo a través de un horno de refinería para su calentamiento.	Iniciar secuencia de apagado seguro al detectar bajo caudal de crudo que ingresa al horno de una refinería para evitar daños al interior del horno por sobrecalentamiento.

4.6 Sistema de Administración de Quemadores (BMS)

Sistema de control dedicado a la seguridad de sistemas de combustión y de asistencia al operador en los arranques y paradas de la preparación de circuitos de combustible y para prevenir daños en el equipamiento de los quemadores [18].

Incluye secuencias como: Permisos de arranque, barrido de gases, habilitación de encendido, encendido de piloto, encendido de quemador, supervisión de llama, regulación, bloqueos de combustible, entre otros [19].

CAPÍTULO V
INSTRUMENTACIÓN ELECTRÓNICA EN SISTEMAS DE SEGURIDAD

Como se ha visto en el Capítulo anterior, los estándares IEC 61508 e IEC 61511 exponen los conceptos referentes a la seguridad de procesos industriales. En este Capítulo se continúa con la evaluación de estas dos normas pero a nivel de los instrumentos que componen los sistemas de seguridad.

5.1 Modos de fallo

Cada componente de un Sistema Instrumentado de Seguridad (SIS) constituye una plataforma de protección expectante a cualquier evento peligroso que puede sufrir cualquiera de estos 2 fallos:

Modo de Fallo seguro.- El sistema activa la protección del proceso sin que exista la necesidad o demanda.

Modo de Fallo peligroso (o no seguro).- El sistema es incapaz de procesar la protección del proceso ante una verdadera demanda o necesidad de protección.

Es imposible evitar la posibilidad que un equipo falle pero si se puede reducir la probabilidad que suceda.

Los fallos peligrosos son los que se deben controlar y mantener lo más bajo posible. De aquí obtenemos el concepto de **"Probabilidad de Fallo ante una demanda"** o **PFD**, el cual es un valor numérico que nos indica la tasa de fallos peligrosos que presenta el equipo. Es esta PFD la característica que realmente se exige limitar a los SIS. Cuanto mayor sea el riesgo, mas bajo será el valor de Probabilidad de fallo ante una demanda (PFD) requerido [15].

5.2 Nivel de Integridad Segura (SIL)

Según los estándares IEC 61508 e IEC 61511, el **Nivel de Integridad Segura (SIL)** relaciona la Probabilidad de Fallo ante la Demanda (PFD) de un SIS con la reducción del riesgo que este ofrece al proceso.

En la Tabla 5.1 se presentan los niveles SIL para **operaciones en demanda**, es decir que su funcionamiento solo se da cuando sucede un fallo en el proceso o en el BPCS.

TABLA Nº 5.1 Niveles SIL para modo de operación en demanda

Modo de Operación en demanda		
Nivel SIL	PFDavg	Factor de Reducción de Riesgo (RRF)
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

En la Tabla 5.2 se presentan los niveles SIL para **operaciones continuas**, es decir que su funcionamiento es continuo y que de existir una fallo en la función de seguridad de todas maneras se presentará un peligro potencial.

TABLA Nº 5.2 Niveles SIL para modo de operación continuo

Modo de Operación Continuo	
Nivel SIL	Probabilidad de fallo peligroso por hora (PFH)
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 $< 10^{-5}$

El Nivel SIL nos exige utilizar instrumentación de alto rendimiento para garantizar que las funciones instrumentadas de seguridad (SIF) sean ejecutadas satisfactoriamente bajo las condiciones establecidas (integridad segura). SIL 4 tiene el mayor nivel de integridad segura mientras que SIL 1 presenta el menor nivel de integridad segura [15].

La relación entre el Factor de Reducción de Riesgo (RRF) y la Probabilidad Media de Fallo ante la Demanda (PFDavg) está dada por la fórmula 5.1:

$$RRF=1/PFDavg \tag{5.1}$$

En la Figura 5.1 observamos un ejemplo numérico que muestra que a mayor reducción de riesgo requerido para determinado proceso, mayor será el nivel SIL de nuestro SIS a utilizar.

En el Anexo B se presentan algunos métodos para obtener el nivel SIL que los procesos peligrosos exigen al SIS a implementar.

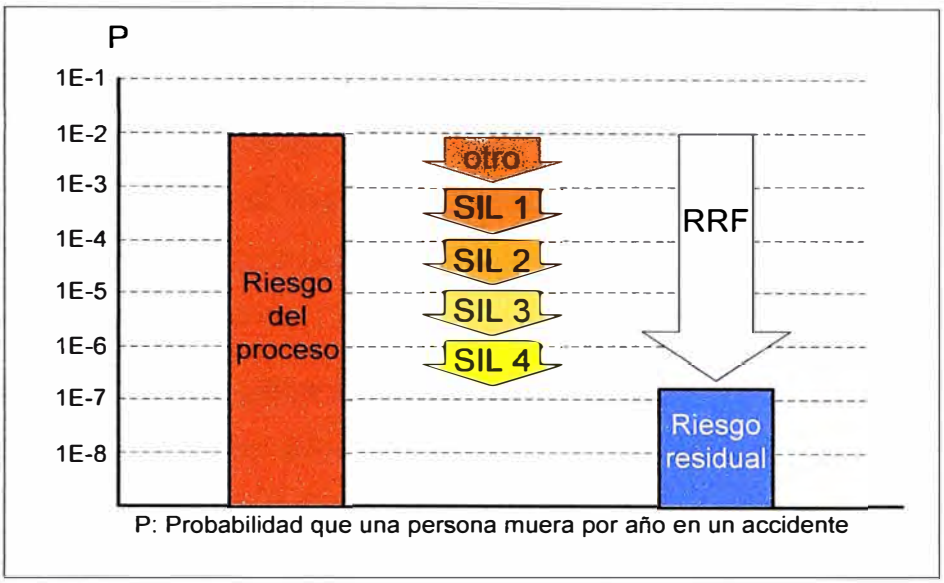


Fig. 5.1 Variación del SIL respecto al RRF

Las Funciones Instrumentadas de Seguridad (SIF) específicas que se ejecutan en los Sistemas Instrumentados de Seguridad (SIS), tienen la Probabilidad de Fallo ante la Demanda, y por consiguiente el nivel SIL, dado por la suma de las probabilidades de fallo de cada sub sistema.

Tomando como base las Tablas 5.1 y 5.2 tenemos que para el caso de operaciones en demanda, la PFD está dada por la fórmula 5.2 [15]:

$$PFD_{SYS} = PFD_S + PFD_L + PFD_{FE} \quad (5.2)$$

Donde,

PFD_{SYS} es la probabilidad de fallo ante la demanda de la función de seguridad específica.

PFD_S es la probabilidad de fallo ante la demanda del sub sistema de sensores.

PFD_L es la probabilidad de fallo ante la demanda del sub sistema de lógica.

PFD_{FE} es la probabilidad de fallo ante la demanda del sub sistema de elementos finales.

Y para las operaciones continuas, la PFD está dada por la fórmula 5.3 (15):

$$PFH_{SYS} = PFH_S + PFH_L + PFH_{FE} \quad (5.3)$$

Donde,

PFH_{SYS} es la probabilidad de fallo peligroso por hora de la función de seguridad específica.

PFH_S es la probabilidad de fallo peligroso por hora del sub sistema de sensores.

PFH_L es la probabilidad de fallo peligroso por hora del sub sistema de lógica.

PFH_{FE} es la probabilidad de fallo peligroso por hora del sub sistema de elementos finales.

5.3 Arquitecturas de sistemas de seguridad

La norma IEC 61508 expone diferentes arquitecturas de los sub sistemas de una función de seguridad con el objetivo de mejorar el desempeño de éstos y así de diferentes maneras puedan aportar una mayor reducción de riesgo (y un mayor nivel SIL) al sistema de seguridad según sea conveniente [15].

5.3.1 Arquitectura 1oo1 (1 sobre 1)

Arquitectura simple de un solo canal donde cualquier fallo no seguro del dispositivo puede provocar un fallo en la función de seguridad ante la demanda. Su esquema se muestra en la Figura 5.2.

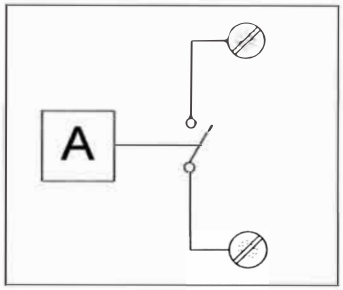


Fig. 5.2 Esquema de arquitectura 1oo1

5.3.2 Arquitectura 1oo2 (1 sobre 2)

En esta arquitectura de 2 canales conectados en paralelo cualquier canal (1 sobre 2) puede ejecutar la función de seguridad. Debe haber un fallo no seguro en los dos dispositivos para que la función de seguridad falle ante la demanda, pero la probabilidad de fallo seguro es mayor. Su esquema se muestra en la Figura 5.3.

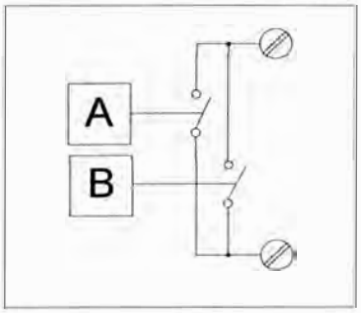


Fig. 5.3 Esquema de arquitectura 1oo2

5.3.3 Arquitectura 2oo2 (2 sobre 2)

Esta arquitectura consiste en 2 canales conectados en serie donde ambos dispositivos (2 sobre 2) deben aportar en conjunto para ejecutar la función de seguridad. Si existe un fallo

no seguro en cualquier canal, la función de seguridad puede fallar ante la demanda. Su esquema se muestra en la Figura 5.4.

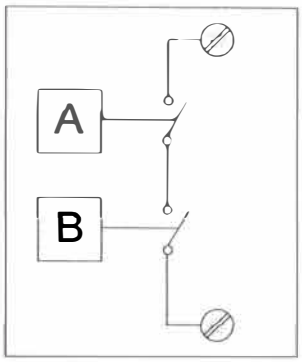


Fig. 5.4 Esquema de arquitectura 2oo2

5.3.4 Arquitectura 2oo3 (2 sobre 3)

Esta arquitectura consiste de 3 canales conectados en paralelo en donde la mayoría (2 sobre 3) deben aportar en conjunto para que se ejecute la función de seguridad. Debe haber un fallo no seguro en 2 canales para que falle la función de seguridad ante la demanda. Su esquema se muestra en la Figura 5.5.

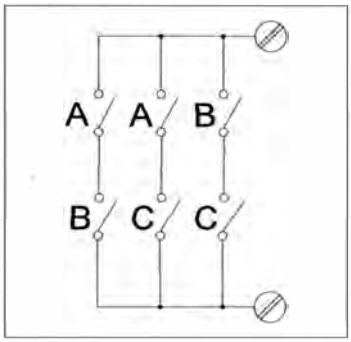


Fig. 5.5 Esquema de arquitectura 2oo3

5.4 Resumen de la probabilidad de fallos de cada arquitectura

Muchas veces el valor de la PFD o PFH de los instrumentos de seguridad son otorgados por el fabricante en un certificado correspondiente. Pero otras veces, la arquitectura que utilizó el fabricante o entidad certificadora para sus pruebas no corresponde con la que se desea implementar en un nuevo SIS. Es por eso que en las tablas que se muestran a continuación se encuentran las ecuaciones que los Ingenieros diseñadores deberán aplicar a cada uno de sus instrumentos que formarán parte del SIS. La Tabla 5.3 contiene la descripción de los términos que se utilizan en las ecuaciones de la Tabla 5.4 de arquitecturas para operaciones en demanda y Tabla 5.5 de arquitecturas para operaciones continuas [15].

En el Anexo D se presentan los certificados de nivel SIL de los instrumentos mencionados en el Capítulo 6 de este informe.

TABLA Nº 5.3 Términos y unidades empleados en el cálculo de la probabilidad de fallos

Abreviatura	Término	Unidades
T_I	Intervalo de prueba	h
MTTR	Tiempo medio hasta el restablecimiento	h
DC	Cobertura del diagnóstico del dispositivo	%
β	Fracción de fallos no detectados que tienen causa común	%
β_D	Fracción de fallos detectados que tienen causa común	%
λ	Tasa de fallos por hora de un canal en un sub sistema	h^{-1}
PFD_G	Probabilidad media de fallo en demanda del sub sistema	
PFD_{SYS}	Probabilidad media de fallo en demanda de la función de seguridad específica	
PFH_G	Probabilidad media de fallo por hora del sub sistema	
PFH_{SYS}	Probabilidad media de fallo por hora de la función de seguridad específica	
λ_D	Tasa de fallos peligrosos por hora de un canal en un sub sistema. Equivalente al 50% de λ. $\lambda_D = \lambda_{DU} + \lambda_{DD}$	h^{-1}
λ_S	Tasa de fallos seguros por hora de un canal en un sub sistema. Equivalente al 50% de λ. $\lambda_S = \lambda_{SU} + \lambda_{SD}$	h^{-1}
λ_{DD}	Tasa de fallos peligrosos detectados por hora de un canal en un sub sistema. $\lambda_{DD} = \frac{\lambda}{2} DC$	h^{-1}
λ_{DU}	Tasa de fallos peligrosos no detectados por hora de un canal en un sub sistema. $\lambda_{DU} = \frac{\lambda}{2}(1 - DC)$	h^{-1}
λ_{SD}	Tasa de fallos seguros detectados por hora de un canal en un sub sistema	h^{-1}
λ_{SU}	Tasa de fallos seguros no detectados por hora de un canal en un sub sistema	h^{-1}
t_{CE}	Tiempo medio de inactividad del equivalente del canal para arquitecturas 1oo1, 1oo2, 2oo2, 2oo3 $t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$	h^{-1}
t_{GE}	Tiempo medio de inactividad del grupo de votación para arquitecturas 2oo2, 2oo3 $t_{GE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{3} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$	h^{-1}

En el Anexo C se muestra el cálculo de β y β_D para el cálculo de la PFD y PFH.

TABLA N° 5.4 PFD de arquitecturas para modo de operación en demanda

Arquitectura	Probabilidad de Fallo en Demanda
1oo1	$PFD_G=(\lambda_{DU}+\lambda_{DD})t_{CE}$
1oo2	$PFD_G=2[(1-\beta_D)\lambda_{DD}+(1-\beta)\lambda_{DU}]^2 t_{CE}t_{GE}+\beta_D\lambda_{DD}MTTR+\beta\lambda_{DU}\left(\frac{T_1}{2}+MTTR\right)$
2oo2	$PFD_G=2(\lambda_{DU}+\lambda_{DD})t_{CE}$
2oo3	$PFD_G=6[(1-\beta_D)\lambda_{DD}+(1-\beta)\lambda_{DU}]^2 t_{CE}t_{GE}+\beta_D\lambda_{DD}MTTR+\beta\lambda_{DU}\left(\frac{T_1}{2}+MTTR\right)$

TABLA N° 5.5 PFH de arquitecturas para modo de operación continuo

Arquitectura	Probabilidad de Fallo Peligroso por hora
1oo1	$PFH_G=\lambda_{DU}$
1oo2	$PFH_G=2[(1-\beta_D)\lambda_{DD}+(1-\beta)\lambda_{DU}]^2 t_{CE}+\beta_D\lambda_{DD}+\beta\lambda_{DU}$
2oo2	$PFH_G=2\lambda_{DU}$
2oo3	$PFH_G=6[(1-\beta_D)\lambda_{DD}+(1-\beta)\lambda_{DU}]^2 t_{CE}+\beta_D\lambda_{DD}+\beta\lambda_{DU}$

5.5 Ejemplo de aplicación de PFD

Consideremos la Función Instrumentada de Seguridad (SIF) mostrada en la Figura 5.6:

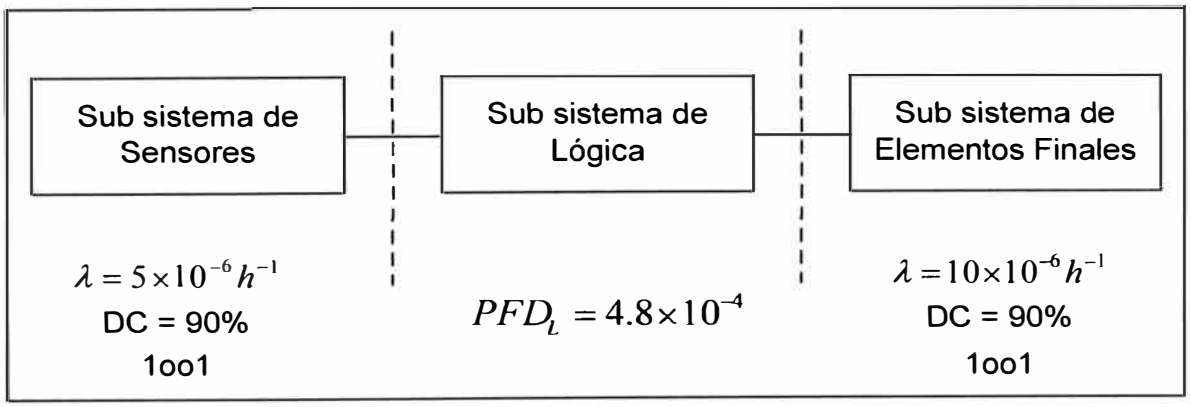


Fig. 5.6 Ejemplo de arquitectura para modo de operación en demanda

Entonces para un periodo de prueba T_1 = 1 año y un MTTR = 8 horas se obtiene:

$PFD_S = 1.1 \times 10^{-3}$

$PFD_{FE} = 2.2 \times 10^{-3}$

y del dato:

$PFD_L = 4.8 \times 10^{-4}$

se obtiene la PFD de la SIF según la fórmula 5.2 y el nivel SIL según la Tabla 5.1:

$PFD_{SYS} = 1.1 \times 10^{-3} + 4.8 \times 10^{-4} + 2.2 \times 10^{-3}$

$\mathbf{= 3.78 \times 10^{-3}}$

= SIL 2

Si la función de seguridad requiere de un nivel SIL 3 es necesario mejorar la PFD de los subsistemas de sensores y de elementos finales. Para ello se emplea alguna arquitectura vista en la sección 5.3.

a) Para los sensores se emplea 2oo3 (asumiendo β =10% y β_D=5%), así

$PFD_S = 1.2 \times 10^{-4}$

b) Para los elementos finales se emplea 1oo2 (asumiendo β =10% y β_D=5%), así

$PFD_{FE} = 2.3 \times 10^{-4}$

Entonces:

$PFD_{SYS} = 1.2 \times 10^{-4} + 4.8 \times 10^{-4} + 2.3 \times 10^{-4}$

$\mathbf{= 8.3 \times 10^{-4}}$

= SIL 3

5.6 Características funcionales de los instrumentos de seguridad

5.6.1 Tolerancia a fallos del hardware (HFT)

En el contexto de integridad segura referida al hardware, el mayor nivel SIL que puede alcanzar una función de seguridad está dado por la tolerancia a fallos del hardware (HFT) y la fracción de fallos seguros (SFF) del subsistema [15]. Las Tablas 5.6 y 5.7 especifican esta relación para subsistemas **tipo A** y **tipo B.**

Un subsistema es **tipo A** si:

a) Los modos de fallo de todos sus componentes están bien definidos; y

b) El desempeño del subsistema bajo condiciones de fallo puede ser completamente determinado.

Un subsistema es **tipo B** si:

a) El modo de fallo de por lo menos uno de sus componentes no está bien definidos; y

b) El desempeño del subsistema bajo condiciones de fallo no puede ser completamente determinado.

TABLA Nº 5.6 Nivel SIL de acuerdo a la HFT y SFF para subsistemas tipo A

Fracción de fallos seguros (SFF)	**Tolerancia a fallos del hardware (HFT)**		
	0	**1**	**2**
< 60 %	SIL 1	SIL 2	SIL 3
60 % - < 90 %	SIL 2	SIL 3	SIL 4
90 % - < 99 %	SIL 3	SIL 4	SIL 4
>= 99 %	SIL 3	SIL 4	SIL 4

TABLA Nº 5.7 Nivel SIL de acuerdo a la HFT y SFF para subsistemas tipo B

Fracción de fallos seguros (SFF)	**Tolerancia a fallos del hardware (HFT)**		
	0	**1**	**2**
< 60 %	No permitido	SIL 1	SIL 2
60 % - < 90 %	SIL 1	SIL 2	SIL 3
90 % - < 99 %	SIL 2	SIL 3	SIL 4
>= 99 %	SIL 3	SIL 4	SIL 4

Una tolerancia a fallos del hardware de N significa que N+1 fallos pueden causar la pérdida de la función de seguridad [15].

La fracción de fallos seguros de un subsistema está definida según la fórmula 5.4 (los términos se encuentran expresados en la Tabla 5.3):

$$SFF = \frac{\lambda_S + \lambda_{DD}}{\lambda} \tag{5.4}$$

5.6.2 Técnicas para la detección de fallos

La Tabla 5.8 que se presenta a continuación muestra algunas técnicas recomendadas por la norma IEC 61508 para la detección y control de los fallos que se puedan dar en los instrumentos [15]. La información presentada es solo referencial y una explicación detallada de cada técnica escapa al objetivo del presente trabajo.

Cada técnica ofrece cierta cobertura a los test de identificación de fallos, expresión denominada Cobertura del Diagnóstico (DC).

TABLA Nº 5.8 Técnicas para la detección y control de fallos

Subsistema	**Técnica de diagnóstico**	**Máximo DC que se puede alcanzar**
Electrónico	Majority voter	99%
	Tests by redundant hardware	90%
	Monitored redundancy	99%
	Hardware with automatic check	99%
Unidades de procesamiento	Self-test by software: walking bit (one-channel)	90%
	Self-test supported by hardware (one-channel)	99%
	Reciprocal comparison by software	99%
Memorias ROM	Word-saving multi-bit redundancy	90%
	Signature of a double word (16-bit)	99%
	Block replication	99%
Memorias RAM	RAM test "walk-path"	90%
	RAM test "galpat" or transparent galpat	99%
	RAM test "Abraham"	99%
Ruta de datos (comunicación interna)	Complete hardware redundancy	99%
	Transmission redundancy	99%
	Information redundancy	99%
Reloj	Watch-dog with separate time base and time-window	99%
	Temporal and logical monitoring	99%

(Nota: Se ha considerado conveniente colocar el nombre de las técnicas de la lista en el mismo idioma que aparecen en la norma, pues algunas de ellas no tienen traducción al español)

CAPÍTULO VI
INSTRUMENTACIÓN ELECTRÓNICA DE SEGURIDAD EN UNA REFINERÍA DE PETRÓLEO

Este Capítulo sugiere, de manera práctica, la aplicación de la instrumentación electrónica descrita en los capítulos anteriores, en una instalación de un Sistema Instrumentado de Seguridad aplicado a los procesos que se dan en la primera etapa de la refinación del petróleo.

6.1 Situación inicial del Sistema de Control

La etapa de Destilación del crudo de una Refinería presenta 4 grupos de procesos bien definidos: Monitoreo del Horno, Líneas de combustible, Vapor de barrido y Ahogamiento y Gases Incondensables.

Consideremos que estos procesos se encuentran operando en la Refinería y que son gobernados por un Sistema de Control Distribuido (DCS) y lo que se desea implementar es un Sistema Instrumentado de Seguridad (SIS) y un Sistema de Administración de Quemadores (BMS). Asimismo, se adicionará un circuito de gas natural al encendido de los quemadores usado como combustible.

A continuación la descripción de la instrumentación perteneciente al DCS instalada en cada proceso junto con sus Diagramas de Instrumentación P&ID. Solo se presenta un horno, pues son los mismos procesos para ambos.

6.1.1 Monitoreo del Horno

En este grupo se monitorea y controla las variables involucradas en el funcionamiento del horno y la temperatura de salida del crudo calentado que irá a la columna de destilación para su fraccionamiento.

a) Se controla el caudal de crudo de entrada a zona convectiva (FT-101, FCV-101).

b) Se monitorea la presión y temperatura de entrada de crudo a zona convectiva (PT-143, TT-259).

c) Se monitorea la presión y temperatura de salida de crudo de zona convectiva (PT-144, TT-36).

d) Se monitorea la temperatura de entrada de crudo a zona radiante (TT-279).

e) Se monitorea la presión y temperatura de salida de crudo de zona radiante (PT-145, TT280, TT-281, TT-1).

f) Se monitorea la temperatura de crudo en el serpentín dentro de la zona radiante (TT-260, TT-261, TT-262, TT-263).

g) Se controla la presión de tiro del horno a través de un dámper en la chimenea (PCZ-105).

La Figura 6.1 muestra el P&ID de las variables del Monitoreo del Horno que van al DCS.

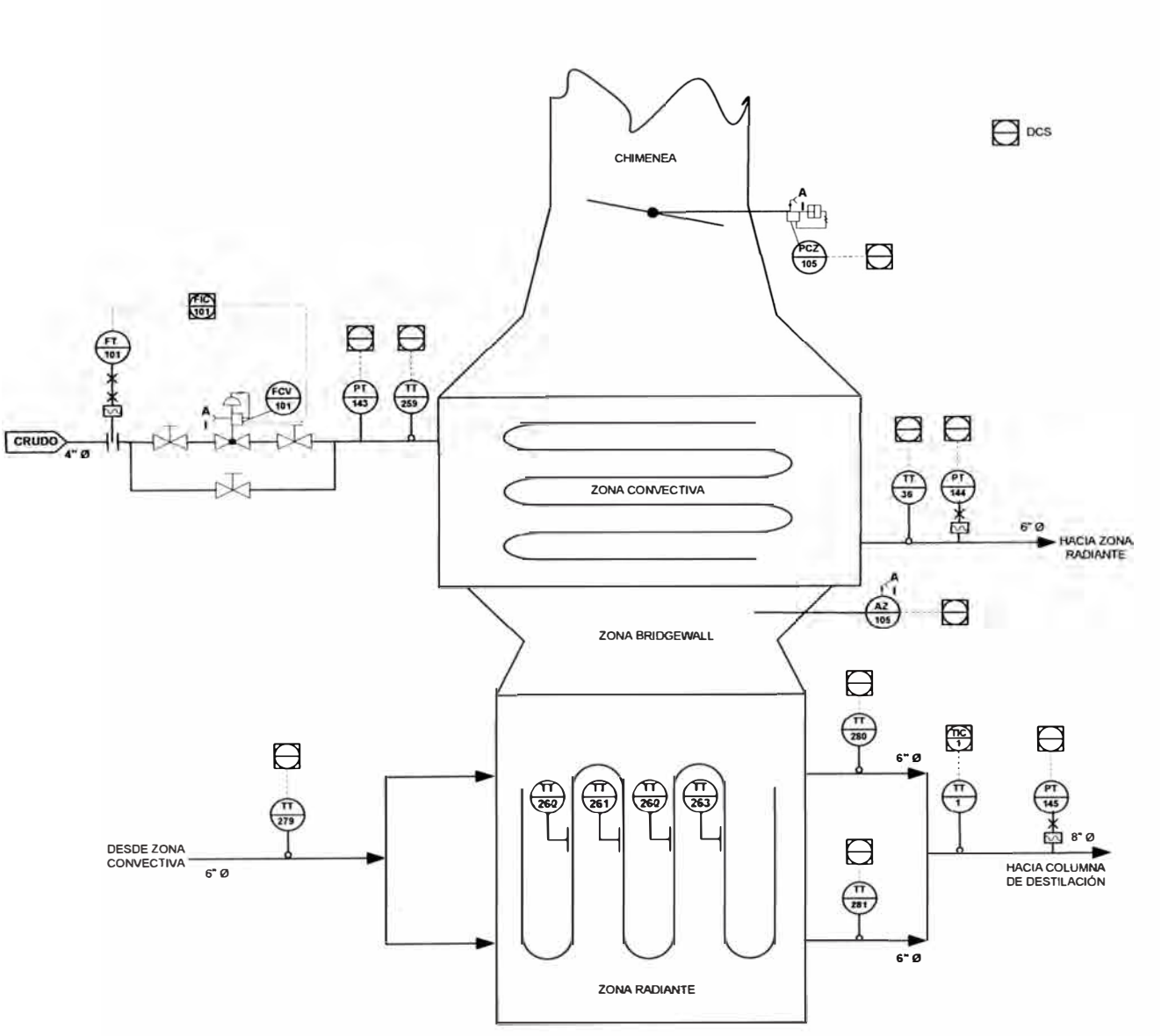


Fig. 6.1 P&ID de Control de Monitoreo de Horno

6.1.2 Líneas de combustible

Para el encendido de los 4 quemadores que posee cada horno, se considera un circuito de residual y otro de vapor de atomización.

El quemador se enciende manualmente y el combustible que quema es residual atomizado (mezclado con vapor).

La Figura 6.2 muestra el esquema del Sistema de Control de Combustión del Horno.

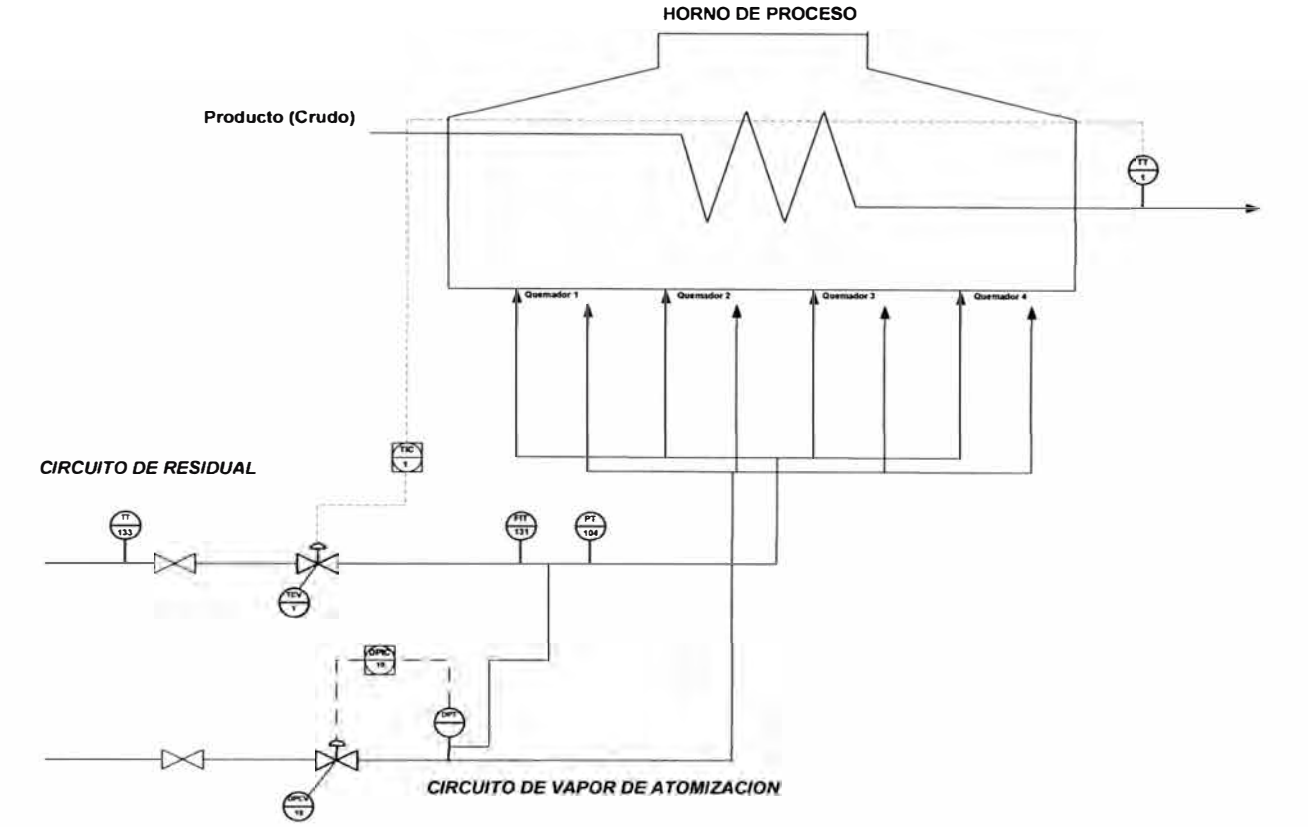


Fig. 6.2 Esquema del Sistema de Control de Combustión del Horno

a) Se controla la temperatura de salida del crudo del horno a través de una válvula de control de flujo de combustible (TCV-1).

b) Se monitorea el caudal de combustible (residual) que consumen los quemadores (FT-131).

c) Se monitorea la presión de la troncal del combustible (residual) antes de ingresar a los quemadores (PT-104).

d) Se controla la presión de retorno de residual a través de una válvula de control (PT-108, PCV-108).

e) Se controla la presión diferencial que debe existir entre vapor saturado y residual a través de una válvula de control de presión (PT-109, DPCV-10).

f) El ingreso de residual y de vapor a los quemadores se realiza de forma manual a través de válvulas compuerta.

La Figura 6.3 muestra el P&ID del Circuito de combustible residual y Circuito de vapor de atomización.

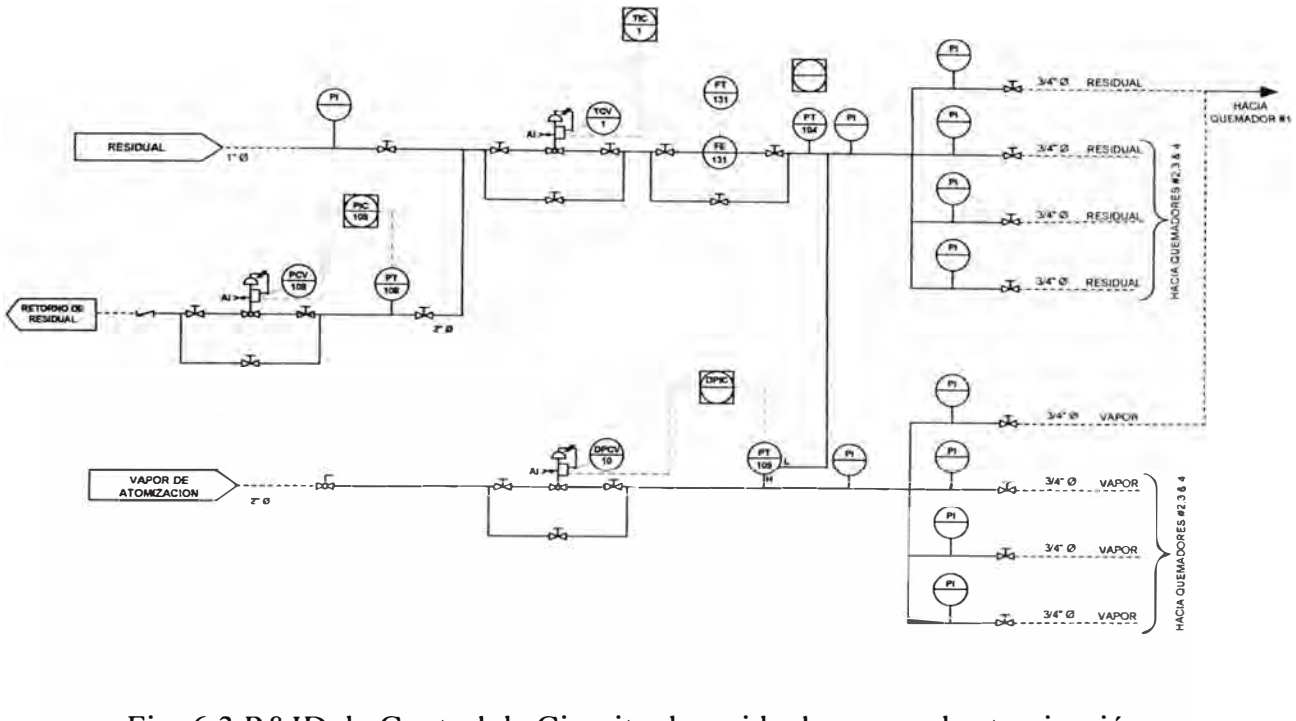


Fig. 6.3 P&ID de Control de Circuito de residual y vapor de atomización.

6.1.3 Circuitos de Vapor de barrido y ahogamiento

Antes de encender el horno, es necesario realizar una limpieza de gases residuales que puedan existir en el interior del mismo, para ello se utiliza vapor saturado. Asimismo, cuando se detecte una situación anómala en el interior del horno, se utiliza vapor saturado para ahogar las llamas de los quemadores y apagarlas inmediatamente.

Inicialmente estos circuitos presentan válvulas de operación manual.

6.1.4 Circuito de gases incondensables

Los gases incondensables que se generan en el proceso de refinación del petróleo, son quemados en uno de los hornos.

a) Se monitorea el caudal de gases incondensables que se queman en el horno (FT-19).

b) El ingreso de gases incondensables a los quemadores se realiza de forma manual a través de válvulas compuerta.

La Figura 6.4 muestra el P&ID del circuito de gases incondensables.

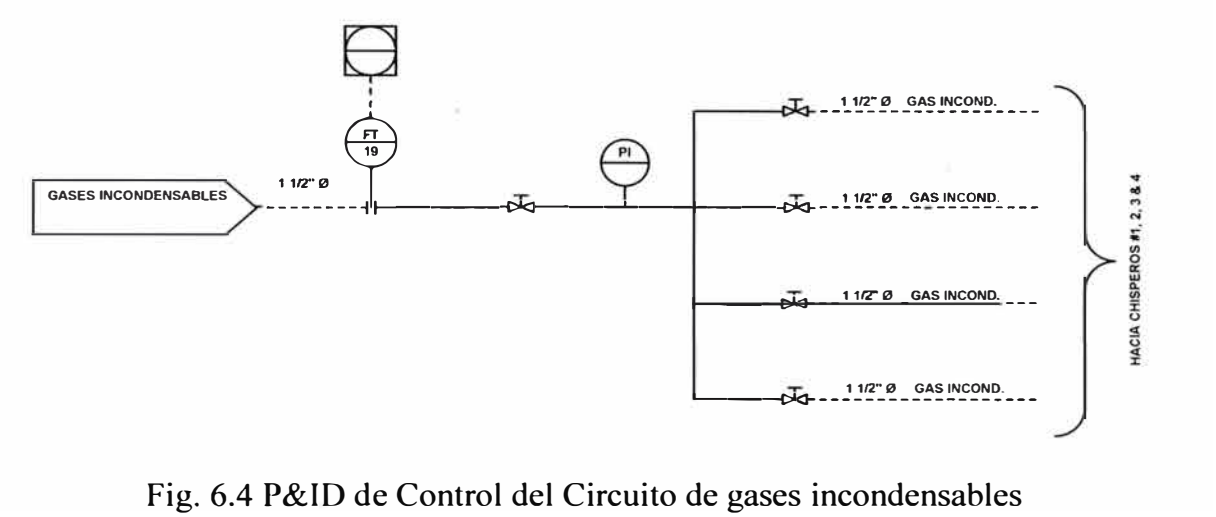


Fig. 6.4 P&ID de Control del Circuito de gases incondensables

6.2 Resultados de la Evaluación del Sistema

A continuación el resumen de los resultados de la evaluación del Sistema Instrumentado de Seguridad (SIS) a implementar y los requisitos necesarios a cumplir.

a) Las Funciones Instrumentadas de Seguridad (SIF) correspondientes al SIS deben cumplir con SIL 3.

b) El Controlador Resolvedor de Lógica debe ser de procesador triple redundante.

c) Los transmisores de variables de campo deben estar en disposición 2oo3. Ver referencia en la Figura 6.5.

d) Las válvulas de corte automático deben estar en disposición 1oo2. Ver referencia en la Figura 6.5.

e) Las solenoides pertenecientes a las válvulas de corte automático deben estar en disposición 1oo1. Ver referencia en la Figura 6.5.

f) La confirmación de apertura / cierre de válvulas de corte automático y manual deben estar en disposición 1oo1. Ver referencia en la Figura 6.5.

g) Las válvulas de control existentes deberán tener confirmación de apertura / cierre que ingresen al controlador de seguridad.

h) Sensores y Elementos finales de control correspondientes a secuencias de arranque y operación del BMS deben cumplir con SIL 1.

i) Total independencia entre el SIS y el DCS.

j) Cada dispositivo de campo deberá tener su propio cableado dedicado. No está permitido el uso de buses de comunicación.

k) Todas las variables que intervienen en una SIF serán medidas por transmisores inteligentes 4 – 20 mA con protocolo HART.

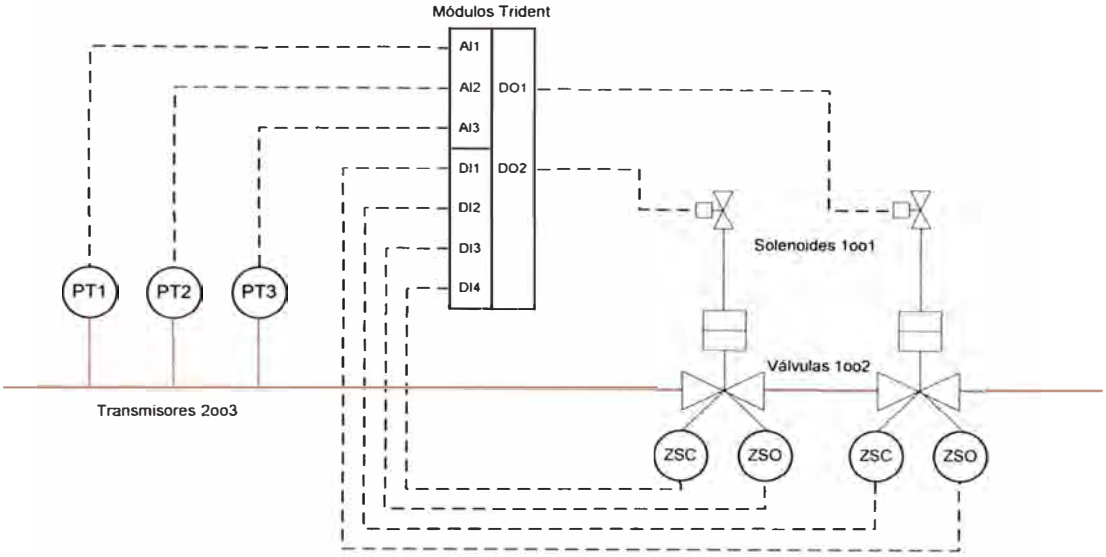


Fig. 6.5 Lazos SIL – Arquitectura típica

6.3 Diagramas del montaje final

A continuación la descripción de la instrumentación de seguridad instalada en cada proceso involucrado en la destilación del crudo junto con sus Diagramas de Instrumentación P&ID. De color rojo aparecen los instrumentos con características de seguridad pertenecientes al SIS y BMS.

6.3.1 Monitoreo del horno

a) Se cambia el posicionador de la válvula de control FCV-101 por uno de nivel SIL2 y los límites de carrera son llevados al sistema de seguridad.

b) Se añade un transmisor de flujo de seguridad con nivel SIL 2 en la entrada de crudo a zona convectiva (FT-9101).

c) Se añaden transmisores de temperatura de seguridad con nivel SIL 2 en disposición 2oo3 a la salida de crudo de zona radiante (TT-9001A, TT-9001B, TT-9001C).

d) Se añade un posicionador con nivel SIL 2 al actuador del dámper (PCZ-105) en la chimenea y los límites de carrera son llevados al sistema de seguridad.

e) Se añaden transmisores de presión de vacío con nivel SIL 2 para medir el tiro en la base del horno, zona bridgewall y chimenea (PT-9401, PT-9402, PT-9403, PT-9404).

f) Se añaden transmisores de temperatura con nivel SIL 2 para medir la temperatura en la

base del horno, zona bridgewall y chimenea (TT-9408, TT-9409, TT-9410).

La Figura 6.6 muestra el P&ID del Sistema de Control y Seguridad del Monitoreo del Horno.

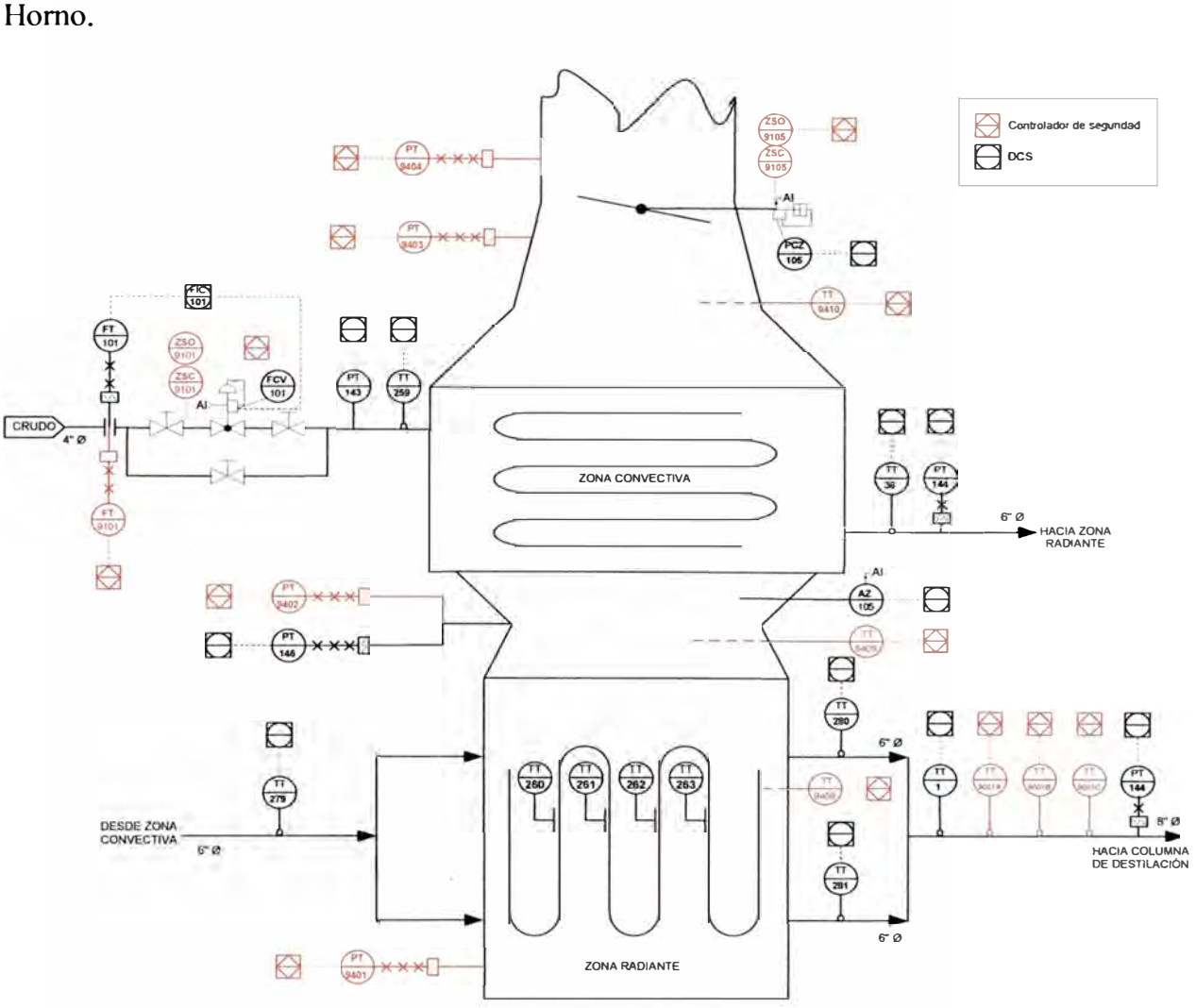


Fig. 6.6 P&ID del Sistema de Control y Seguridad del Monitoreo del Horno

6.3.2 Líneas de combustible

a) Se automatizan los ingresos de combustible a los quemadores de los hornos.

b) Se agregan detectores de llama IR/UV a las lanzas de los quemadores para detectar si están encendidas (BIT).

La Figura 6.7 muestra el esquema del Sistema de Control y Seguridad del Monitoreo del Horno

Circuito de Residual

a) Se cambia el posicionador de la válvula de control TCV-1 por uno de nivel SIL 2 y los límites de carrera son llevados al sistema de seguridad.

b) Se añaden transmisores de presión de seguridad con nivel SIL 2 en disposición 2oo3 en

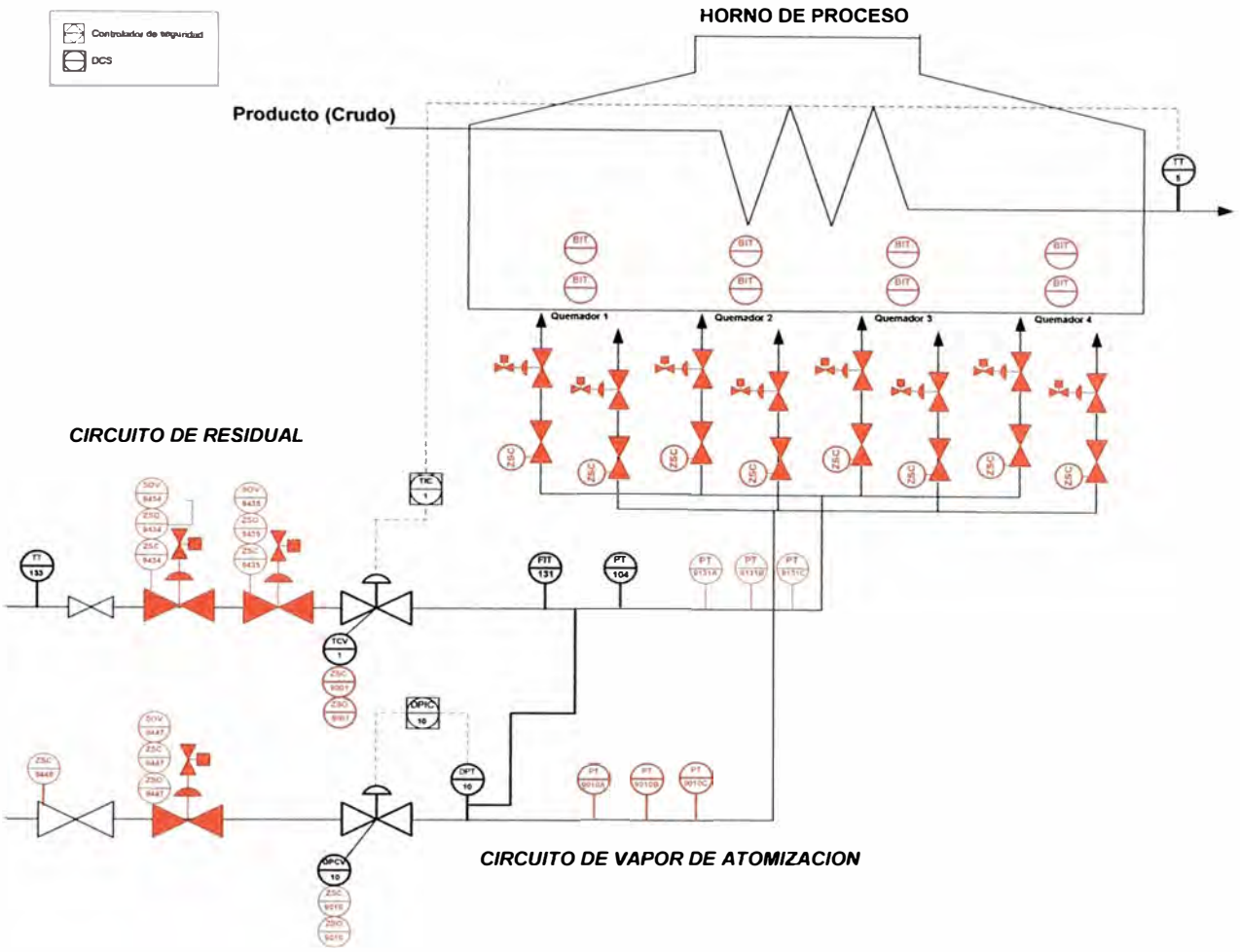


Fig. 6.7 Esquema de Sistema de Control y Seguridad de Combustión del Horno

la línea troncal (PT-9131A, PT-9131B, PT-9131C).

c) Se añaden válvulas automáticas de seguridad en la línea troncal en disposición 1oo2 accionadas mediante válvulas solenoides con nivel SIL 3 (SOV-9434, SOV-9435).

d) Se cambia el posicionador de la válvula de control PCV-108 por uno de nivel SIL 2 y los límites de carrera son llevados al sistema de seguridad.

e) Se añaden válvulas automáticas de seguridad en los ingresos de cada quemador accionadas mediante válvulas solenoides con nivel SIL 3 (SOV-9440, SOV-9441, SOV-9442, SOV-9443).

f) Se cambian las válvulas compuerta en los ingresos de cada quemador por válvulas esféricas manuales con límites de carrera que van al sistema de seguridad (ZSC-9436, ZSC-9437, ZSC-9438, ZSC-9439).

La Figura 6.8 muestra el P&ID del Sistema de Control y Seguridad de los Circuitos de residual y vapor de atomización.

Circuito de Vapor de atomización

a) Se cambia el posicionador de la válvula de control DPCV-10 por uno de nivel SIL 2 y los límites de carrera son llevados al sistema de seguridad.

b) Se añaden transmisores de presión de seguridad con nivel SIL 2 en disposición 2oo3 en la línea troncal (PT-9410A, PT-9410B, PT-9410C).

c) Se añade una válvula automática de seguridad en la línea troncal accionadas mediante válvula solenoide con nivel SIL 3 (SOV 9447).

d) Se añaden válvulas automáticas de seguridad en los ingresos de cada quemador accionadas mediante válvulas solenoides con nivel SIL 3 (SOV-9440, SOV-9441, SOV-9442, SOV-9443).

e) Se cambian las válvulas compuerta en los ingresos de cada quemador por válvulas esféricas manuales con límites de carrera que van al sistema de seguridad (ZSC-9448, ZSC-9449, ZSC-9450, ZSC-9451).

La Figura 6.8 muestra el P&ID del Sistema de Control y Seguridad de los Circuito de residual y vapor de atomización.

Circuito de Gas Combustible

a) Se considera el posicionador de la válvula de control TCV-150 de nivel SIL 2 y los límites de carrera son llevados al sistema de seguridad.

b) Se consideran transmisores de presión de seguridad con nivel SIL 2 en disposición 2oo3 en la línea troncal antes del ingreso a quemadores (PT-9150A, PT-9150B, PT-9150C).

c) Se considera una válvula automáticas de seguridad en la línea de venteo accionada mediante válvula solenoide con nivel SIL 3 (SOV-9413).

d) Se considera un transmisor de presión de seguridad con nivel SIL 2 en la línea troncal (PT-9150D).

e) Se consideran válvulas automáticas de seguridad en los ingresos de cada quemador accionadas mediante válvulas solenoides con nivel SIL 3 (SOV-9419, SOV-9420, SOV-9421, SOV-9422).

f) Se consideran válvulas esféricas manuales con límites de carrera que van al sistema de seguridad (ZSC-9415, ZSC-9416, ZSC-9417, ZSC-9417).

La Figura 6.9 muestra el P&ID del Sistema de Control y Seguridad del Circuito de gas combustible).

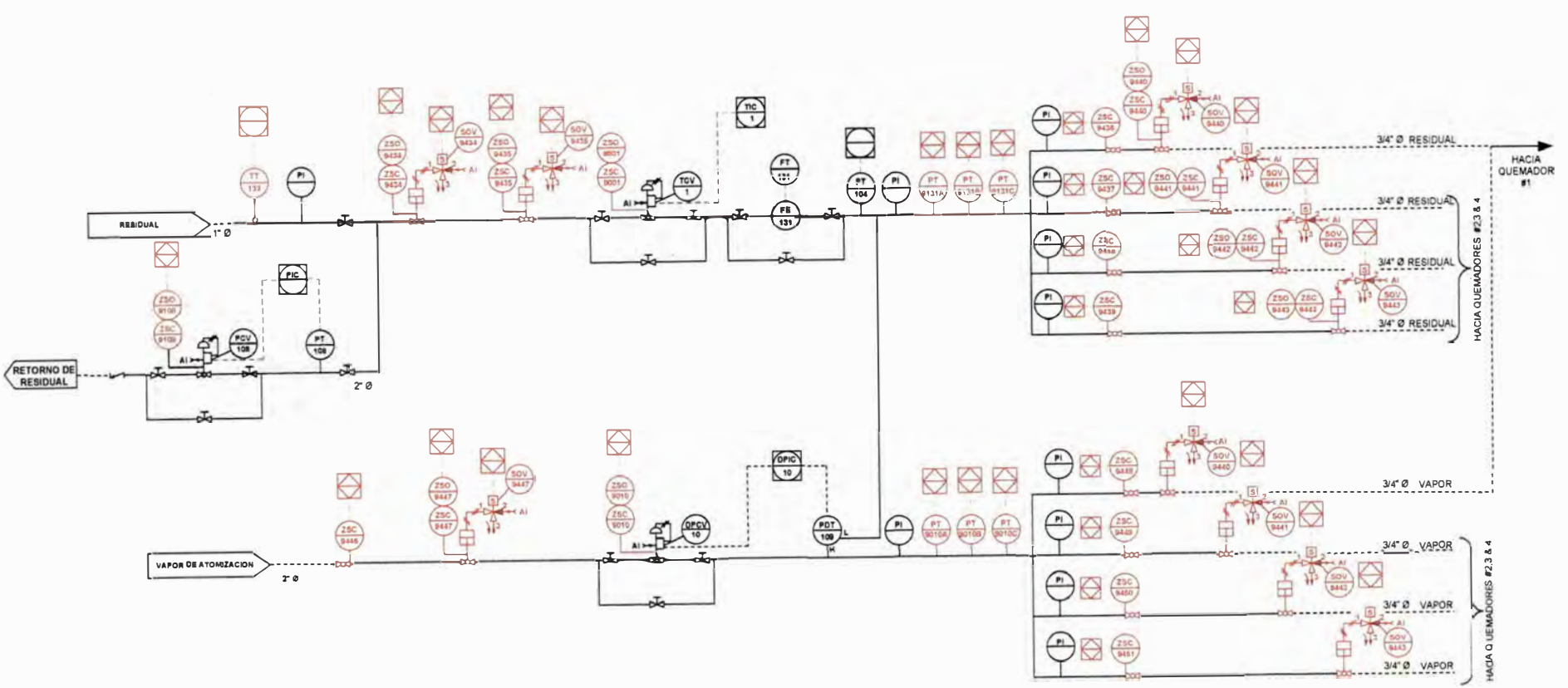


Fig. 6.8 P&ID del Sistema de Control y Seguridad del Circuito de residual y vapor de atomización

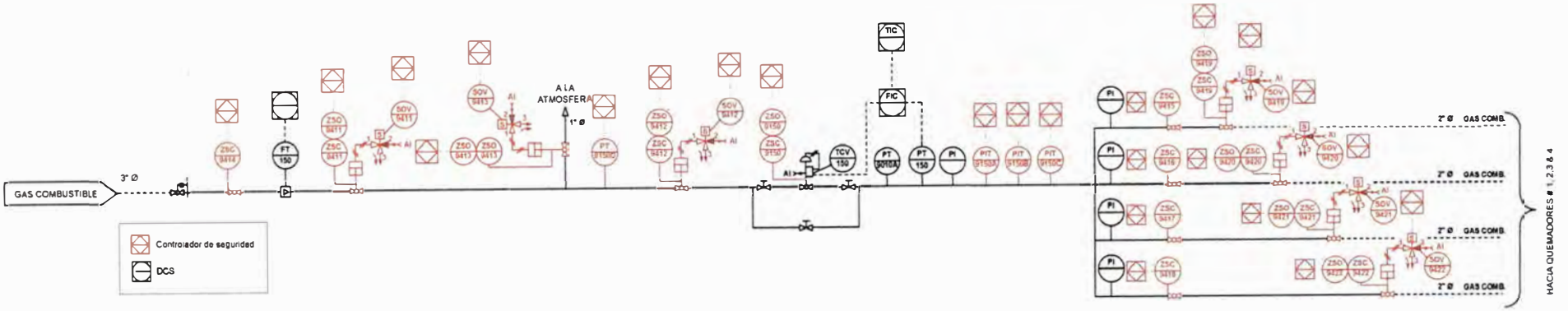


Fig. 6.9 P&ID del Sistema de Control y Seguridad del Circuito de gas combustible

6.3.3 Circuito de Gas Piloto

a) Se consideran válvulas automáticas de seguridad en la línea troncal accionadas mediante válvulas solenoides con nivel SIL 3 (SOV-9423, SOV-9424).
b) Se considera una válvula automáticas de seguridad en la línea de venteo accionada mediante válvula solenoide con nivel SIL 3 (SOV-9425)

c) Se considera un transmisor de presión de seguridad con nivel SIL 2 en la línea troncal (PT-9405).

d) Se consideran válvulas solenoides de seguridad en los ingresos de cada quemador (SOV-9430, SOV-9431, SOV-9432, SOV-9433).

e) Se consideran válvulas esféricas manuales con límites de carrera que van al sistema de seguridad (ZSC-9426, ZSC-9427, ZSC-9428, ZSC-9429).

La Figura 6.10 muestra el P&ID del Sistema de Control y Seguridad del Circuito de gas piloto.

6.3.4 Circuitos de Vapor de barrido y ahogamiento

a) Se añade un transmisor de presión de seguridad con nivel SIL 2 a cada circuito (PT-9407, PT-9406).

b) Se añaden válvulas automáticas de seguridad en disposición 1oo2 accionadas mediante válvulas solenoides con nivel SIL 3 (SOV-9470, SOV-9471, SOV-9467, SOV-9468).

c) Se cambian las válvulas compuerta por válvulas esféricas manuales con límites de carrera que van al sistema de seguridad (ZSC-9469, ZSC-9466).

La Figura 6.11 muestra el P&ID del Sistema de Control y Seguridad del Circuito de vapor de barrido y ahogamiento.

6.3.5 Circuito de gases incondensables

a) Se añaden transmisores de presión de seguridad con nivel SIL 2 en disposición 2oo3 en la línea troncal (PT-9154A, PT-9154B, PT-9154C).

b) Se añaden válvulas automáticas de seguridad en la línea troncal en disposición 1oo2 accionadas mediante válvulas solenoides con nivel SIL 3 (SOV-9456, SOV-9457).

c) Se añaden válvulas automáticas de seguridad en los ingresos de cada quemador accionadas mediante válvulas solenoides con nivel SIL 3 (SOV-9462, SOV-9463, SOV-

9464, SOV-9465).

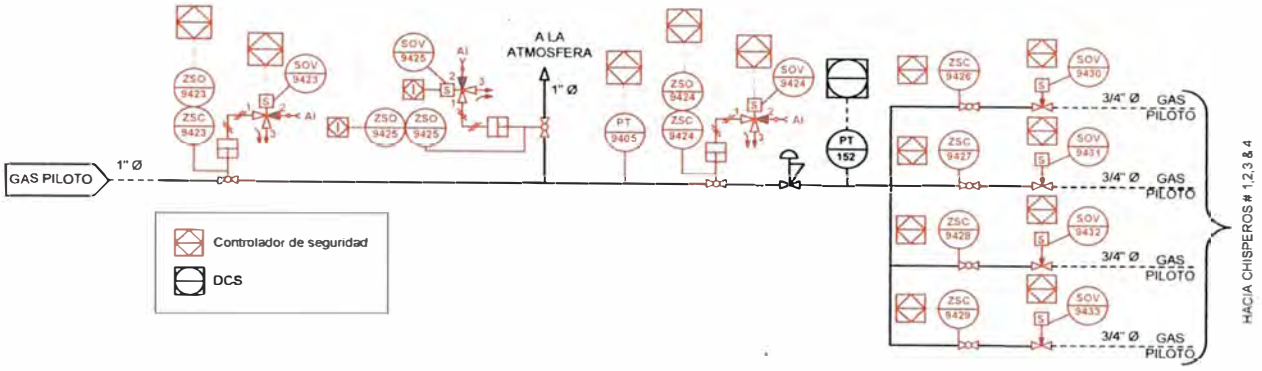


Fig. 6.10 P&ID del Sistema de Control y Seguridad del Circuito de gas piloto

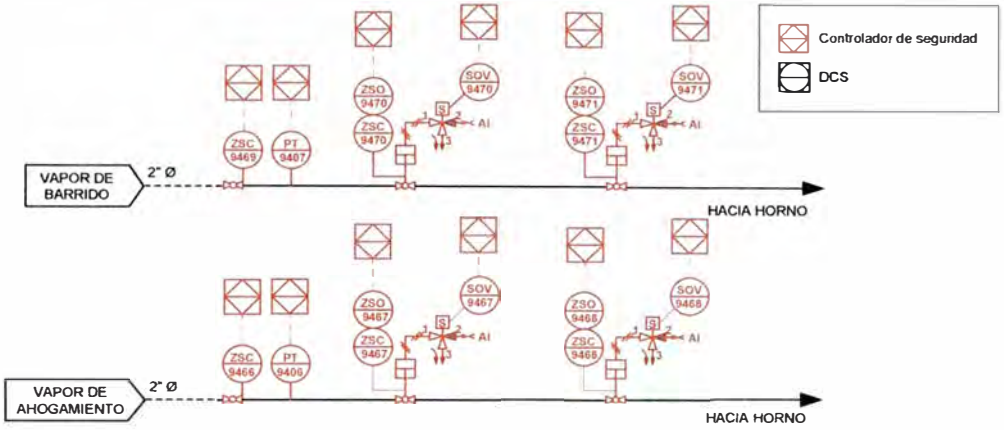


Fig. 6.11 P&ID del Sistema de Control y Seguridad de los Circuitos de vapor de barrido y ahogamiento

d) Se cambian las válvulas compuerta en los ingresos de cada quemador por válvulas esféricas manuales con límites de carrera que van al sistema de seguridad (ZSC-9458, ZSC-9459, ZSC-9460, ZSC-9461).

La Figura 6.12 muestra el P&ID del Sistema de Control y Seguridad del Circuito de vapor de gases incondensables.

6.4 Especificaciones de la instrumentación de seguridad utilizada

A continuación las especificaciones técnicas de los instrumentos mencionados en la implementación de un SIS y que aparecen en los diagramas P&ID de la sección 6.3.

6.4.1 Transmisores de presión manométrica y de vacío

a) Transmisor de presión manométrica Marca Foxboro, Modelo IGP10-T.

b) Transmisor de presión de vacío Marca Foxboro, Modelo IGP20-T.

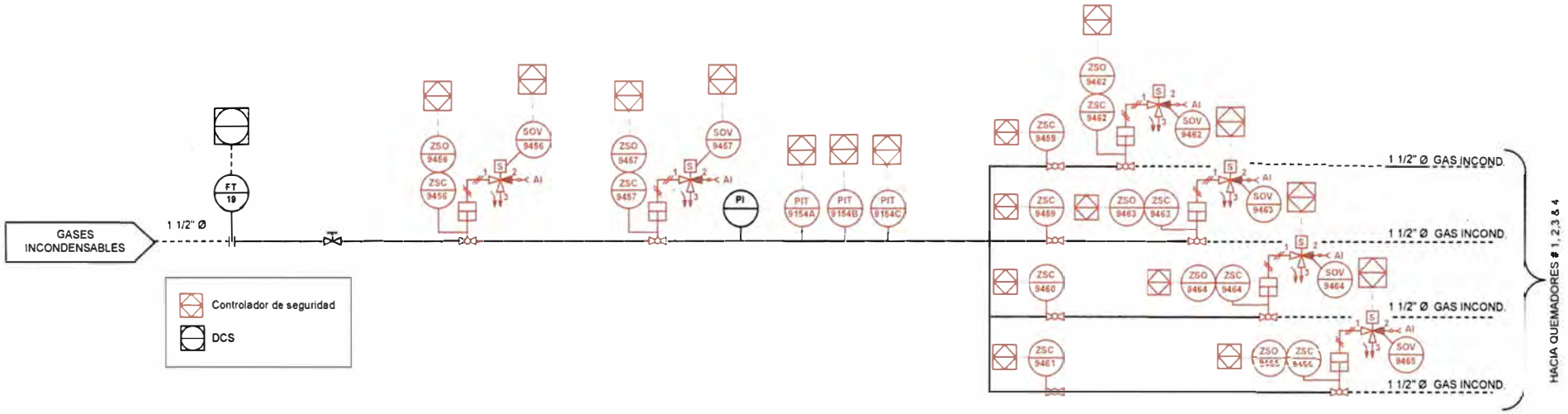


Fig. 6.12 P&ID del Sistema de Control y Seguridad del Circuito de gases incondensables

c) Transmisión analógica 4 - 20 mA y Digital HART.

d) Precisión +/- 0.06 % del span.

e) Diafragma de acero inoxidable 316.

f) Cumple con requerimientos de Compatibilidad Electromagnética de Directiva Europea EMC conforme a estándares IEC EN 50081-2, EN 50082-2 e IEC 61000-4-2 a 61000-4-6.

g) Diseñado a prueba de explosión para operar en atmósferas explosivas según aprobación FM.

h) Certificado de calibración.

i) Certificado de conformidad.

j) Certificado de SIL 2. Ver Anexo D.

6.4.2 Transmisores de temperatura

a) Transmisor de temperatura Marca Foxboro, Modelo RTT15-T

b) Precisión +/- 0.05 % del span.

c) Con termocupla tipo J para las líneas de proceso y tipo K para monitoreo de horno.

d) Valor de salida configurable entre 3.5 mA o 23 mA para la detección de circuito abierto del sensor.

e) Rutina de auto calibración y auto diagnóstico automática.

f) Inmunidad EMC según Directiva EU 89/336/EEC.

g) Diseñado a prueba de explosión para operar en atmósferas explosivas según aprobación FM.

h) Certificado de calibración.

i) Certificado de conformidad.

j) Certificado de SIL 2. Ver Anexo D.

6.4.3 Controlador triple redundante

a) Módulo del procesador triple redundante modelo Trident 3101.

b) Sistema de votación de la lógica 2oo3 (2 sobre 3).

c) Cada módulo de entrada y salida cuenta con triple circuito electrónico (llamados

canales) que procesan en paralelo y de manera independiente la data.

d) Inmunidad EMC según Directiva EU 89/336/EEC.

e) Aprobado para trabajar en sistemas de seguridad ESD, BMS, SIS.

f) Sistema de alarma con indicación local para: fallo en alimentación, problemas con la aplicación o integridad del sistema, alarmas especificadas por el usuario.

g) Certificado de SIL 3. Ver Anexo D.

6.4.4 Válvulas automáticas

a) Válvula esférica de paso total Marca Spirax Sarco, Modelo M33F.

b) Válvula con diseño a prueba de fuego (fire safe) según norma API 607.

c) Válvula con cuerpo de acero al carbono y esfera hueca de acero inoxidable.

d) Actuador neumático Marca Spirax Sarco, Modelo BVA300.

e) Actuador de cuarto de vuelta de simple efecto.

f) Presión de trabajo del actuador de 60 psi.

g) Actuador con certificado de hermeticidad según API 598.

h) Solenoide de aire de 3 vías marca Asco, Modelo 8320

i) Solenoide con bobina de 24 Vdc.

j) Certificado de SIL 3 para las solenoides. Ver Anexo D.

6.4.5 Posicionadores eléctricos

a) Posicionador inteligente Marca Foxboro, Modelo SRD960-BH.

b) Con función de auto diagnóstico y auto calibración.

c) Inmunidad EMC según Directiva EU 89/336/EEC.

d) Diseñado a prueba de explosión para operar en atmósferas explosivas según aprobación FM.

e) Certificado de SIL 3. Ver Anexo D.

CONCLUSIONES Y RECOMENDACIONES

1. Los procesos industriales poseen peligros que no deben dejar de ser tomados en cuenta, debido a que pueden ocasionar accidentes lamentables.
2. Los sistemas de control operados por DCS o PLC aseguran la continuidad operativa de la planta, pero no ayudan mucho a reducir los riesgos de los procesos.
3. Los niveles de riesgo de los procesos peligrosos son disminuidos considerablemente con la implementación de un Sistema Instrumentado de Seguridad (SIS).
4. Los instrumentos que forman parte de un SIS deben cumplir con características especiales normadas por el IEC en sus estándares IEC 61508 e IEC 61511.
5. Una de las características más importantes de un instrumento de seguridad es la PFD (probabilidad de fallo ante una demanda). De acuerdo a este valor se puede determinar en cuanto puede disminuir el riesgo de un determinado proceso.
6. Los procesos de una refinería de petróleo poseen altos niveles de riesgo que resulta necesario considerar un SIS con nivel SIL 3.
7. Es necesario identificar el nivel de riesgo de cada proceso para luego obtener el nivel SIL de cada función de seguridad que corresponde implementar.
8. Los conceptos de seguridad deben ser comprendidos en su totalidad para poder diseñar adecuadamente un SIS. Los fabricantes de instrumentos proporcionan certificados asociados a los instrumentos, en los cuales se tiene valores numéricos correspondientes a los parámetros de seguridad, que sirven para realizar los cálculos respectivos.
9. Es necesario que las autoridades locales competentes consideren estos estándares y que exijan su implementación en la industria de procesos.

ANEXO A
ESTRUCTURA DE LOS ESTÁNDARES IEC 61508 E IEC 61511

A.1 Estructura del Estándar IEC 61508

Nombre del estándar:

"Seguridad Funcional de los sistemas de seguridad eléctricos / electrónicos / electrónicos programables"

(*Functional safety of electrical/electronic/programmable electronic safety-related systems*)

Partes:

Parte 1: Requerimientos generales (*General requirements*)

Parte 2: Requerimientos para sistemas de seguridad eléctricos / electrónicos / electrónicos programables (*Requirements for electrical / electronic / programmable electronic safety-related systems*).

Parte 3: Requerimientos de software (*Software requirements*).

Parte 4: Definiciones y abreviaturas (*Definitions and abbreviations*).

Parte 5: Ejemplos de métodos para determinar el nivel de integridad segura (*Examples of methods for the determination of safety integrity levels*).

Parte 6: Guía para la aplicación de las partes 2 y 3 (*Guidelines on the application of parts 2 and 3*).

Parte 7: Resumen de técnicas y mediciones (*Overview of techniques and measures*).

A.2 Estructura del Estándar IEC-61511

Nombre del estándar:

"Seguridad Funcional - Sistemas instrumentados de seguridad para la industria de procesos"

(*Functional safety — Safety instrumented systems for the process industry sector*)

Partes:

Parte 1: Marco, definiciones, sistema, requerimientos de hardware y software (*Framework, definitions, system, hardware and software requirements).*

Parte 2: Guía para la aplicación de IEC 61511-1 (*Guidelines for the application of IEC 61511-1*).

Parte 3: Guía para la determinación del nivel de integridad segura requerido (*Guidance for*

the determination of the required safety integrity levels).

ANEXO B
MÉTODOS PARA EL CÁLCULO DEL NIVEL SIL DE LAS FUNCIONES INSTRUMENTADAS DE SEGURIDAD

Un paso importante para la implementación de un Sistema Instrumentado de Seguridad es determinar el Nivel de Integridad Segura (SIL) que requieren las diversas Funciones Instrumentadas de Seguridad (SIF), para ello existen diversos métodos desarrollados que permiten un eficiente cálculo del mismo. Entre algunos de ellos tenemos:

1. Método cuantitativo
2. Método semi-cuantitativo
3. Método Matriz de Riesgos
4. Método cualitativo de Gráfico de Riesgos
5. Método semi-cualitativo de Gráfico de Riesgos Calibrado.
6. Análisis de Capas de Protección

El uso de uno u otro método está regido, entre otros factores, por:

a) La complejidad de la aplicación.
b) Los lineamientos de las autoridades reguladoras.
c) La naturaleza del riesgo.
d) La experiencia y habilidades del personal involucrado en el desarrollo del trabajo.
e) La información disponible sobre los parámetros del riesgo.

Dos de los métodos más comunes y sencillos de aplicar son: Método cuantitativo y Método cualitativo de Gráfico de Riesgos.

B.1 Método cuantitativo

El modelo para ilustrar el principio general se muestra en la Fig. 4.3. Los pasos a seguir son los siguientes y se necesitan realizar para cada función de seguridad a ser implementada:

a) Determinar el riesgo tolerable en una Tabla similar a la Tabla 4.1 (F_t).
b) Determinar el riesgo del proceso (Fnp).
c) Determinar la reducción de riesgo necesario (PFD) para conseguir el riesgo tolerable de acuerdo a la fórmula B.1:

$$PFD_{avg} < F_t / F_{np} \qquad (B.1)$$

d) Obtener el nivel SIL de la Tabla 5.1.

Ejemplo:

Sea una función instrumentada de seguridad a implementar cualquiera:

a) Riesgo tolerable del proceso equivalente a un 10% de probabilidad que falle una vez en el tiempo de vida de la planta de 10 años. Esto es equivalente a un fallo en 100 años, o una vez en 8.8×10^5 horas. Entonces, $F_t = 1 / 8.8 \times 10^5 = 1.1 \times 10^{-6}$

b) Un análisis del proceso indica que éste puede fallar una vez en un año, es decir, el riesgo del proceso es uno en 8.8×10^3 horas. Entonces, $F_{np} = 1/ 8.8 \times 10^3 = 1.1 \times 10^{-4}$

c) La reducción de riesgo necesaria que debe ofrecer el SIS a implementar estará dado de acuerdo a la fórmula B.1 por:

$$PFD_{avg} \leq F_t / F_{np}$$
$$\leq 1.1 \times 10^{-6} / 1.1 \times 10^{-4}$$
$$\leq 10^{-2}$$

d) La SIF requiere por lo menos un nivel **SIL 2**.

B.2 Método Cualitativo de Gráfico de Riesgos

Este método está basado en la ecuación del riesgo: R = f x C;

Donde:

R es el riesgo sin el sistema de seguridad;

f es la frecuencia del evento peligros sin el sistema de seguridad;

C es la consecuencia del evento peligroso.

La frecuencia f, en este caso estará influenciada por 3 factores:

a) frecuencia y tiempo de exposición en la zona peligrosa;

b) la posibilidad de evitar el evento peligroso;

c) la probabilidad de que el evento peligroso tenga lugar sin la adición de un sistema de seguridad – llamada la probabilidad de ocurrencia no deseada.

Esto produce los siguientes 4 parámetros relacionados al riesgo:

a) Consecuencia del evento peligroso (C);

b) Frecuencia y tiempo de exposición en la zona peligrosa (F);

c) Posibilidad de evitar el evento peligros (P);

d) Probabilidad de la ocurrencia no deseada W).

La combinación de los parámetros de riesgo establece un gráfico de riesgo como el mostrado en la Figura C.1. Parámetros con mayor sub índice indican mayor riesgo ($C_A < C_B < C_C < C_D$; $F_A < F_B < F_C$; $P_1 < P_2$; $W_1 < W_2 < W_3$). El nivel SIL de la función SIF es obtenida luego de recorrer el camino adecuado de la Figura B.1 según exija el proceso.

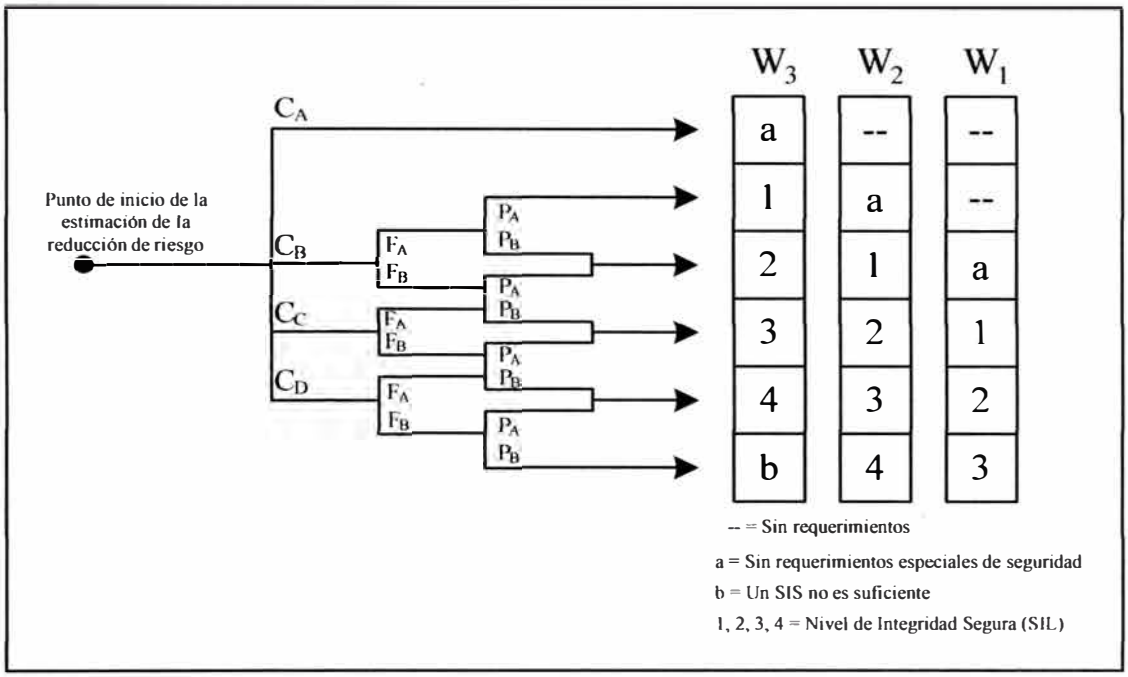


Fig. B.1 Esquema general del Gráfico de Riesgos

Los parámetros indicados en la Figura B.1 y sus pesos deben ser definidos para cada situación específica dentro de la planta.

Ejemplo:

Sea una función instrumentada de seguridad a implementar cualquiera. El gráfico de riesgos se muestra en la Figura B.2.

Los parámetros de riesgos identificados son:

a) C_B = Consecuencia de daños permanentes serios a una o más personas. Muerte de una persona

b) F_B = Elevada frecuencia de permanecer en la zona de riesgo

c) P_B = Probabilidad casi imposible de evitar el evento peligroso.

d) W_2 = Probabilidad media que el evento no deseado ocurra.

La SIF requiere por lo menos un nivel **SIL2.**

La lista completa de parámetros se observan en la Tabla B.1.

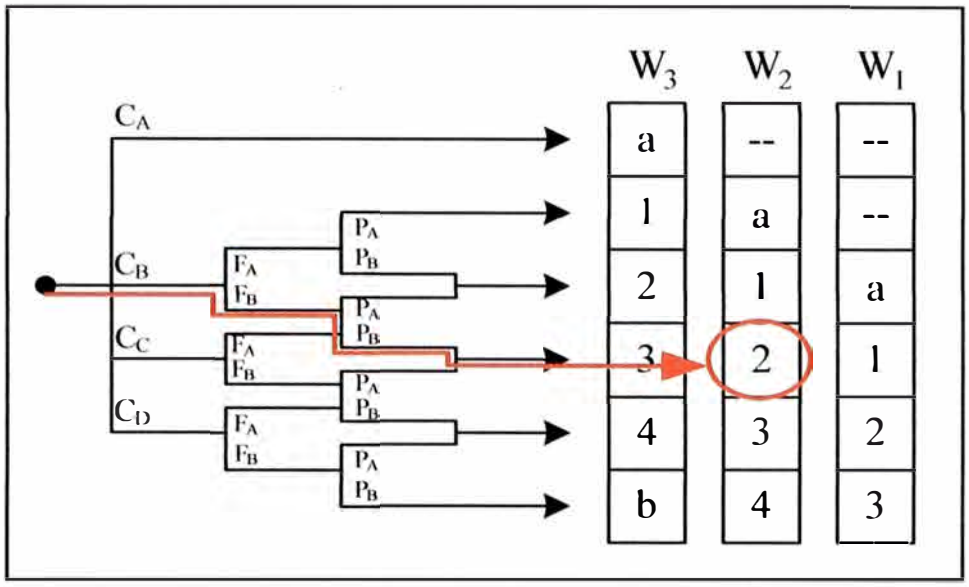


Fig. B.2 Identificación de Nivel SIL según el Gráfico de Riesgos

TABLA N° B.1 Ejemplo de Parámetro del riesgo

Parámetro del riesgo		**Clasificación**
Consecuencia (C)	C_A	Daño menor
	C_B	Daños permanentes serios a una o más personas. Muerte de una persona
	C_C	Muerte de varias personas
	C_D	Muchas personas muertas
Frecuencia y tiempo de exposición en la zona peligrosa (F)	F_A	Rara de permanecer expuesto
	F_B	Elevada de permanecer expuesto
Posibilidad de evitar el evento peligroso (P)	P_A	Posible bajo ciertas condiciones
	P_B	Casi imposible
Probabilidad de ocurrencia del evento no deseado (W)	W_1	Baja probabilidad de ocurrencia
	W_2	Media probabilidad de ocurrencia
	W_3	Alta probabilidad de ocurrencia

ANEXO C
CÁLCULO DE β Y β_D PARA EL CÁLCULO DE LA PFD Y PFH

Existen los fallos de algún componente que resultan en el fallo del canal del sistema que forman parte, pero existe una probabilidad, mucho menor, que estos fallos independientes ocurran en todos los canales de un sistema multicanal (1oo2, 2oo2, 2oo3, etc.). Esta probabilidad es calculada utilizando técnicas bien establecidas.

El factor β debe ser calculado de manera separada para subsistemas de sensores, de lógica y de elementos finales.

a) **β** es el factor de fallos comunes no detectados por los test de diagnóstico.

b) $\boldsymbol{\beta_D}$ es el factor de fallos comunes detectados por los test de diagnóstico.

Según la Tabla C.1,

β es obtenido utilizando el puntaje $S = X + Y$

β_D es obtenido utilizando el puntaje $S_D = X(Z+1) + Y$

TABLA Nº C.1 Valor de β o β_D

Puntaje S ó S_D	Valor de β o β_D para:	
	Subsistema de lógica	Subsistema de sensores o elementos finales
más de 120	0.50%	1%
70 a 120	1%	2%
45 a 70	2%	5%
menos de 45	5%	10%

Los valores de X y Y se obtienen de la Tabla C.2. El usuario debe evaluar que medidas aplican al sistema en evaluación y sumar los valores correspondientes de cada columna de X_{LS} y Y_{LS} para el subsistema de lógica, o X_{SF} y Y_{SF} para los sensores o elementos finales para finalmente obtener como suma los valores de X y Y respectivamente.

El valor de Z se obtiene de las Tablas C.3 y C.4. y está basado en la frecuencia y la cobertura del test de diagnóstico.

TABLA Nº C.2 Valor de X y Y para subsistemas de lógica, sensores y elementos finales

Ítem	Subsistema de lógica		Subsistema de sensores y elementos finales	
	X_{LS}	Y_{LS}	X_{SF}	Y_{SF}
Separación / Segregación				
¿Todos los cables de señal de los canales han sido enviados de forma separada?	1.5	1.5	1	2
¿Los canales del subsistema de lógica están en circuitos impresos separados?	3	1		
¿Los canales del subsistema de lógica están en gabinetes o tableros separados?	2.5	0.5		
Si los sensores / elementos finales tienen electrónica de control dedicada, ¿la electrónica para cada canal está en circuitos impresos separados?			2.5	1.5
Si los sensores / elementos finales tienen electrónica de control dedicada, ¿la electrónica de cada canal está en interiores y en gabinetes o tableros separados?			2.5	0.5
Nota: La Tabla completa lista 8 grupos con 39 ítems de mediciones a evaluar en el sistema. La Tabla completa se encuentra en el Anexo D de la norma IEC 61508-6				

TABLA Nº C.3 Valor de Z para subsistemas de lógica

Cobertura del diagnóstico	Intervalo del test de diagnóstico		
	Menor a 1 min	Entre 1 a 5 min	Mayor a 5 min.
≥ 99%	2	1	0
≥ 90%	1.5	0.5	0
≥ 60%	1	0	0

TABLA Nº C.4 Valor de Z para subsistemas de sensores y elementos finales

Cobertura del diagnóstico	Intervalo del test de diagnóstico			
	Menor a 2 h	Entre 2 h a 48 h	Entre 48 h y 1 semana	Mayor a 1 semana
≥ 99%	2	1.5	1	0
≥ 90%	1.5	1	0.5	0
≥ 60%	1	0.5	0	0

ANEXO D
CERTIFICADOS DE NIVEL SIL DE LOS INSTRUMENTOS

D.1 Certificado de los transmisores de presión Foxboro IGP10-T, IGP20-T

TÜVRheinland®

ZERTIFIKAT
CERTIFICATE

Nr./No. 968/EZ 308.01/09

Prüfgegenstand **Product tested**	I/A Single Range Hart Pressure Transmitter	**Zertifikats-Inhaber** **Holder of the certificate**	Invensys Systems, Inc. 33 Commercial Street Foxboro, MA 02035-2099 United States of America
Typbezeichnung **Type designation**	I/A Single Range Hart Pressure Transmitter IAP10-T IDP10-T IGP10-T IAP20-T IGP20-T	**Verwendungs-zweck** **Intended application**	The I/A Single Range Hart Transmitter is intended to be part of safety related control systems, where the safe state is to fail the analogue output (4/20 mA) high or low (per customer configuration.
Prüfgrundlagen **Codes and standards forming the basis of testing**	IEC 61508 1998-2000		
Prüfungsergebnis **Test results**	The I/A Single Range Hart Transmitter is suitable for safety related applications up to SIL 2 (IEC 61508).		
Besondere Bedingungen **Specific requirements**	For the use of the I/A Single Range Hart Transmitter the installation instruction (released by Invensys Systems), including recommendations for risk assessment and requirements for maintenance shall be considered.		

TÜVRheinland® Functional Safety Type Approved **FS**

Der Prüfbericht-Nr. 968/EZ 308.01/09 vom 2009-06-05 ist Bestandteil dieses Zertifikates.
Der Inhaber eines für den Prüfgegenstand gültigen Genehmigungs-Ausweises ist berechtigt, die mit dem Prüfgegenstand übereinstimmenden Erzeugnisse mit dem abgebildeten Prüfzeichen zu versehen.

The test report-no. 968/EZ 308.01/09 dated 2009-06-05 is an integral part of this certificate.
The holder of a valid licence certificate for the product tested is authorised to affix the test mark shown opposite to products which are identical with the product tested.

TÜV Rheinland Industrie Service GmbH
Geschäftsfeld ASI
Automation, Software und Informationstechnologie
Am Grauen Stein, 51105 Köln
Postfach 91 09 51, 51101 Köln

H. Gall

2009-06-05

Datum/Date | Firmenstempel/Company stamp | Dipl.-Ing. Heinz Gall

Industrie Service

TUVRheinland
Precisely Right.

LICENCE CERTIFICATE
for TÜV Rheinland Test Mark

No. 968/EZ 308.01/09

Licence Holder:	Invensys Systems, Inc. 33 Commercial Street Foxboro, MA 02035-2099 United States of America		
Manufacturer:	Invensys Systems, Inc. 33 Commercial Street Foxboro, MA 02035-2099 United States of America		
Date of Application:	**File Ref.:**	**Date of Issue:**	
2008-07-09	968/EZ 308.01/09	2009-06-05	
			Annual Fee-Units
Description:	I/A Single Range Hart Pressure Transmitter with defined behaviour under fault conditions		
Product tested:	I/A Single Range Hart Pressure Transmitter		
Type:	Review report-no.: 968/EZ 308.01/09 for complete model code		
Safety Category & Performance Level:	N/A		
Safety Integrity Level:	SIL 2, according to IEC 61508:2000		
Supply voltage.	15.5 - 42 VDC		
Yearly fee:			6

The test sample
- [ ] will be kept by TÜV Rheinland Industrie Service GmbH
- [X] will be kept by the Licence Holder for the disposal of TÜV Rheinland Industrie Service GmbH

Special Remarks: see test report-no.: 968/EZ 308.01/09 dated 2009-06-05 and Certificate No.: 968/EZ 308.01/09 dated 2009-06-05

Test Mark:

TÜVRheinland Functional Safety Type Approved FS

The Licence for the using of the TÜV Rheinland Test Mark is only valid for the licence holder and can only be transferred from TÜV Rheinland Industrie Service GmbH to third persons.

The right for the using of the Test Mark is restricted to such products which are described and are examined by TÜV Rheinland Industrie Service GmbH appropnately

This Licence certificate has to be given back to TÜV Rheinland Industrie Service GmbH if it is being declared as invalid

Furthermore all clauses of the Test Mark Regulations apply

TÜV Rheinland Industrie Service GmbH
Geschäftsfeld ASI
Automation, Software und Informationstechnologie
Am Grauen Stein, 51105 Köln
Postfach 91 08 51, 51101 Köln

2009-06-05
Date

Company stamp

H. Gall
Dipl.-Ing. Heinz Gall

INVENSYS PROCESS SYSTEMS

IPS Functional Safety Data Sheet

Models	**IDP10, IAP10, IAP20, IGP10, IGP20**
Electronics Selection	-T (HART Protocol)
Safety Output	4 to 20 mA
Type of Assessment	IEC 61508: 1998-2000
Assessor	TÜV Rheinland®
Certification	SIL 2
Device Type	B
Hardware Fault Tolerance	0
Safe Failure (SFF)	90.06%
Average Probability of a Dangerous Failure on Demand (PDF_{avg})	$1.6\ 10^{-3}$
Probability of a Dangerous Failure per Hour (PFH)	$1.8\ 10^{-7}$ 1/h
Diagnostic Coverage	$\geq$ 90%
Safety Architecture	1oo1
Proof Test Interval	1 Year
λ	3680 FIT
λ_s	2150 FIT
λ_{dd}	1160 FIT
λ_{du}	366 FIT
Valid Model Selection	-S2 Model Code Option
Valid Firmware Version	5.02

Avantis Foxboro SimSci-Esscor Triconex SCADA

D.2 Certificado de los transmisores de temperatura Foxboro RTT15-T

Invensys Process Systems
33 Commercial Street
Foxboro, MA 02035 USA
T + 1 508 543 8750
F + 1 508 549 6750
www.invensys.com

SIL DECLARATION OF CONFORMITY

We, Manufacturer:

Invensys Systems, Inc.
33 Commercial Street
Foxboro, Massachusetts 02035
U.S.A.

declare under our sole responsibility that the

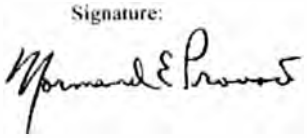
RTT15-T Temperature Transmitter with Thermocouple (1)
RTT15-T Temperature Transmitter with 4-wire RTD (2)

have been assessed to applicable IEC 61508 requirements in support of SIL2 applications and the following parameters:

Product	RTT15-T Temperature Transmitter with Thermocouple (1)	RTT15-T Temperature Transmitter with 4-wire RTD (2)
SIL	2	2
Proof test interval	1 Year	1 Year
Device Type	B	B
HFT	0	0
SFF	92.3%	92.3%
PFD_{avg}	1.86×10^{-3}	8.54×10^{-4}
λdu	425 FIT	195 FIT
λdd	4973 FIT	2203 FIT
λsu	142 FIT	142 FIT
λsd	0 FIT	0 FIT
MTTF	21 Years	45 Years
DCs	0%	0%
DCd	92%	92%

I, the undersigned, hereby declare that the products specified above conform to the listed standard:

Signature:



Name: Normand E. Provost
Title: Manager Product Qualification
Date: May 17, 2006

D.3 Certificado de las válvulas solenoides ASCO 8320

This manufacturer may use this mark

Reports:
ASCO Q08/12-38 R003 FMEDA Report V1 R1
ASCO Q08/12-38 R005 IEC 61508 Assessment Report V1 R1

Validity:
This assessment is valid for the Series 8320 Solenoid Valves

This assessment is valid until May 31, 2012

Revision 1.0 May 2009

exida®
Certification S.A.

Certificate / Certificat
Zertifikat / 合格証

ASCO 08/12-38 C003

exida hereby confirms that the

Series 8320 Solenoid Valves

ASCO Numatics, Florham Park, NJ USA

Have been assessed per the relevant requirements of:

IEC 61508 Parts 1, 2

and meets requirements providing a level of integrity to:

Systematic Integrity: SIL 3 Capable

Random Integrity: Type A Device

PFD_{AVG} and Architecture Constraints must be verified for each application

Safety Function:
The Series 8320 Solenoid Valves will move to the safe position within the specified safety time when the solenoid is placed in its failsafe state (de-energized or energized).

Application Restrictions:
The unit must be properly designed into a Safety Instrumented Function per the Safety Manual requirements.

Product Assessor

Auditor

Page 1 of 2

Certificate / Certificat / Zertifikat / 合格証

ASCO 08/12-38 C003

Systematic Integrity: SIL 3 Capable

Random Integrity: Type A Device

PFD_{AVG} and Architecture Constraints must be verified for each application

SIL 3 Capability

The product has met manufacturer design process requirements of Safety Integrity Level (SIL) 3. These are intended to achieve sufficient integrity against systematic errors of design by the manufacturer.
A Safety Instrumented Function (SIF) designed with this product must not be used at a SIL level higher than stated without "prior use" justification by end user or diverse technology redundancy in the design.

IEC 61508 Failure Rates

For valves used in a final element assembly, SIL must be verified for the specific application using the following failure rate data.

Failure rates for the Series 8320 Solenoid Valves in FIT*

Failure Category	λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF
8320 De-energize on trip	0 FIT	233 FIT	0 FIT	150 FIT	60.8%
8320 Energize on trip	0 FIT	192 FIT	0 FIT	191 FIT	50.2%
8320 De-energize on trip, PVST	0 FIT	233 FIT	148 FIT	2 FIT	99.6%
8320 Energize on trip, PVST	0 FIT	192 FIT	189 FIT	2 FIT	99.6%

Applications

8320, NC	8320, Normally Closed, De-energize on trip
8320, NC	8320, Normally Open, Energize on trip

SIL Verification

The Safety Integrity Level (SIL) of an entire Safety Instrumented Function (SIF) must be verified via a calculation of PFD_{AVG}, considering redundant architectures, proof test interval, proof test effectiveness, any automatic diagnostics, average repair time and the specific failure rates of all products included in the SIF. Each subsystem must be checked to assure compliance with minimum hardware fault tolerance (HFT) requirements.

* FIT = 1 failure / 10^9 hours

exida®
Certification S.A.

Form	Version	Date
C61508	2.03	Mar 2009

D.4 Certificado del controlador Trident 3101

TÜVRheinland®

ZERTIFIKAT
CERTIFICATE

Nr./No. 968/EZ 101.11/09

Prüfgegenstand **Product tested**	Safety Related Programmable Electronic System 2oo3 with diagnostics (2oo3D) and 3-2-1-0 OR 3-2-0 configurable mode of operation	**Zertifikats-inhaber** **Licence holder**	Invensys Systems Inc. - Triconex 15345 Barranca Parkway Irvine, California 92618 United States of America
Typbezeichnung **Type designation**	Trident System	**Hersteller** **Manufacturer**	wie Zertifikatsinhaber same as licence holder

Prüfgrundlagen **Codes and standards forming the basis of testing**	IEC 61508 Part 1 - 7 2000 IEC 61511 2004 ANSI/ISA S84.01/2004 EN 50156-1 2004 IEC 61131-2 2007	IEC 61326-3-1 2007 EN 50178 1997 EN 54-2 1997/A1 2006 NFPA 72 2007 NFPA 85 2007
Bestimmungsgemäße Verwendung **Intended application**	Safety Related Programmable Electronic System for process control Burner Management (BMS), emergency shut down, where the demand safe state is the de-energized state Applications where the demand state is the de-energized or energized state The system is suitable for safety related applications up to SIL 3 (IEC 61508, IEC 61511), considering the results of the test report no. 968/EZ 101.11/09 dated 2009-10-21	
Besondere Bedingungen **Specific requirements**	For the use of the systems the test report mentioned above, the Safety Manual, the User Manual and the official list of product documentation, hardware components and software modules released by Triconex and TÜV Rheinland have to be considered	

Dieses Zertifikat ist gültig bis 21.10.2014

This certificate is valid until 2014-10-21

Der Prüfbericht-Nr. 968/EZ 101.11/09 vom 21.10.2009 ist Bestandteil dieses Zertifikates

Der Inhaber eines für den Prüfgegenstand gültigen Genehmigungs-Ausweises ist berechtigt, die mit dem Prüfgegenstand übereinstimmenden Erzeugnisse mit dem abgebildeten Prüfzeichen zu versehen.

The test report-no. 968/EZ 101.11/09 dated 2009-10-21 is an integral part of this certificate.

The holder of a valid licence certificate for the product tested is authorized to affix the test mark shown opposite to products which are identical with the product tested.

TÜVRheinland

Functional Safety
Type Approved

FS

TÜV Rheinland Industrie Service GmbH

2009-10-21
Datum/Date

Firmenstempel/Company stamp

Dipl.-Ing. Heinz Gall

D.5 Certificado de los posicionadores Foxboro SRD960-BH

Failure Modes, Effects and Diagnostics Analysis

Project:
Intelligent Positioner SRD 991 and SRD 960

Customer:
Foxboro Eckardt GmbH
Stuttgart
Germany

Contract No.: Foxboro 04/08-16
Report No.: Foxboro 04/08-16 R001
Version V1, Revision R1, July 2007
Rainer Faller

Management summary

This report summarizes the results of the hardware assessment according to IEC 61508 carried out on the intelligent positioner SRD 991 / SRD 960. The considered safety-related application of the intelligent positioner SRD 991 / SRD 960 is as a shutdown device with fail-safe single-acting (spring return) actuation.

The intelligent positioners differ by their explosion protection. SRD 991: EEx ia and SRD 960: EEx d / EEx ia. For functional safety applications, the intelligent positioner SRD 991 / SRD 960 can be operated in three modes:

- 0..20 mA shutdown mode, shutdown threshold: 0,2 mA
- 0..20 mA shutdown mode, shutdown threshold: 1,5 mA
- 4..20 mA positioner mode, shutdown threshold: 3,8 mA.

In shutdown mode, an input current of less than the shutdown threshold (0.2 mA or 1,5 mA) leads to a shutdown of the corresponding pressure output. The different levels of shutdown threshold are to compensate possible leakage currents of the driving output.

In positioner mode, an input current of less than 3,8 mA leads to a shutdown of the corresponding pressure output, provided the positioner is configured per the Safety Manual TI EVE 0105 S. All other possible input variants or electronics are not covered by this report.

The hardware assessment consists of a Failure Modes, Effects and Diagnostics Analysis (FMEDA). A FMEDA is one of the steps taken to achieve functional safety assessment of a device per IEC 61508. From the FMEDA, failure rates are determined and consequently the Safe Failure Fraction (SFF) is calculated for the device. For full assessment purposes all requirements of IEC 61508 must be considered.

The failure rates used in this analysis are the basic failure rates for electronic components from the Siemens standard SN 29500. For mechanical components experience-based *exida* data and field failure evaluations from Eckardt S.A.S. France were used.

The control electronics of the intelligent positioner SRD 991 / SRD 960 are considered to be a Type B[1] subsystem with a hardware fault tolerance of 0. The pneumatics of the intelligent positioner SRD 991 / SRD 960 are considered to be a Type A[2] subsystem with a hardware fault tolerance of 0.

Table 1: Summary for SRD 991 / SRD 960 as shutdown device, threshold 0,2 mA – Type A device, IEC 61508 failure rates

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC_S[3]	DC_D
0 FIT	327 FIT	0 FIT	20 FIT	94%	0%	0%

These failure rates do not include failures resulting from incorrect use of the intelligent positioner, in particular humidity entering through incompletely closed housings or inadequate cable feeding through the PG inlets.

A user of the intelligent positioner SRD 991 / SRD 960 can utilize these failure rates in a probabilistic model of a safety instrumented function (SIF) to determine suitability in part for safety instrumented system (SIS) usage in a particular safety integrity level (SIL).

Type B component: "Complex" component (using micro controllers or programmable logic); for details see 7.4.3.1.3 of IEC 61508-2.

Type A component: "Non-complex" component (all failure modes are well defined); for details see 7.4.3.1.2 of IEC 61508-2.

[3] DC means the diagnostic coverage (safe or dangerous).

The failure rates are valid for the useful life of the instrument. According to section 7.4.7.4 note 3 of IEC 61508-2, experience has shown that the useful lifetime often lies within a range of 8 to 12 years.

Table 2: Summary for SRD 991 / SRD 960 as shutdown device, threshold 0,2 mA – PFD_{AVG} values

T[Proof] = 1 year	T[Proof] = 2 year	T[Proof] = 5 years	T[Proof] = 10 years
8.8E-05	1.8E-04	4.4E-04	8.8E-04

The boxes marked in yellow ( ) mean that the calculated PFD_{AVG} values are within the allowed range for SIL 3 according to table 2 of IEC 61508-1 but do not fulfill the requirement to not claim more than 20% of this range, i.e. to be better than or equal to 2.0E-04. The boxes marked in green ( ) mean that the calculated PFD_{AVG} values are within the allowed range for SIL 3 according to table 2 of IEC 61508-1 and table 3.1 of ANSI/ISA–84.01–1996 and do fulfill the requirement to not claim more than 20% of this range, i.e. to be better than or equal to 2.0E-04.

Table 3: Summary for SRD 991 / SRD 960 as shutdown device, threshold 1,5 mA – Type A device, IEC 61508 failure rates

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC_S	DC_D
0 FIT	342 FIT	1 FIT	27 FIT	93%	0%	4%

Table 4: Summary for SRD 991 / SRD 960 as shutdown device, threshold 1,5 mA – PFD_{AVG} values

T[Proof] = 1 year	T[Proof] = 2 year	T[Proof] = 5 years	T[Proof] = 10 years
1.2E-04	2.4E-04	5.9E-04	1.2E-03

Table 5: Summary for SRD 991 / SRD 960 as smart positioner, shutdown threshold: 3,8 mA – Type B device, IEC 61508 failure rates

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC_S	DC_D
43 FIT	572 FIT	73 FIT	73 FIT	90%	7%	50%

Table 6: Summary for SRD 991 / SRD 960 as smart positioner, shutdown threshold: 3,8 mA – PFD_{AVG} values

T[Proof] = 1 year	T[Proof] = 2 year	T[Proof] = 5 years	T[Proof] = 10 years
3.2E-04	6.4E-04	1.6E-03	3.2E-03

The boxes marked in yellow ( ) mean that the calculated PFD_{AVG} values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 but do not fulfill the requirement to not claim more than 20% of this range, i.e. to be better than or equal to 2.0E-03. The boxes marked in green ( ) mean that the calculated PFD_{AVG} values are within the allowed range for SIL 2 according to table 2 of IEC 61508-1 and table 3.1 of ANSI/ISA–84.01–1996 and do fulfill the requirement to not claim more than 20% of this range, i.e. to be better than or equal to 2.0E-03.

SIL Konformitätserklärung
Declaration of conformity

invensys
ECKARDT

Eckardt SAS · 20, rue de la Marne · F-68360 Soultz
Foxboro Eckardt GmbH · Pragstr. 82 · D-70376 Stuttgart

Stuttgart, 05.2.2007

Funktionale Sicherheit nach IEC 61508 / IEC 61511
Functional Safety according to IEC 61508 / IEC 61511

Wir erklären, dass die Geräte
We declare, that the devices

SRD991-BHxxx, SRD991-BDxxx
SRD960-BHxxx, SRD960-BDxxx

für den Einsatz in einer sicherheitsgerichteten Anwendung entsprechend der IEC 61511-1 geeignet sind, wenn die Sicherheitshinweise und die nachfolgenden Parameter beachtet werden:
are suitable for use in a safety related application according IEC 61511-1,
if the safety instructions and the following parameters are observed:

Einsatzart Usage	Stromabschaltung unter Schwelle 0,2mA Shutdown device, threshold 0,2mA	Stromabschaltung unter Schwelle 1,5/2mA Shutdown device, threshold 1,5/2mA	Normalabschaltung Smart positioner
SIL	3	2	2
Prüfintervall / Proof test interval	≤ 1 Jahr / year		
Gerätetyp / Device Type	A	A	B
HFT	0 [1] (einkanalige Verwendung / single channel usage)		
SFF	94%	93%	90%
PFG_{avg}	$8{,}8 \times 10^{-5}$	$1{,}2 \times 10^{-4}$	3.2×10^{-4}
λ_{du}	20 FIT	27 FIT	73 FIT
λ_{dd}	0 FIT	1 FIT	73 FIT
λ_{su}	327 FIT	342 FIT	572 FIT
λ_{sd}	0 FIT	0 FIT	43 FIT
DC_S	0%	0%	7%
DC_D	0%	4%	50%

[1] gemäß Kapitel / according to chapter 11.4.4 of IEC 61511-1

Robert Leng
General Manager
Eckardt SAS

Gilles Annenkoff
Quality Manager
Eckardt SAS

Dr. Joachim Seckler
Development Manager
Foxboro Eckardt GmbH

ANEXO E
GLOSARIO DE TÉRMINOS

E.1 Abreviaturas

En la Tabla E.1 se presentan las abreviaturas utilizadas en el despliegue del presente informe basadas en las definiciones expuestas por las normas IEC 61508 e IEC 61511.

TABLA N° E.1 Lista de abreviaturas

	Expresión completa en inglés	Traducción en español
ALARP	As low as reasonably practicable	Tan bajo como sea razonablemente práctico
ANSI	American National Standards Institute	Instituto Nacional Estadounidense de Estándares
BMS	Burner management system	Sistema de administración de quemadores
BPCS	Basic process control system	Sistema básico de control de procesos
DC	Diagnostic coverage	Cobertura del diagnóstico
DCS	Distributed control system	Sistema de control distribuido
E/E/PE	Electrical/electronic/programmable electronic	Eléctrico/electrónico/electrónico programable
E/E/PES	Electrical/electronic/programmable electronic system	Sistema eléctrico/electrónico/electrónico programable
EMC	Electro-magnetic compatibility	Compatibilidad electro-magnética
HFT	Hardware fault tolerance	Tolerancia a fallas del hardware
IEC	International Electrotechnical Commission	Comisión Electrotécnica Internacional
ISA	International Society of Automation	Sociedad Internacional de Automatización
ISO	International Organization for Standardization	Organización Internacional para la Estandarización
MooN	«M» out of «N»	«M» sobre «N»
NFPA	National Fire Protection Association	Asociación Nacional de Protección contra Incendios
PFD	Probability of failure on demand	Probabilidad de fallo ante la demanda
PFDavg	Average probability of failure on demand	Probabilidad media de fallo ante la demanda
PLC	Programmable logic controller	Controlador lógico programable
RRF	Risk reduction factor	Factor de reducción del riesgo
SFF	Safe failure fraction	Fracción de fallo seguro
SIF	Safety instrumented function	Función instrumentada de seguridad
SIL	Safety integrity level	Nivel de integridad segura
SIS	Safety instrumented system	Sistema instrumentado de seguridad

E.2 Definiciones

Cobertura del diagnóstico (DC – Diagnostic coverage)

Relación entre la tasa de fallos detectados y el total de fallos del componente o sub sistema como resultado del test de diagnóstico del instrumento.

Consecuencia

Es el grado del daño causado por un Accidente (heridas graves, muertes, contaminación ambiental, destrucción de la propiedad, etc.).

E/E/PE

Dispositivos basados en tecnología eléctrica (electro – mecánicos), electrónica (estado sólido) y de computadoras (programables).

Fallo

Culminación de la factibilidad de un equipo de ejecutar una función requerida.

Factor de Reducción de Riesgo (RRF – Risk Reduction Factor)

Es el orden de magnitud en que puede reducirse el nivel de riesgo de un proceso, medido generalmente en potencias de 10.

Función Instrumentada de Seguridad (SIF – Safety Instrumented Function)

Función que ejecuta un Sistema Instrumentado de Seguridad (SIS), con la intención de lograr o mantener un estado seguro para el proceso, ante la ocurrencia de un evento peligroso.

Integridad Segura

Probabilidad media que el Sistema Instrumentado de Seguridad (SIS) ejecute satisfactoriamente las Funciones Instrumentadas de Seguridad necesarias bajo las condiciones establecidas en un periodo de tiempo.

Instrumento / Instrumentación

Aparato usado para el desempeño de una acción. Los sistemas instrumentados en el sector de procesos están compuestos típicamente por sensores (por ejemplo, de presión, flujo, transmisores de temperatura), resolvedores de lógica o sistemas de control (por ejemplo, PLC, DCS), y elementos finales (por ejemplo, válvulas de control). En casos especiales, los sistemas instrumentados pueden ser sistemas instrumentados de seguridad (SIS).

MooN ("M" out of "N")

Sistema instrumentado de seguridad o parte de él, compuesto por "N" canales independientes, donde "M" canales son suficientes para ejecutar la función instrumentada de seguridad.

Nivel de Integridad Segura (SIL – Safety Instrumented Level)

Nivel discreto (de 4 existentes) para especificar los requisitos de Integridad Segura de las Funciones Instrumentadas de Seguridad (SIF) a ser asignados al Sistema Instrumentado de

Seguridad (SIS). SIL 4 tiene el mayor nivel de integridad segura mientras que SIL 1 presenta el menor nivel de integridad segura.

Nivel de Riego

Es un valor numérico que nos permite percibir en qué medida podremos esperar que ocurra un accidente y cuál será el daño que éste podría causar.

Nivel de Riesgo Aceptable (NRA)

Es un valor numérico que define el Nivel de Riesgo, por debajo del cual, podrá aceptarse que las personas, la población, el medio ambiente o el patrimonio de la Empresa, sean expuestos.

Nivel de Riesgo Inaceptable (NRI)

Es un valor numérico que define el Nivel de Riesgo, por encima del cual, bajo ningún punto de vista, podrá exponerse a las personas, a la población, al medio ambiente o al patrimonio de la Empresa.

Nivel de Riesgo Tolerable (NRT)

Es un valor numérico que define el Nivel de Riesgo al cual pudiera exponerse a las personas, a la población, al medio ambiente o al patrimonio de la Empresa, toda vez que su reducción hacia valores de Riesgo Aceptable fuera imposible o muy costosa de implementar.

Peligro

Fuente potencial de producir daño físico a las personas de manera directa o indirecta. *(Esta definición presentada por IEC excluye daños a la propiedad o el ambiente que no producen daño a las personas; es por ello que difiere de modernas definiciones)*

Probabilidad de fallo ante la demanda (PFD – Probability of failure on demand)

Probabilidad que el sistema reciba una verdadera demanda o pedido de protección, pero por alguna inhibición interna, es incapaz de procesarla dejando al proceso sin protección frente al riesgo inminente.

Proceso

Equipo, maquinaria, aparato o planta usada para elaboración, transformación, almacenamiento, transporte, etc., de materiales, productos y subproductos (durante el

desarrollo del cual pudieran generarse accidentes industriales).

Proceso peligroso

Proceso que tiene el potencial de producir serios daños a las personas (a la propiedad o al medio ambiente) producto de un mal funcionamiento.

Redundancia

Uso de múltiples elementos o sistemas para la ejecución de la misma función; la redundancia puede ser implementada por elementos idénticos (redundancia idéntica) o por diversos elementos (redundancia diversa)

Riesgo

Combinación de la frecuencia de ocurrencia del daño y la severidad o consecuencia del daño.

Seguro

Libre de riesgo inaceptable.

Sistema Básico de Control de Procesos (BPCS – Basic Process Control System)

Sistema que responde a señales de entrada del proceso, de su equipamiento asociado, otros sistemas programables o del operador y que genera señales de salida causando que el proceso y su equipamiento asociado operen de la manera deseada.

Sistema Instrumentado de Seguridad (SIS)

Sistema usado para implementar una o más Funciones Instrumentadas de Seguridad (SIF). Un SIS está formado por una combinación de sensores, resolvedores de lógica y elementos finales.

Tiempo medio de restablecimiento (MTTR – Mean Time to Restoration)

Intervalo de tiempo entre un diagnóstico de falla y la restauración completa a operación normal.

Tolerancia a fallos del hardware (HFT – Hardware Fault Tolerant)

Es la habilidad de un componente o subsistema de mantener su Función Instrumentada de Seguridad (SIF) correspondiente en presencia de una o más fallos peligrosas en el hardware.

BIBLIOGRAFIA

[1] Grupo Universitario de Investigación Analítica de Riesgos (GUIAR) de la Universidad de Zaragoza, "Accidente de Bophal", [Online]. Disponible en http://www.unizar.es/guiar/1/Accident/Bhopal.htm

[2] Grupo Universitario de Investigación Analítica de Riesgos (GUIAR) de la Universidad de Zaragoza, "Accidente de Cubato", [Online]. Disponible en http://www.unizar.es/guiar/1/Accident/Cubatao.htm

[3] Grupo Universitario de Investigación Analítica de Riesgos (GUIAR) de la Universidad de Zaragoza, "Accidente de San Juan de Ixhuatepec", [Online]. Disponible en http://www.unizar.es/guiar/1/Accident/San_Juan.htm

[4] Ron Bell, "Introduction to IEC 61508" en Tenth Australian Workshop on Safety-Related Programmable Systems (SCS 2005), Sydney, Australia, [Online]. Disponible en http://crpit.com/confpapers/CRPITV55Bell.pdf

[5] Robert E. Young, "Petroleum Refining Process Control and Real-Time Optimization" en IEEE Control System Magazine, Vol. 26 No. 6, Diciembre 2006, pags. 73 – 83.

[6] U.S. Energy Information Administration, "Oil: Crude and Petroleum Products Explained", [Online]. Disponible en http://tonto.eia.doe.gov/energyexplained/index.cfm?page=oil_refining#tab2

[7] Shell Company, "Refining Process", [Online]. Disponible en http://www.shell.com/home/content/src/about_src/refining_process/

[8] Antonio Creus Sole, "Instrumentación Industrial", 7ma edición, Noviembre 2005.

[9] International Electrotechnical Commission, "P-IEC 61508-1 ed1.0 withdrawn – Publication detail". Disponible en http://webstore.iec.ch

[10] International Electrotechnical Commission, "IEC 61511-1 ed1.0 – Publication detail". Disponible en http://webstore.iec.ch

[11] MTL Instruments, "An introduction to Functional Safety and IEC61508", [Online]. Disponible en http://www.mtl-inst.com/images/uploads/datasheets/App_Notes/AN9025.pdf

[12] International Society of Automation, "ANSI/ISA-84.00.01-2004 Part 1 (IEC 61511-1

Mod) – Publication detail". Disponible en http://www.isa.org/

[13] Health and Safety Executive, "ALARP at a glance", [Online]. Disponible en http://www.hse.gov.uk/risk/theory/alarpglance.htm

[14] Iberfluid Instruments, "Introducción a los Sistemas SIL", [Online]. Disponible en http://www.iberfluid.com/consierge/docs/1046_articles_657_SIL.doc

[15] International Electrotechnical Commission, "International Standard IEC 61508, Functional safety of electrical/electronic/programmable electronic safety-related systems". Edición 1998

[16] International Electrotechnical Commission, "International Standard IEC 61511, Functional safety — Safety instrumented systems for the process industry sector". Edición 2003

[17] Yuri Alexis Rizo Delgado, "Automatización segura", [Online]: Disponible en http://enersapq.com.co/enersa/images/SafeAutomation1.pdf

[18] National Fire Protection Association, "NFPA 85, Boiler and Combustion System Hazards Code", Edición 2001.

[19] Jorge Bourdette, "Seguridad y Disponibilidad en Calderas y Hornos" en ABB Automation World 2008, Argentina