ANEXO D
SISTEMAS INSTRUMENTADOS DE SEGURIDAD

Los sistemas instrumentados de seguridad son sistemas automatizados, diseñados a prueba de fallas. Estan constituidos por lazos de seguridad conformados por sensores, controladores logicos y elementos finales de seguridad. Estos sistemas de seguridad aplican normalmente a variables criticas y situaciones de control que no pueden ser atendidos por operarios debido a su complejidad, velocidad de desarrollo y porque requieren detectarse de manera temprana y oportuna.

Los sistemas de control están diseñados para permitir un acceso relativamente fácil porque los operadores deben realizar cambios frecuentes, a diferencia de los sistemas de seguridad que demandan estrictos procedimientos de seguridad y control de acceso con el fin de prevenir cambios accidentales.

Los sistemas de control de procesos son activos y dinámicos, tienen entradas y salidas analógicas y permite realizar operaciones matemáticas. Por lo tanto, la mayoría de las fallas en los sistemas de control son inherentemente de auto-revelación y no es necesario un diagnóstico amplio para informar estos fallos, mientras que los sistemas de seguridad son pasivos o inactivos y muchas fallas no se revelan a sí mismo. Los sistemas de seguridad requieren pruebas efectivas de auto-diagnóstico, algo que muchos sistemas de control no incorporan de manera muy eficaz.

En la tabla 1, se encuentran las diferencias entre el sistema de control básico del proceso y un sistema instrumentado de seguridad:

Sistema de control del proceso básico (BPCS)	**Sistema instrumentado de seguridad**
Activo/Dinámico	Pasivo/durmiente
Uso continuo	Uso esporádico
Entradas/Salidas Analógicas, lazos de control, calculo numérico y matemática.	Entrada/salidas analógicas y discretas, control discreto y lógica simple.
Fallas auto reveladas.	Fallas ocultas.
No necesita diagnóstico.	Necesidad de diagnósticos extensivos, periódicos y pruebas para verificación de la integridad.
Flexibilidad para permitir cambios frecuentes.	Se evitan los cambios frecuentes y los mismos deben ser controlados y documentados según los ciclos de vida del SIS.
Tiempo medio para reparar crítico, para evitar largas paradas de producción.	Tiempo medio para reparar, muy crítico, hace referencia al termino disponibilidad.
Control manual manejado por operadores.	Permiten muy poca interacción humana.

Tabla 1. Sistemas instrumentados de seguridad y BPCS

Los SIS están conformados principalmente por tres partes:

a) Las entradas del sistema, que representan las señales provenientes de los sensores de campo o por otro tipo de dispositivo que afecte las secuencias lógicas, estas señales de entrada son las señales del proceso que se están midiendo las variables del proceso.
b) La lógica de enclavamiento implementada en el controlador lógico, representa en forma simbólica la toma de decisiones generadas por el estado de las entradas y define el estado de las salidas, por lo tanto es el encargado de monitorear las entradas y tomar la acción correctiva ante una condición de falla en el proceso.
c) Las salidas del sistema, que son las señales destinadas a operar los equipos o elementos finales de control conectados al proceso, estos dispositivos se encuentran entre el elemento controlador lógico y el proceso, ejecutando una acción de paro.

La constante evolución en la tecnología, ha permitido que los usuarios finales puedan seleccionar instrumentación con un grado de seguridad mayor y de esta manera los procesos productivos operen de forma segura de acuerdo a los estándares de seguridad funcional. Características que deberían considerarse en los componentes del sistema instrumentado de seguridad son:

1.1. Dispositivos de campo

Para una configuración de sensor 1oo2, algunos usuarios les gusta pasar por alto los dos sensores a la vez, pero a otros les gusta tener una derivación para cada sensor. Si ambos sensores están excluidos, será necesario para poner en marcha medidas para asegurar que el riesgo se mantiene tolerable. Puede ser posible, pero esto debe abordarse al comienzo del diseño.

Del mismo modo, algunas operaciones de los procesos no son compatibles con la válvula que se mueve mientras se ejecuta el proceso o la instalación de una derivación alrededor de la válvula puede ser poco práctica. En estos casos, el diseño debe permitir probar el SIS en la medida de lo posible, es decir, al menos a través de la válvula de solenoide. En este caso, algún tipo de derivación alrededor del solenoide se puede incluir en el diseño de los controles habituales alarmante o de procedimiento para esta derivación.

1.1.1. Sensores

Los sensores son dispositivo o combinación de dispositivos que miden las condiciones del proceso, pueden ser transmisores, interruptores de proceso, interruptores de posición, entre otros.

Los requerimientos generales para operación a falla segura que se deben cumplir en sensores son:

a) Durante una operación normal de proceso los contactos de los sensores deben estar cerrados y energizados.

b) En el caso de falla de energía, las señales de los transmisores deben ir a un estado seguro.
c) En el caso de usar transmisores, se deben configurar de tal forma que se pueda aprovechar la señal fuera de rango que normalmente ofrecen los transmisores.
d) Cuando se requieran más de dos sensores, se debe: realizar conexiones separadas a proceso para cada sensor, las señales de entrada al procesador lógico las debe hacer en módulos de entrada separados o un módulo de entrada que garantice la reducción de fallas de causa común y cumpla con la integridad requerida.
e) En el caso de sensores del tipo interruptores, el contratista debe llevar a cabo los arreglos y cálculos necesarios para realizar la supervisión de los lazos correspondientes a estos sensores, la supervisión debe proveer la siguiente información: interruptor activado, interruptor desactivado, circuito abierto y corto circuito.

Los sensores inteligentes deben estar protegidos contra escritura para evitar la modificación accidental desde una ubicación remota, a menos que una adecuada revisión de seguridad permite el uso de lectura / escritura. La revisión debe tener en cuenta los factores humanos, como incumplimiento de los procedimientos.

1.1.2. Elementos finales:

Elementos finales como las válvulas deben seleccionarse de acuerdo a las condiciones específicas del proceso y la función deseada. Por lo tanto, está permitido el empleo de válvulas de bola, de mariposa, o algún otro tipo que justifique su uso en aplicaciones de seguridad. Los factores que deben considerarse para la determinación de los requerimientos de válvulas son:

- Requerimientos de corte, la experiencia que se tenga con las válvulas, modos de falla de la válvula, procedimientos operativos que disminuyan su efectividad, requerimientos de pruebas, requerimientos de diagnóstico, requerimientos de indicadores de posición o interruptores de posición, entre otros.
- Determinación de la posición segura en caso de falla de energía

Cuando aplique y de acuerdo al diseño en particular de ciertas instalaciones es necesario contar con válvulas de desvío y de bloqueo, sobre todo en aquellas válvulas del SIS que cierran a falla de aire/energía y que de probarse en línea causen serios problemas operacionales, en otras ocasiones, es necesario proveer a la válvula del SIS sólo con bloqueos (por ejemplo en válvulas que a falla abren). En los casos donde se requiera contar con desvío y bloqueos, se debe considerar la instalación de dos válvulas de purga/venteo (dependiendo del servicio en la línea) instaladas entre las válvulas de bloqueo corriente arriba y corriente abajo de la válvula del SIS, en este caso, se deben utilizar interruptores de posición que alarmen en el cuarto de control del SIS cuando la válvula de desvío sea abierta o cuando alguna de las válvulas de bloqueo sean cerradas. Las válvulas de desvío (bypass) y de bloqueo deben ser mecánicamente enclavadas a fin de evitar que

las válvulas de corte del SIS puedan ser desviadas o bloqueadas respectivamente de forma inadvertida. Los interruptores de desviación BYPASS deberán ser protegidos por bloques o contraseñas para prevenir el uso no autorizado. Si las opciones o desviaciones se seleccionan en el BPCS y descarga en el SIS, fallas en el BPCS puede interferir con la capacidad de los SIS para operar en demanda.

Todas las válvulas deben de contar con indicadores de posición local. Se debe marcar con flechas en ambos lados de la válvula la dirección del flujo.

Las válvulas de derivación o bypass aseguran que los elementos finales de control no se activen durante las pruebas de los sensores o del controlador, pero el uso de BYPASS manuales para desactivar válvulas de bloqueo del sistema no es recomendable por el uso equivocado en que podría resultar. Por esta razón la posición del bypass debe ser señalada de manera clara al operador y se debe establecer procedimientos precisos para su uso.

1.2. Cableado y fuentes de energía.

En los cables y líneas de control se debe considerar el recubrimiento y blindaje como medidas de protección contra grasa, solvente e interferencias electromagnéticas. Además se debe evitar que las rutas de cables pasen por áreas de alto riesgo o muy vulnerables.

Cada dispositivo de campo individual tendrá su propio cableado dedicado al sistema de entrada / salida, excepto en los casos siguientes:

- Múltiples sensores discretos conectados en serie a una sola entrada y los sensores monitorean la condición de un mismo proceso (por ejemplo, sobrecargas del motor).
- Varios elementos finales están conectados a una única salida.

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

Las fuentes de energía incluyen a la energía eléctrica, neumática (aire de instrumentos) e hidráulica (central hidráulica) entre otros. La conexión a tierra se incluye dentro de la categoría de energía eléctrica.

La redundancia en la fuente de energía eléctrica debe aplicarse mediante el uso de una fuente alterna con transferencia automática, un suministro de potencia interrumpible (UPS) o bien una batería de respaldo. Se debe contar con un interruptor de transferencia automática con restablecimiento manual para la transferencia de la fuente de energía primaria a la fuente de respaldo en caso de pérdida del suministro de energía.

1.3. Controlador lógico:

El controlador lógico en el SIS puede ser:

a) Sistemas eléctricos lógicos usando tecnología electro-mecánica
b) Sistemas lógicos electrónicos usando tecnología electrónica

Sistemas lógicos “Electrónico Programable” (EP) usando sistemas electrónicos programables: Comprenden PLCs, sistemas microprocesados, sistemas de control distribuido, sensores y actuadores inteligentes.

Hay un número de tecnologías disponibles para utilizar en sistemas instrumentados de seguridad, como los sistemas neumáticos, relés electromecánicos, relés de estado sólido, y controladores lógicos programables (PLC). Cada tecnología tiene sus ventajas y desventajas, pero para la selección se deben tener en cuenta factores como el presupuesto, tamaño, nivel de riesgo, la complejidad, la flexibilidad, el mantenimiento, la interfaz, la comunicación y los requisitos de seguridad.

- **Sistemas neumáticos:**
  Los sistemas neumáticos se utilizan normalmente en aplicaciones pequeñas donde hay un deseo de simplicidad, seguridad intrínseca y donde la energía eléctrica no está disponible.

- **Sistemas relé:**
  Los sistemas de relé ofrecen una serie de ventajas:

  - Simplicidad.
  - Bajo costo de instalación y mantenimiento.
  - Inmune a la mayoría de las formas de interferencia EMI / RFI.
  - Disponible en diferentes rangos de tensión.
  - Tiempo de respuesta rápido.
  - No requiere software.
  - A prueba de fallos.

  Desventajas:

  - Disparos en falso: los sistemas de relé normalmente son no redundantes. Esto significa que la falta de un solo relé puede resultar en un falso disparo en el proceso, impactando significativamente los costos de operación en general.
  - La complejidad: Cuanto mayor es un sistema relé, es más difícil de manejar. Un sistema relé es manejable hasta 10 entradas y salidas.
  - No hay comunicación en serie: los sistemas relé no ofrecen ningún tipo de comunicación a otros sistemas.
  - Falta de medios inherentes a las pruebas o desviaciones: los sistemas basados en relés no ofrecen ninguna característica estándar para las pruebas o la realización de derivaciones. Los

sistemas de relé están basados en señales lógicas discretos (encendido/apagado).

- **Sistemas de estado sólido:**
  Estos sistemas han sido diseñados para reemplazar los relés y los circuitos de estado sólido con baja potencia. Estos sistemas son relativamente caros en comparación con otras opciones, las aplicaciones son limitadas y no son de uso común en la industria.

  Los sistemas de estado sólido tienen una serie de ventajas:

  - Las capacidades de pruebas y derivación: los sistemas de estado sólido se han construido para ejecutar funciones de seguridad en general e incluyen funciones para realizar pruebas.
  - Capacidades de comunicación en serie.
  - El uso principal de sistemas de estado sólido es en aplicaciones de niveles de integridad de seguridad altos, como SIL 4.

  Los sistemas de estado sólido presentan las siguientes desventajas:

  - Cableado: están cableados, de forma similar a los relés.
  - La lógica binaria: realizan el mismo tipo de lógica binaria (encendido/apagado) de los relés.
  - Alto costo
  - No redundante: Al igual que los relés, se suelen suministrar en una configuración no redundante.
  - Estos sistemas no utilizan tarjetas con canal de múltiples entradas y salidas.

- **Microprocesador, PLC.**
  Los sistemas basados en software son utilizados en el mayor porcentaje de solicitudes.

  Estos sistemas tienen las siguientes ventajas:

  - Costo razonable.
  - Facilidad y flexibilidad para hacer cambios.
  - Comunicación en serie.
  - Interfaces de operador gráfico.
  - Auto-documentación.

  Los PLC son de uso general, sin embargo, no fueron diseñados para aplicaciones críticas de seguridad. La mayoría de las unidades no tienen la capacidad de diagnóstico, las características a prueba de fallos, o los niveles de eficacia de la redundancia para su uso más allá de aplicaciones SIL 1. Son dispositivos especialmente diseñados y certificados para cumplir

con una determinada tasa de probabilidad de falla peligrosa, con distintas arquitecturas.

Los PLC de seguridad incluyen diagnósticos internos extensos que permiten realizar pruebas cruzadas de funcionamiento, de manera tal que una falla pueda ser detectada normalmente antes de que una acumulación de fallas conduzca a una situación peligrosa

Los siguientes requerimientos podrían ser solo aplicados a controladores lógicos usados en SIS los cuales tienen implementado SIF de SIL 1 o SIL 2.

- Comprender los modos de falla insegura;
- Uso de técnicas para configuraciones de seguridad que direcciones la identificación de modos de falla;
- El software integrado tiene un buen historial de uso para aplicaciones de seguridad;
- Protección contra modificaciones no autorizadas o no deseadas
- Capacidad de ejecutar requerimientos de funciones y que usos previos han mostrado que hay una baja probabilidad que este falle de alguna manera la cual podría encabezar un evento peligroso o fallas sistemáticas en el hardware y software.
- Aplicación de medidas para detectar fallas en la ejecución del programa e iniciar una adecuada reacción, estas medidas comprenden: un programa de vigilancia de la secuencia, protección del código contra la modificación o la detección de fallos de supervisión en línea y confirmación de fracaso o una programación diversa.

Para aplicaciones SIL 2, un manual de seguridad que incluyen restricciones para la operación, mantenimiento y detección de fallas deberá estar disponible para cubrir las configuraciones típicas del controlador lógico. Debe estar diseñado a falla segura en caso de pérdida de energía o bien cuando falla el sistema o alguno de sus componentes clave. El procesador lógico y sus módulos deben contar con autodiagnóstico. La lógica interna de cada CPU debe traer incorporadas rutinas diagnósticas y de prueba automática en línea, y detección de fallas para determinar el estado de cada módulo o del subconjunto que está dentro del sistema. La unidad de control debe ser capaz de funcionar de acuerdo a los parámetros climáticos propios del sitio de instalación, ser resistente a los golpes, vibración, descargas electrostáticas, interferencia electromagnética y radiofrecuencia.

A la unidad de control se le debe dar mantenimiento en línea sin perder la protección.

1.4. Interfaces

El diseño de la interfaz del operador del SIS deberá ser tal que eviten cambios en las aplicaciones software del SIS. Cuando la información de seguridad necesita

ser transmitida desde el BPCS al SIS, entonces, los sistemas deben ser utilizados de forma selectiva, para permitir la escritura del BPCS a las variables específicas del SIS.

En la comunicación externa se debe considerar aquella que se lleva a cabo entre un SIS y uno o más sistemas independientes para efectuar intercambio de información de monitoreo y de comandos de acción, el contratista debe verificar que esta comunicación no comprometa la integridad del SIS.

La interfaz de operador que se utiliza para transmitir información entre el operador y el SIS pueden incluir:

- **Pantallas de video**
  La presentación de la pantalla es importante, porque diseños con una gran cantidad de información en una pantalla puede conducir a que los operadores interpretan mal los datos y toman acciones equivocadas. Los colores, los indicadores y la buena distribución de la información se deben utilizar para guiar al operador a la información importante a fin de reducir la posibilidad de confusión. Los mensajes deben ser claros, concisos y sin ambigüedades.

  El operador debería tener suficiente información en una pantalla para transmitir rápidamente información crítica. Es importante mostrar la coherencia y los métodos, las convenciones de alarma y componentes de la pantalla utilizada debe ser coherente con la muestra BPCS.

- **Paneles:**
  Los paneles deben estar dispuestos para asegurar que el diseño de los botones, lámparas, medidores e interruptores no es confuso y es de fácil acceso para el operador.

  Los interruptores de apagado para distintas unidades de proceso o equipos, que tienen el mismo aspecto y/o están agrupados, pueden resultar en el cierre equivocado de un equipo debido a que el operador estaba bajo estrés en una situación de emergencia. Los componentes de los paneles deben estar físicamente separados y etiquetados de su función.

- **Anunciador:**
  Los anunciadores de eventos peligrosos pueden ser visuales y sonoros, deben estar instalados de tal manera que permitan tener una reacción inmediata por parte de los operarios.

- **Impresoras:**
  Las impresoras son útiles para registrar la secuencia en que ocurren los hechos, pruebas diagnósticas y otros eventos, con estampado de fecha, hora y la identificación por número de etiqueta.

Si la impresión es una función de reserva (la información es almacenada y luego impresos bajo demanda o en un horario de tiempo), entonces el buffer debe ser de un tamaño para que la información no se pierda, y bajo ninguna circunstancia la funcionalidad SIS está comprometida debido a espacio lleno de memoria.

Si la impresora no funciona, se apaga, se desconecta, se queda sin papel o se comporta de manera anormal, no debe comprometer las funciones instrumentadas de seguridad.

La información del estado del SIS estará disponible como parte de la interfaz del operador. Esta información puede incluir:

a) La secuencia del proceso.
b) Indicación de que la acción protectora del SIS ha ocurrido.
c) Indicación de que una función de protección se pasa por alto.
d) Indicación de que una acción automática (s), como la degradación de la votación y/o gestión de fallos se ha producido;
e) Estado de los sensores y elementos finales;
f) La pérdida de energía, donde esa pérdida de energía impacta la seguridad;
g) Los resultados de los diagnósticos;
h) Modo de funcionamiento del SIS, programas, datos, medios de desactivación en la comunicación de las alarmas, prueba, derivación, mantenimiento, diagnóstico, servicios de votación y manejo del fallo.
i) Fallas del equipo debido a las condiciones ambientales que afectan al SIS.
j) Histórico de alarmas y secuencia de eventos.
k) Pantallas operativas de mantenimiento periódico.
l) Registro para control y auditoria del mantenimiento del sistema.

2. CARACTERÍSTICAS FUNCIONALES DE LOS SIS

2.1. Confiabilidad (MTTF)

La fiabilidad de los sistemas de seguridad puede definirse como el tiempo promedio entre las fallas que ocurren en el sistema. En este contexto, falla significa la ocurrencia de una situación inesperada que causa un valor incorrecto de salida.

La cuota de avería es la medida utilizada para determinar número de averías por unidad de tiempo.

$$Cuota\ de\ averia = \lambda = \frac{averias\ por\ unidad\ de\ tiempo}{Número\ de\ componentes\ expuestos\ a\ averia\ funcional}$$

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

$$\text{MTTF} = \frac{1}{\lambda}$$

La fiabilidad es la probabilidad de éxito de un dispositivo en el intervalo de tiempo de 0 a t, la figura 1 indica la fiabilidad de un dispositivo, en función del tiempo. Al aumentar el tiempo de cero a TTF (Time To Fail), tiempo estimado de avería o intervalo de tiempo máximo dentro del cual se prevé que el sistema se podría averiar con una probabilidad cercana al 100%. En el tiempo **t,** se tendrá una probabilidad del 76% de operatividad sin averías.

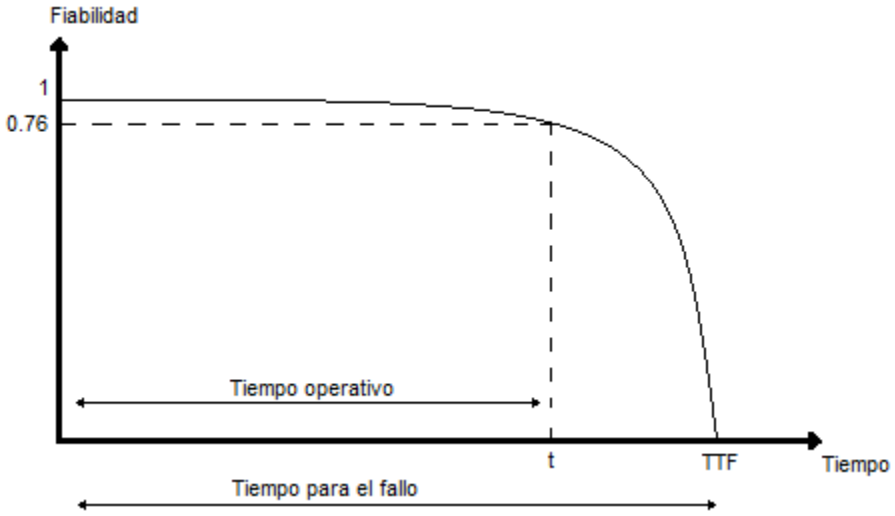

Figura 1. Grafico de la fiabilidad de un dispositivo.

La fiabilidad está en función del tiempo de funcionamiento, las unidades de medida son en porcentaje por tiempo de funcionamiento.

2.2. Disponibilidad (MTTR, MTBF)

La disponibilidad en sentido genérico, relaciona el tiempo en que el sistema ha estado disponible y el tiempo total incluido la reparación.

$$Disponibilidad = \frac{Tiempo\ operatividad}{Tiempo\ operatividad + Tiempo\ reparación}$$

$$Disponibilidad = \frac{MTTF}{MTBF} = \frac{\frac{1}{\lambda}}{\frac{1}{\lambda} + \frac{1}{\mu}} = \frac{\mu}{\mu + \lambda}$$

MTBF (Mean Time Between Failure), tiempo medio entre fallas, es un término que se aplica solo a los dispositivos reparables. MTTF (Mean Time To Failure), tiempo

medio de falla y MTTR (Mean Time To Repair), tiempo medio de reparación, es un valor medio, es decir el tiempo medio entre dos averías funcionales sucesivas.
Se expresan:

$$MTBF = MTTF + MTTR$$

El indicador de la probabilidad de bloqueos espurios de planta causados por averías seguras del sistema o dispositivo:

$$MTBFs = \frac{1}{\lambda s}$$

Indicador de la probabilidad de bloqueos de seguridad de la planta causados por el fallo de la función de seguridad:

$$MTBFd = \frac{1}{\lambda d}$$

El término MTTR se determina con la siguiente ecuación:

$$Cuota\ de\ reparación = \frac{1}{MTTR} = \mu$$

La cuota de reparación μ es constante en el tiempo.

2.3. Diagnóstico: SFF, HFT, CD, averías.

Los diagnósticos en línea estarán en capacidad de identificar, localizar y reportar las siguientes fallas:

a) Fallas permanentes en las cuáles un componente del sistema o algún módulo sufre una falla irreversible.
b) Fallas temporales al azar en los cuáles los defectos sucesivos están interrelacionados.
c) Fallas intermitentes donde aparecen funcionamientos defectuosos con algún grado de periodicidad.
d) Fallas de circuitos de detección de escrutinios y fallas.
e) Fallas de memoria, todas las funciones RAM y ROM.
f) Fallas de microprocesador.
g) Fallas de comunicación.
h) Fallas de direccionamiento.
i) Fallas de módulo de entrada y salida.
j) Fallas de suministro de energía.
k) Problemas de sensor de campo.
l) Circuitos de I/O (entradas/salidas) abiertos o en corto circuito.
m) Alambres interrumpidos, bobinas de relé, contactos, terminales y fusibles de I/O abiertos.

El SIS puede presentar los siguientes estados:

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

Estado de falla peligrosa: Estado en que el SIS esta en la condicion de no actuar ante una posible demanda del sistema o falla en demanda, es decir, se presenta cuando existe el evento iniciador y la SIF no se ejecuta por una falla.
Las fallas que se pueden presentar en los estados de falla segura y peligrosa en el SIS se clasifican además en:

Fallas detectadas: Al ocurrir revelan su presencia o pueden ser detectadas mediante diagnóstico. Cuando se detecta, el proceso se lleva a una condición segura, de modo que la falla no genere una situación de peligro.

Falla no detectada:
- No revelan su presencia o permanecen en estado latente.
- Se busca disminuirlas aumentando la capacidad de diagnóstico, el cual puede ser automático o manual.

El concepto de falla segura para plantas y equipo es el retorno al estado seguro en caso de falla del sistema lógico de protección, sensores, actuadores o fuentes de alimentación. Este requerimiento debe realizarse des energizando para disparo las salidas del SIS.

El autodiagnóstico del sistema no logra descubrir el elemento fallado en el SIS. La falla se mantiene oculta y solo se puede descubrir a través de la inspección y prueba periódica del sistema.

Hay una variedad de nombres y definiciones para una causa común. En esencia, un fallo de causa común se puede definir como un factor de estrés individual o el fracaso que afecta a varios elementos o partes de un sistema. Una forma de referirse a este tipo de problemas es el "factor beta." Este es el porcentaje de todos los fallos detectados en una "sección" o "corte" de un sistema redundante que podría afectar a componentes idénticos, y que todo el sistema falle.

Los fallos sistemáticos, también llamado fallas funcionales, el impacto de un sistema completo y por lo tanto a veces clasificado como fallos de causa común. Ejemplos de fallas sistemáticas por lo general los errores humanos en el diseño, mantenimiento, modificación e instalación del hardware, errores de software e interacción humana. Sin embargo, el calor, las vibraciones, y otros factores externos todavía puede tenerse en cuenta en la definición. Tales fallas pueden

afectar un sistema redundante o no redundante. Este tipo de fallas son más difíciles de cuantificar.
El diagnostico implica los siguientes conceptos:

- **Averías:**

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

λd = λdd + λdu
λs = λsd + λsu
λ= λdd + λdu + λsd + λsu

λ = cuota de averías total.
λdd (dangerous detected) = Cuota de averías detectadas peligrosas;
λdu (dangerous undetected) = Cuota de averías no detectadas peligrosas;
λsd (safe detected) = Cuota de averías detectadas seguras;
λsu (safe undetected) = Cuota de averías no detectadas seguras.

- **SFF:**

La SFF representante las fracciones de avería que conducen a un estado seguro y aquellas detectadas por medidas diagnosticas que tienen como efecto una acción segura definida.

La fracción de falla segura SFF, es suministrada por el proveedor de la instrumentación, y es calculada para cada dispositivo, componente o subsistema utilizado en cada SIF. La ecuación para calcular la SFF es:

$$SFF = 1 - \frac{\lambda du}{\lambda du + \lambda dd + \lambda su + \lambda sd}$$

$$SFF = 1 - \frac{\lambda du}{\lambda}$$

- **HTF:**

La tolerancia a fallos del hardware es la capacidad de un componente o subsistema de continuar para poder llevar a cabo la necesaria función instrumentado de seguridad en la presencia de uno o más fallos peligrosos en el hardware. Una tolerancia a fallos del hardware de uno (1) significa que hay, por ejemplo, dos dispositivos y la arquitectura es tal que el fallo peligroso de uno de los dos componentes o subsistemas no impide que se produzca la acción de seguridad. Dependiendo de la aplicación, la tasa de fallo de un componente y el intervalo de prueba, una redundancia adicional puede ser requerida para satisfacer las SIL de la SIF. Para el controlador lógico, la tolerancia a fallos de hardware mínima será como se muestra en la tabla 2.

SIL	Tolerancia a fallos de hardware mínima		
	SFF< 60%	SFF 60% a 90%	SFF>90%
1	1	0	0
2	2	1	0
3	3	2	1
4	Aplicación de requerimientos especiales(IEC 61508)		

Tabla 2. Tolerancia a fallas del Controlador

Para todos los subsistemas, por ejemplo, sensores, elementos finales y controladores lógicos, la tolerancia a fallos de hardware mínimos se muestran en la Tabla 3, siempre que el modo de falla dominante es el estado seguro o las fallas peligrosas se detectan, de lo contrario la tolerancia a fallos se incrementa en uno.

SIL	Tolerancia a fallos de hardware minima
1	0
2	1
3	2
4	Aplicación de requerimientos especiales (IEC 61508)

Tabla 3. Toleracia a fallas HW

Para determinar si el modo de falla dominante es el estado de seguridad es necesario tener en cuenta:

- La conexión del proceso del dispositivo;
- Uso de la información de diagnóstico del equipo para validar la señal de proceso;
- utilizar el comportamiento a prueba de fallos inherentes (por ejemplo, la señal cero, la pérdida de potencia resulta en una caja fuerte del Estado).

La norma IEC 61508 clasifica los elementos o subsistemas en dos tipos: A y B.

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

- Los modos de falla de todos los componentes que lo constituyen están bien definidos.
- El comportamiento del subsistema bajo condiciones de falla puede ser completamente determinado.
- Para el subsistema existen suficientes datos de fallas confiables, extraídos de experiencia en campo.

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

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

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

$$DC = \frac{\lambda \mathrm{dd}}{\lambda \mathrm{d}}$$

Arquitecturas
La arquitectura del sistema indica el arreglo e interconexión de los componentes o módulos del SIS. La arquitectura del SIS tiene un impacto directo en la integridad global de seguridad, influenciando asimismo en su confiabilidad. Esta debe de aplicarse a fin de ampliar la integridad de seguridad o mejorar la tolerancia a fallas, el diseñador debe determinar los requerimientos de redundancia para lograr el SIL y la confiabilidad requerida de todos los componentes del SIS como son sensores, controladores lógicos y elementos finales de control.
La selección de la arquitectura del SIS debe incluir las siguientes etapas:

a) Selección de diseño energizado o des energizado para disparo.
b) Selección de redundancia idéntica o diversa para los sensores, controladores lógicos y elementos finales del control del SIS.
c) Selección de redundancia para las fuentes de potencia y de suministro de energía al SIS.
d) Selección de los componentes de la interface con el operador.
e) Selección de las interfaces de comunicación entre el SIS y otros subsistemas.

Las Estructuras de Votación de los Controladores se relacionan con los distintos niveles de seguridad. “NooM” significa: que N canales 1 de los M disponibles deben votar por un disparo de la parada de emergencia para que esta sea ejecutada. Un sistema será Redundante cuando dos o más Canales ejecutan la misma función.

“Canal” entendemos al conjunto Sensor-Entrada-Lógica Salida-Actuador que realiza una determinada función.

La letra “D”’, utilizada en la descripción de algunas de las arquitecturas de votación, indica que el Diagnóstico es utilizado para alterar las decisiones de paro; en aquellas que no tienen esta indicación, el diagnóstico se utiliza sólo para generar alarma.

Lógica de votación **MooN** (M out of N)
M: indica cuantos componentes operan normalmente.
N: indica con qué frecuencia se desarrolla la SIF (redundancia).

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

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

Arquitectura 1oo1:
Esta arquitectura consiste en un solo elemento, donde cualquier falla segura des energiza la salida y cualquier falla peligrosa impide que una señal de alarma válida no sea procesada correctamente. Esta arquitectura no es tolerante a fallas ni posee modo de protección de falla. La ventaja del sistema 1oo1 es que tiene el costo inicial de instalación más bajo de todas las configuraciones. En la figura 2 se presenta el diagrama esquemático de un logic solver con arquitectura de votación 1oo1.

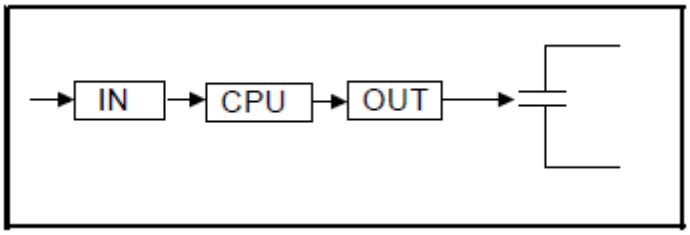

Figura 2. Arquitectura 1oo1

Arquitectura 1oo2:
Esta arquitectura consiste en dos elementos conectados en serie en donde cada elemento puede comandar un disparo a la salida. Por lo tanto, debe haber una falla peligrosa en ambos elementos antes de que una señal de alarma válida no pueda ser procesada. El sistema ofrece una baja probabilidad de moverse al estado de falla peligrosa, pero incrementa la probabilidad de moverse al estado de falla segura. Se asume que cualquier prueba de diagnóstico sólo reporta las fallas encontradas y no cambia el estado o la votación de la salida. Las ventajas del sistema 1oo2 es que presenta buena inmunidad en contra de las fallas ocultas y, por lo tanto, una mayor disponibilidad de seguridad que un diseño 1oo1. Su desventajas son: mayor costo que el diseño 1oo1 y mayor susceptibilidad a disparos en falso (una señal falsa en cualquiera de los elementos resultará en un disparo del sistema). En la figura 3 se presenta el diagrama esquemático de un logic solver con arquitectura de votación 1oo2.

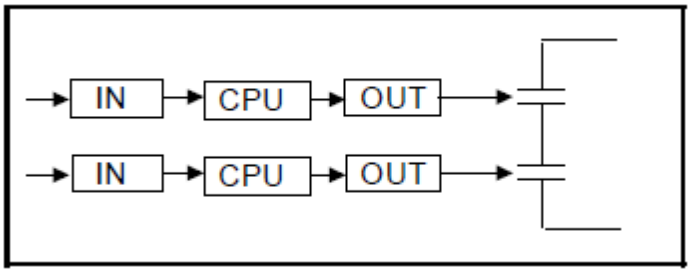

Figura 3. Arquitectura 1oo2

Arquitectura 2oo2:

Esta arquitectura consiste en dos elementos conectados en paralelo en donde ambos elementos tienen que demandar un disparo antes que un disparo pueda llevarse a cabo. Se asume que cualquier prueba de diagnóstico sólo reporta las fallas encontradas y no cambia el estado o la votación de la salida. El diseño 2oo2 presenta la mejor inmunidad contra los disparos en falso (es usado principalmente en sistemas de control de producción en el cual el costo de una parada del proceso es extremadamente alta). Tiene como desventaja que una falla oculta o no de un elemento puede impedir un disparo válido desde el otro elemento. Por ejemplo, si los dos elementos necesitan detectar una condición de disparo y uno de los sensores ha fallado de forma tal que nunca producirá una señal de disparo, este elemento fallado impedirá la ocurrencia de un disparo válido. La arquitectura 2oo2 es buena para prevenir disparos en falsos pero es una arquitectura pobre para sistemas de seguridad. En la figura 4 se presenta el diagrama esquemático de un logic solver con arquitectura de votación 2oo2.

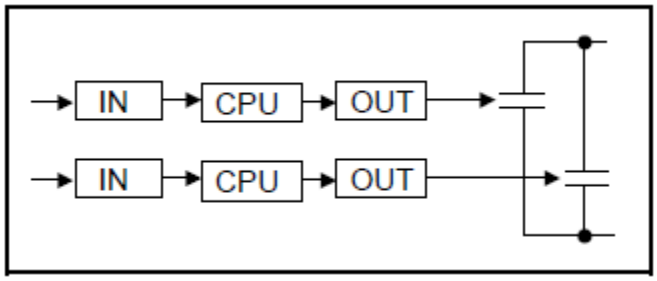

Figura 4. Arquitectura 2oo2

Arquitectura 2oo3

Esta arquitectura consiste en tres elementos conectados en paralelo con un arreglo de votación mayoritario para las señales de salida, en donde el estado de salida no cambia si sólo un canal entrega un resultado diferente al de los otros dos canales. Se asume que cualquier prueba de diagnóstico sólo reporta las fallas encontradas y no cambia el estado o votación de la salida. El diseño 2oo3 es una arquitectura robusta en contra de las fallas ocultas y disparos en falso. Un elemento puede fallar, sin iniciar un disparo en falso, y los dos elementos restantes continúan ofreciendo protección contra una condición de disparo válida. El diseño 2oo3 también ofrece la capacidad de colocar un elemento fuera de servicio para prueba o mantenimiento mientras mantiene el resto de la protección activa. La habilidad de comparar las señales de tres elementos incrementa

ampliamente el diagnostic coverage (DC). La desventaja del diseño 2oo3 es que tiene el costo inicial más alto. El espacio y las conexiones necesarias para instalar tres elementos son mayores que el que se necesita para instalar las configuraciones 1oo1 o 1oo2. Aunque el costo inicial de tres elementos es alto, el costo típico global del ciclo de vida es sustancialmente menor debido a la eliminación o reducción de los disparos en falsos. En la figura 5 se presenta el diagrama esquemático de un logic solver con arquitectura de votación 2oo3.

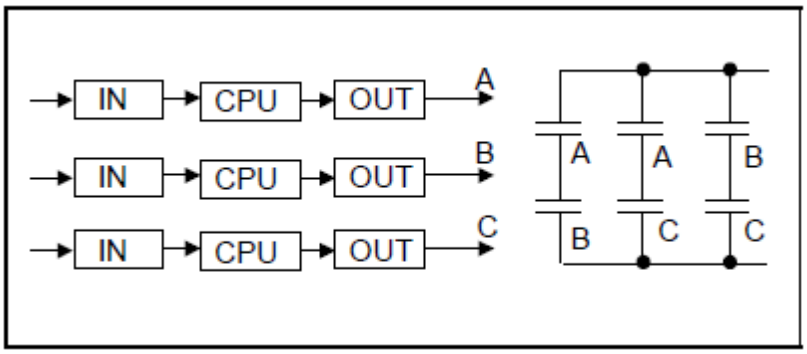

Figura 5. Arquitectura 2oo3

Arquitectura 1oo1D

Esta arquitectura consta de un solo elemento con una salida controlada por diagnóstico. Este sistema representa un uso de gran valor para aplicaciones de seguridad. En algunos sistemas la salida controlada por diagnóstico es un watchdog timer externo, que controla una salida serial independiente que lleva al sistema a un estado seguro cuando el timer no es actualizado. En sistemas más avanzados, el diagnóstico integrado controla una salida en serie independiente que lleva al sistema a un estado desenergizado cuando una falla dentro del módulo es detectada. En este modelo, el diagnóstico permite que una falla peligrosa detectada sea convertida en una falla segura. En la figura 6 se presenta el diagrama esquemático de un logic solver con arquitectura de votación 1oo1D.

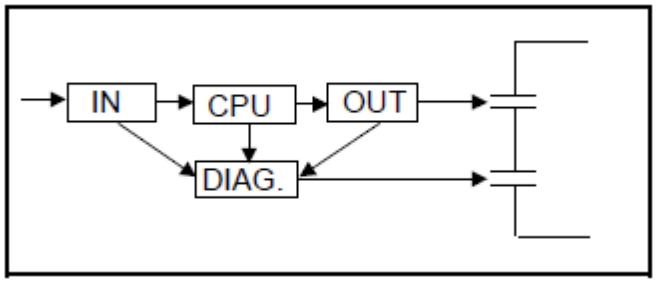

Figura 6. Arquitectura 1oo1D

Arquitectura 1oo2D:

Esta arquitectura consiste en dos configuraciones 1oo1D colocados en un estilo 2oo2. Debido a que 1oo1D protege contra las fallas peligrosas, dos unidades son cableadas en paralelo para proteger contra las fallas seguras. Adicionalmente, con esta configuración, si las pruebas de diagnóstico en cualquiera de los elementos

detectan una falla, entonces la votación de salida es adaptada de forma tal que el estado de salida del sistema sigue lo indicado por el otro elemento. Si las pruebas de diagnóstico encuentran fallas en ambos elementos entonces la salida se coloca en el estado de disparo. En la figura 7 se presenta el diagrama esquemático de un logic solver con arquitectura de votación 1oo2D.

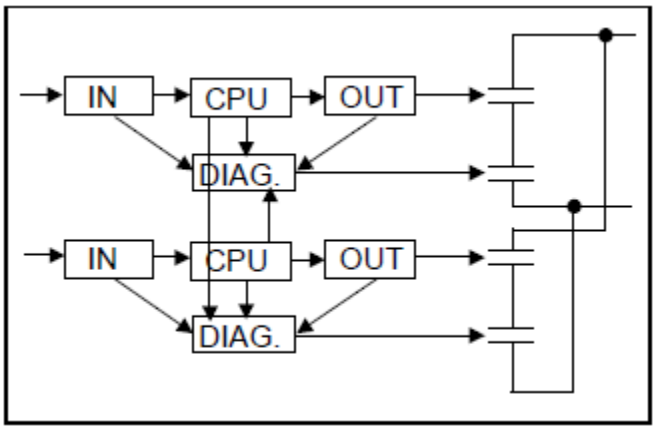

Figura 7. Arquitectura 1oo2D

Arquitectura 2oo2D

Esta arquitectura es básicamente igual a la arquitectura 1oo2D pero con menos líneas de diagnóstico, como se puede apreciar en la figura 8 en la cual se presenta el diagrama esquemático de un logic solver con arquitectura de votación 2oo2D.

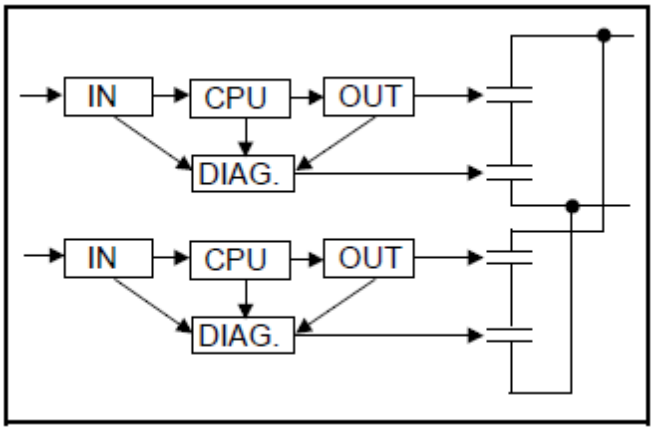

Figura 8. Arquitectura 2oo2D

BIBLIOGRAFIA

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

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

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

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

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

[6]. César Cassiolato. “Fiabilidad de los Sistemas de Medición y Sistemas Instrumentados de Seguridad”. SMAR Equipamentos Industriais Ltda. Disponible en: http://www.smar.com/newsletter/marketing/index186.html. Acceso en Mayo 5 de 2012]