

SISTEMAS DE PROTECCION SEGURA PARA PROCESOS INDUSTRIALES

Artículo SS-106-02 Septiembre de 2001

por Ing. **Roberto Fernández Blanco**
FUNCTIONAL SAFETY EXPERT

1- INTRODUCCIÓN

El objetivo de la ciencia de la Seguridad, la Prevención y la Protección apunta a la elaboración de técnicas que permitan implementar medios y mecanismos que garanticen una efectiva **Reducción de los Riesgos (Risk Reduction)** de siniestros a niveles apropiados de seguridad (**Negligible and Acceptable Residual Risks**).

En procesos donde los costos de implementación para alcanzar el nivel aceptable de riesgo pueden llegar a ser incompatibles con los costos de inversión y de operación de la planta (pudiendo hacerlos inviables), se acepta una reducción de los riesgos hasta un nivel "razonable o tolerable" conocido como **ALARP** (As Low As Reasonably Practicable) resultante de una muy cuidadosa evaluación.

El propósito esencial es hacer viable la operación de una planta dentro del objetivo de proteger la salud y la vida de las personas (tanto de la planta como de la comunidad), el medio ambiente, los bienes de la comunidad y de producción, la capacidad productiva de la planta y su plena y eficiente continuidad operativa.

Visto desde el ángulo opuesto (que suele ser el más convincente) se **trata de evitar** los diferentes tipos de costos y gastos que se sumarán a causa del incidente, tales como gastos médicos, legales e indemnizatorios por internaciones, curas, tratamientos, rehabilitaciones, convalecencias, discapacidades, invalidez o muerte, o bien los resultantes por destrucción parcial o total de bienes ajenos y propios. Entre estos últimos estarán afectados los medios de producción, de almacenamiento, de servicios complementarios, pérdida de materia prima, de productos intermedios, de productos terminados, etc.

A todo esto se sumará la pérdida total o parcial de la capacidad productiva con sus consecuencias por lucro cesante, incumplimientos, compensaciones, penalidades, indemnizaciones y pérdida de clientes y de mercado.

Por añadidura se sumarán los costos de reparación, reposición, verificación total de lo que se salvó, de lo que se reparó y de lo que se repuso como nuevo, ordenamiento, adecuación, puesta a punto, etc.

“El sentido común y la experiencia recomiendan prevenir antes que curar.”

2- ACTITUD ALERTA

Una actitud confiada, desprevenida y aletargada caracteriza muchos de los aspectos de nuestra vida cotidiana cuando nos habituamos a circunstancias que se suceden con cierta monotonía y sin riesgos aparentes.

Esta forma de comportamiento se incorpora a nuestras vidas como una predisposición de conducta que relaja nuestros sentidos, que adormece nuestros reflejos, que nos torna desatentos y descuidados y que debilita nuestra capacidad de alerta para anticiparnos, prevenir y protegernos frente a acontecimientos peligrosos.

Es parte de la misma conducta laza el calificar de imprevisto, inesperado y/o impensado (con la connotación acentuada como algo imposible de anticipar o imaginar) a todo acontecimiento que "nos toma por sorpresa precisamente por no haberlo previsto".

Es importante incorporar como mecanismo de conducta un "estado de actitud alerta" respecto de la posibilidad y probabilidad de riesgos reales que forman parte de nuestra vida cotidiana, en particular cuando nos desempeñamos en el medio industrial.

En este sentido es probable que, por sus características, mucho nos ayude el tener presente el siguiente triste accidente ocurrido hace unos diez años:

“Una familia compuesta por ambos padres y dos niños estaban en su auto esperando que el tren terminara de pasar para cruzar las vías y continuar su camino.

Al levantarse las barreras habilitando el paso, el padre avanzó con el auto tomando la precaución de confirmar, “por si acaso”, que no estuviera viniendo un tren del lado contrario.

Cuando estaban atravesando las vías del tren que acababa de pasar fueron arrollados por el último vagón de dicho tren que se había desprendido unos trescientos metros atrás y continuaba retrasadamente su carrera por inercia. Solo se salvó, pese a sus heridas, uno de los niños”
¿Impensable? ¿Imprevisible? Nada de eso. Solamente tan poco probable que naturalmente no se nos ocurre pensar en ello”.

Antes de que esto sucediera quizás hubiera parecido una exageración el estar alertas respecto de un posible “vagón desprendido” que, retrasado, nos alcanzara justo en el momento en que confiadamente estamos cruzando las vías.

En el orden industrial es, al día de hoy, una obligación inexcusable el adoptar el nivel apropiado de precauciones y/o protecciones contra los riesgos de un posible “vagón desprendido”.

3- PELIGROS Y RIESGOS

En todo proceso industrial se dan situaciones de peligro latente (Hazards) capaces de derivar en acontecimientos peligrosos (Hazardous Events) de distinta magnitud.

Se llama riesgo (Risk) a la probabilidad de que dicho acontecimiento peligroso (Hazardous Event) resulte en un accidente o incidente con daños y/o lesiones de diversa magnitud.

La evaluación y/o cuantificación del riesgo (Risk Assessment) resulta de la combinación de dos factores:

- (a) La probabilidad de que se produzca el incidente (Risk Probability), y
- (b) La magnitud o severidad de sus consecuencias (Risk Severity).

- La Probabilidad de Ocurrencia del accidente se ha tabulado en cinco categorías: (1-Improbable, 2- Remota, 3-Ocasional, 4- Probable, 5- Frecuente).
- La Severidad o magnitud de las Consecuencias también se ha tabulado en otras cinco categorías (I-Despreciable, II-Menor, III-Seria, IV-Severa, V-Catastrófica).

El Nivel de Riesgo Global (Overall Risk Level) resulta de una matriz que combina ambos factores y conduce a tres niveles de riesgos típicos para los procesos industriales (bajo, medio y alto) al que se ha incorporado además un cuarto nivel por encima de los anteriores para su aplicación en áreas nucleares y aeroespaciales.

Cada uno de estos cuatro niveles requiere de una garantizada calidad y performance de los Equipos y Sistemas de Seguridad a ser incorporados en el proceso para obtener la necesaria Reducción del Riesgo, por eso se los ha bautizado como Safety Integrity Levels, siendo este concepto conocido en la jerga de seguridad por sus iniciales “SIL”. (SIL1-Riesgo Bajo, SIL2- Riesgo Medio, SIL3-Riesgo Alto, SIL 4-Riesgo Especial).

4- METODOS DE ANALISIS Y EVALUACION DE RIESGOS

Al diseñarse un proceso con posibles situaciones de peligro debe realizarse un cuidadoso y metódico análisis para determinar las “consecuencias” de todas las posibles “desviaciones” o apartamientos de las condiciones operativas previstas como normales. Este análisis de situaciones Peligrosas (Hazards) y de dificultades Operativas se conoce como HAZOP (Hazards and Operability Analysis) y permite obtener conclusiones que conduzcan a una revisión del diseño básico del

proceso para facilitar su operatividad, mejorar su eficiencia productiva y hacer el proceso lo más inherentemente seguro que sea posible (Inherent Safety).

Superada la etapa del HAZOP e identificados los peligros (Hazards) de envergadura que persisten pese a las mejoras introducidas como resultantes del HAZOP, se pasa a una segunda etapa específica de análisis de estos peligros, Hazard Analysis o HAZAN, para evaluarlos y finalmente cuantificarlos (Risk Analysis, Risk Assessment, Probabilistic Risk Assessment , Quantitative Risk Assessment).

Existen varios otros métodos independientes y/o complementarios de identificación y cuantificación de riesgos tales como FMEA (Failure Mode and Effect Analysis), FTA (Fault Tree Analysis), ETA (Event Tree Analysis) , WHAT-IF Analysis, LOPA (Layers of Protection Analysis), cada uno de ellos con particulares beneficios según su aplicación a distintos tipos específicos de procesos y componentes.

Una vez identificados los peligros capaces de provocar un acontecimiento riesgoso y evaluados en su probabilidad de ocurrencia y en su potencial de daño (lesiones, muertes, destrucción y otras consecuencias), queda definido el nivel SIL, esto es, el “requerimiento mínimo de nivel de integridad segura” exigible al sistema y/o plataformas de protección para reducir los riesgos al apropiado nivel de seguridad (Negligible Risk Level , Acceptable Risk Level o ALARP).

5- NORMAS IEC 61508 y 61511

Una larga y penosa historia de catástrofes en procesos peligrosos insuficientemente protegidos por desconocimiento y/o exceso de confianza, o mal protegidos por la aplicación de técnicas incorrectas, creó la necesidad de emitir un paquete de recomendaciones que tomaron la forma de Norma o Standard de uso forzoso.

Las Normas IEC 61508 e IEC 61511 “Functional Safety of Electrical/ Electronic/ Programmable Electronic Safety Related Systems” imponen rigurosas condiciones de seguridad-de uso mandatorio- en la integración de equipos y sistemas de protección, que deben ser estrictamente observadas por tres razones fundamentales:

- Porque tendrá Ud. la más adecuada protección para salvaguarda de su personal (Ud. incluido), de sus bienes y de su negocio,
- Porque ninguna compañía Aseguradora sería va a aprobar una instalación que no haya implementado sus plataformas de Reducción de Riesgos en un todo de acuerdo con las exigencias de esta Norma (de no hacerlo así quedaría involucrada en las responsabilidades), y
- Porque todo accidente, incidente o siniestro que se demuestre indebidamente protegido por la no observancia de la Norma, enfrentará al usuario con serios problemas legales.

La Norma IEC debe ser cumplida rigurosamente y, tal como la misma lo impone, los sistemas a ser utilizados para reducir el riesgo operativo de un proceso a nivel tolerable deben garantizar su capacidad de adecuarse (o superar) al nivel de seguridad SIL reclamado por dicho proceso.

A tal efecto la Norma IEC 61508 ha impuesto el uso de equipos electrónicos programables de diseño especial conocidos como PES (Programmable Electronic Safety Controllers) los que deben estar rigurosamente aprobados por alguno de los Institutos Internacionales de Aplicación (TÜV-Technischer Überwachungs-Verein y/o FM Global-Factory Mutual Global) como aptos para su aplicación en la protección de procesos del específico nivel SIL requerido.

Es de simple sentido común el comprender que un muy buen equipo para ciertos tipos de aplicaciones puede ser absolutamente inadecuado para aplicaciones en procesos de riesgo.

Pero no es siempre evidente, tal como sucede con el clásico y bien ponderado PLC (Programmable Logic Controller) cuyo uso está “expresamente no recomendado” (casi prohibido) para aplicaciones de seguridad para todos los niveles SIL, aun incluso con sus variantes mejoradas con redundancias

de módulos de entradas/salidas, con Unidad Central Procesadora con Back Up, con external watch dogs, hardwired parallel trip circuits, feedbacks de outputs sobre inputs con análisis de discrepancias, y otros medios y/o mecanismos incorporados con el propósito de apuntar a una mayor garantía de continuidad operativa segura.

“Concretamente los PLC standards no permiten implementar sistemas con el grado de seguridad necesario para ser aprobados y clasificados como aptos para operar en ningún Nivel de exigencia SIL.”

Al no cumplir con las exigencias de la Norma no pueden ni deben ser usados como equipos de protección segura.

Sin embargo, y a pesar de todo el conocimiento actual sobre el tema de seguridad y de las regulaciones vigentes, son aun numerosos los casos de empresas que continúan operando con (y, lo que es peor, aún aceptando) equipos de aparente gran confiabilidad por sus muchas virtudes pero portadores de un invisible bajo nivel de seguridad (alto riesgo).

Vale la pena mencionar que la NFPA, en relación con sistemas de protección para calderas, recomienda:

“Es vital que el diseñador del sistema de seguridad esté totalmente familiarizado con las bondades y prestaciones del equipo a microprocesadores a utilizar, pero muy fundamentalmente con las flaquezas y posibilidades de fallas del mismo”.

Para diseñar un sistema seguro lo esencial es prever los peligros a que pueden conducir sus fallas propias, en particular sus fallas silenciosas e invisibles.

Por su parte Factory Mutual en su Approval Standard Nbr 7605 es terminante, “deben observarse las IEC 61508 y 61511”.

A la pregunta ¿como puede un usuario “estar seguro” de que el sistema de seguridad SIS (Safety Instrumented System) que está comprando “es realmente seguro”?, la Norma responde:

**Defina el nivel “SIL de Reducción de Riesgo” que corresponda a “cada una de las funciones de seguridad SIF” (Safety Instrumented Function) requeridas por su proceso e instrumento su sistema SIS con equipos PES-LS (logic solvers) aprobados por TÜV o FM como aptos para ser usados en el mas alto Nivel SIL resultante, completando la implementación de cada SIF con componentes (sensores, actuadores, etc) cuyos Failure Rate (o SIL) individuales permitan integrar la configuración que “satisfaga el nivel de integridad SIL exigido a cada lazo de seguridad SIF”. (Ver Art. SN-042 del mismo autor en sitio web).

Si su proceso exige algunas Funciones de Seguridad con nivel SIL 3 de reducción de riesgo, Ud. no puede ni debe protegerse con un equipamiento y/o configuración/implementación aprobado para un nivel inferior, por ejemplo uno apto para Nivel SIL 2.

Como comentario marginal cabe agregar que los procesos industriales con mayor grado de facilidad o peligrosidad para provocar deflagraciones, explosiones, radiaciones intensas, contaminación tóxica, etc, con daños y lesiones más o menos importantes, requieren varias Funciones de Seguridad que caen forzosamente en las categorías o Niveles SIL 2 y SIL 3.

6- PLATAFORMAS DE PROTECCIÓN (LAYERS OF PROTECTION)

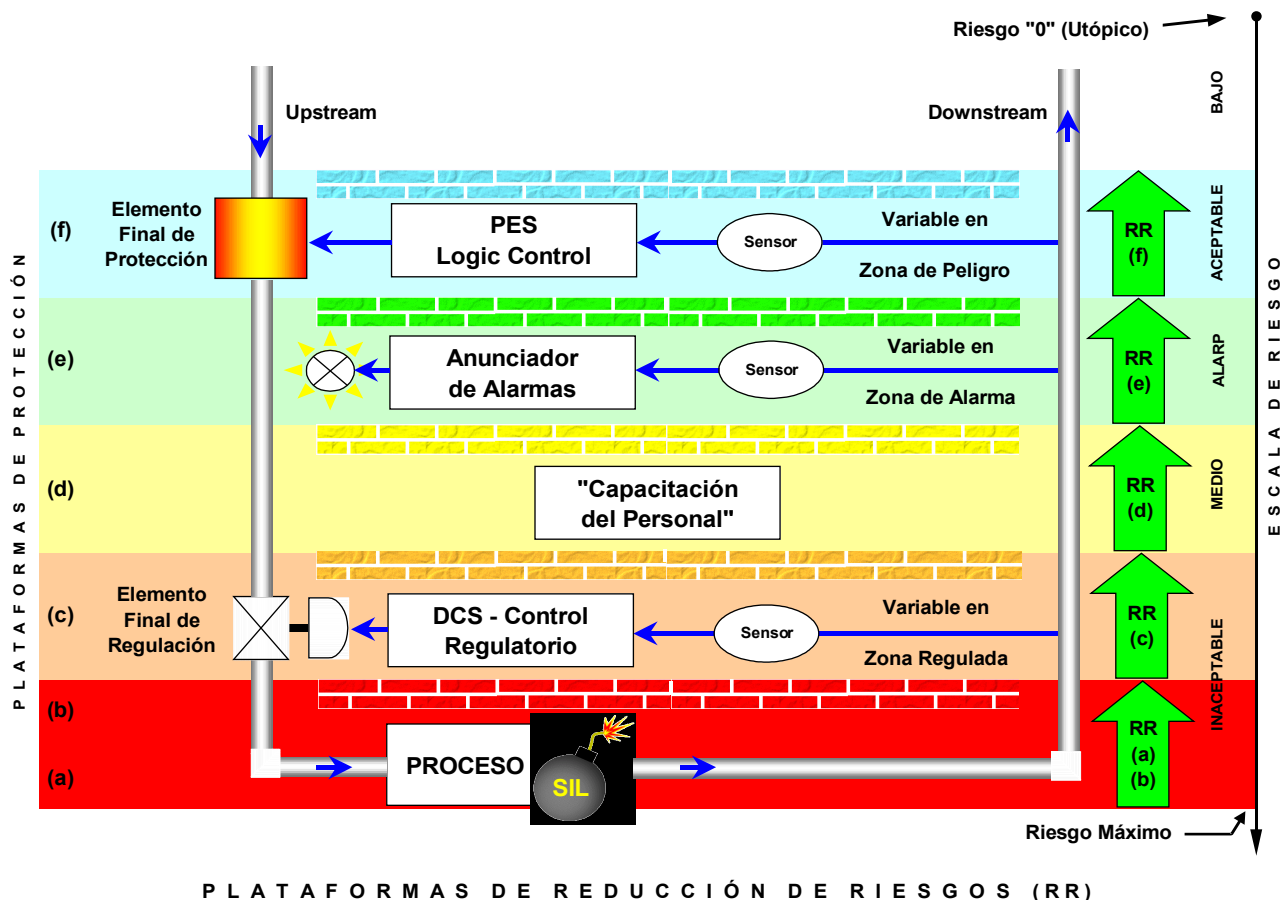
Definido un proceso, decidida su instalación, establecidos sus requerimientos operativos e identificadas sus situaciones de peligro (HAZARDS), se deben diseñar y disponer (como capas de cebollas) las sucesivas plataformas de medición, control, alarmas, protección, contención y mitigación, para obtener una operación eficiente en condiciones de alta seguridad (adecuada reducción del nivel de riesgo).

Estas etapas y plataformas de Reducción de Riesgo (R R) incluyen:

- RR(a) Análisis HAZOP, HAZAN y otros que correspondan para evaluar y cuantificar el riesgo.

- RR(b) Adecuación del diseño del proceso a la configuración de máxima seguridad inherente posible . Determinación del SIL.
- RR(c) Identificación de las variables del proceso a ser reguladas y supervisadas, determinación de sus valores óptimos de operación, sus rangos, sus bandas de operación y sus Límites de Regulación.
- Estructuración del Sistema de lazos de Medición y de Control Regulatorio.
- RR(d) Implementación de las instrucciones para el personal para una operación eficiente y segura incluyendo las instrucciones para situaciones de emergencia.
- RR(e) Determinación de los valores Límites de Alarma de aquellas variables que puedan escaparse de las bandas de regulación automática y , en función de ellos, implementar una Plataforma de Alarmas para alertar y reclamar la intervención del personal operativo.
- RR(f) Definición de los parámetros de seguridad y sus valores Límites de Seguridad para cada Función o Lazo de Protección o Seguridad, los que, en caso de ser superados, deberán disparar el accionamiento de una lógica automática de protección o Sistema Instrumentado de Seguridad (SIS) (Safety Instrumented System) que deberá ser implementado con componentes aptos (y en lo posible aprobados por TUV y/o FM) para proteger el proceso de acuerdo con el nivel SIL que este exige por cada SIF (Safety Instrumented Function).
- Este sistema SIS (PESS, Programmable Electronic Safety System según la IEC 61508) se integra como una cadena independiente de seguridad cuyo primer eslabón es el sensor o detector (generalmente de campo) de la variable peligrosa cuya desviación o apartamiento por fuera de los Límites de Seguridad puede dar lugar al siniestro.
- Este eslabón transfiere su demanda de protección a través del eslabón PESC (Programmable Electronic Safety Controller) o PES-LS (Programmable Electronic Safety-Logic Solver) hasta lograr que el último eslabón de la cadena (actuador final de protección, válvula de bloqueo, etc) ejecute la acción protectora requerida sobre el proceso.
- RR(g) Implementación de los mecanismos directos de protección física y mecánica (discos de ruptura, válvulas de alivio, drenajes rápidos, etc).
- RR(h) Plataforma externa de contención tales como diques, fosas de derrame, etc.
- RR(i) Acciones de emergencia y mitigación para combatir, atenuar la severidad del incidente, limitar los daños y prevenir nuevos peligros subyacentes.
- RR(j) Procedimientos de evacuación y escape.

Una vez implementadas estas etapas y plataformas de Protección “se sugiere como muy conveniente un nuevo análisis HAZOP / HAZAN” para asegurarse de que las mismas, a la vez que aportan protecciones y seguridades no están simultáneamente introduciendo nuevos peligros. El objeto de interés específico de este artículo se limita al alcance de la Reducción de Riesgo RR(f), última frontera de contención del peligro “dentro” del proceso.



7- REDUCCIÓN DEL RIESGO

Cada una de las plataformas de protección que se incorpora a un proceso peligroso produce una específica Reducción de los diferentes Riesgos que es función de dos factores:

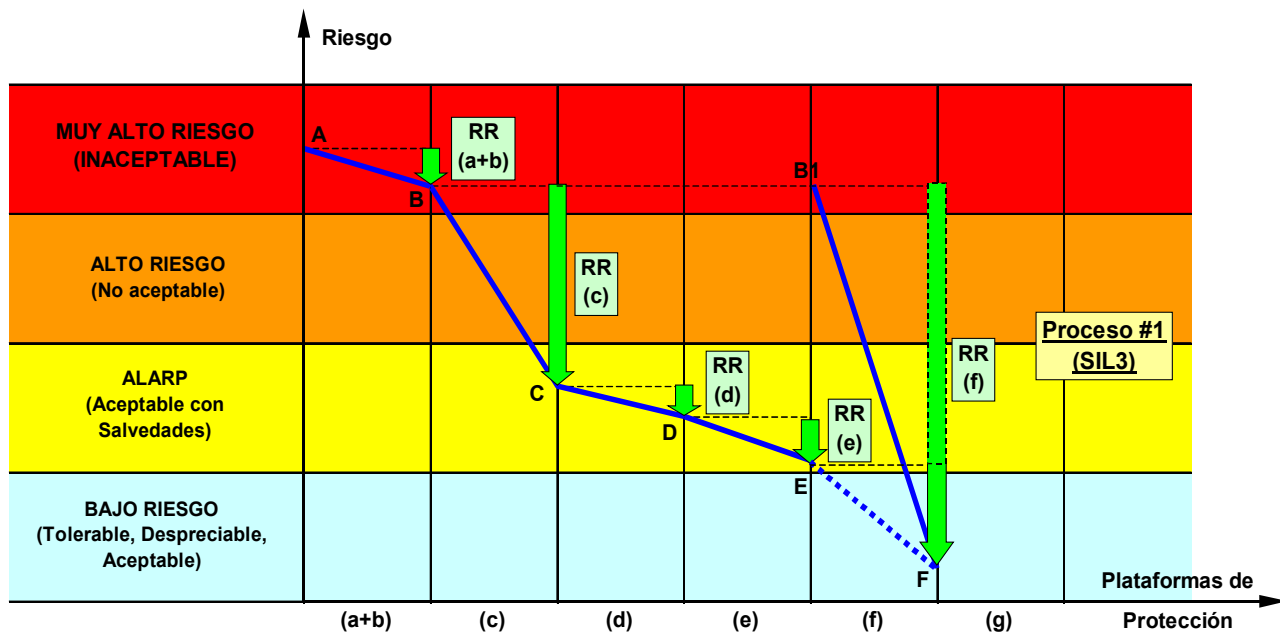
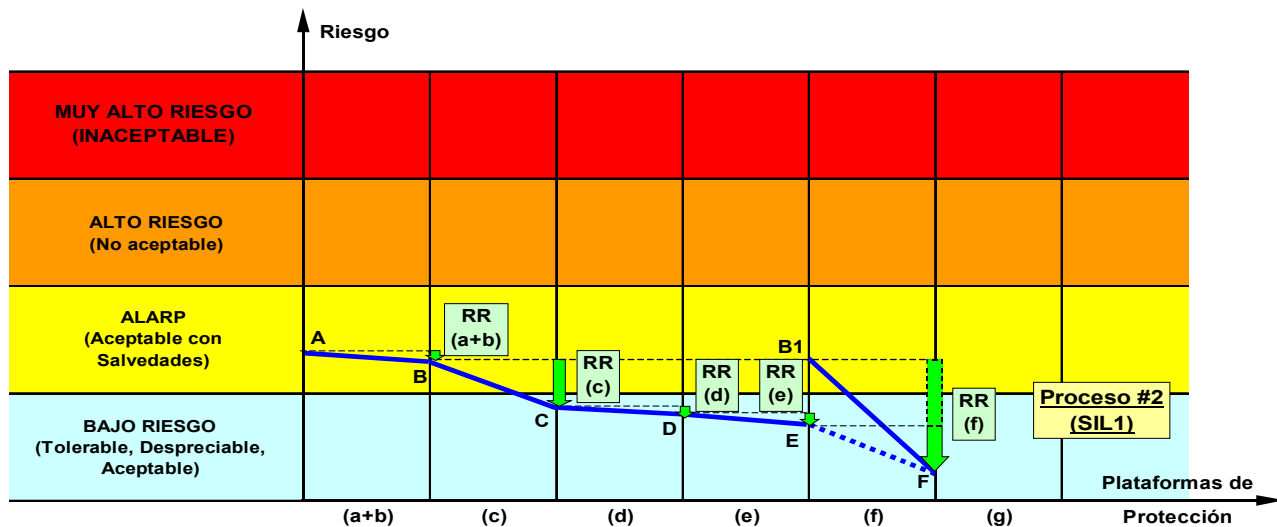
- Del tipo y características del proceso, y
- II. De la calidad del diseño y de la implementación de cada plataforma de protección.

Un proceso continuo de alto nivel de riesgo intrínseco requerirá, muy probablemente, de una mayor complementación de plataformas de protección de características más complejas y elaboradas.

Se ha dado el caso de procesos donde el replanteo resultante del análisis HAZOP y/u otros (etapas o plataformas (a) +(b) en nuestro listado) han permitido modificar el proceso en su esencia haciéndolo más inherentemente seguro y, en consecuencia, simplificándolo sustancialmente.

Es este el primer paso a dar en el diseño de todo tipo de proceso.

Los gráficos que siguen ilustran acerca de los saltos de Reducción de Riesgo en dos tipos de procesos, el primero con Funciones de Seguridad de alto riesgo inherente SIL3 (riesgo inicial en el punto "A")-que exige la participación de casi todas las plataformas de contención enumeradas en el capítulo anterior. (En el gráfico nos extendemos hasta la plataforma (f) – Sistema de Seguridad - por ser este nuestro motivo de interés)- y el segundo un proceso con Funciones de Seguridad de bajo riesgo inherente de exigencia SIL1.



El análisis de estas curvas de Reducción de Riesgo nos muestra que:

- i. Con la aplicación de las plataformas (a) +(b) se obtiene una Reducción de Riesgo del nivel "A" al nivel "B", representada por la flecha o vector RR (a+b),
- ii. La plataforma (c), implementada con el Sistema de Regulación, hace bajar el riesgo al nivel del punto "C", representado por el vector RR(c). (Se advierte que no siempre el Sistema de Regulación colabora plenamente en la Reducción de los Riesgos).

- iii. De manera similar una buena capacitación del personal aumenta la seguridad haciendo bajar el riesgo al punto "D", vector RR(d), y su complementación con un adecuado sistema de alarmas contribuye aún más a aumentar la seguridad reduciendo el riesgo al punto "E", vector RR(e).
- iv. Especial atención merece el efecto de la plataforma implementada con el Sistema Instrumentado de Seguridad (SIS o PESS, Programmable Electronic Safety System) que reduce el riesgo hasta el nivel del punto "F".

Estos gráficos muestran dos vectores, uno que resulta del aumento de seguridad que va del punto "E" al punto "F" y otro que resulta del salto del punto "B1" al punto "F", vector RR(f).

Esto quiere significar que si cada plataforma de protección cumple adecuadamente con su propósito, el sistema de seguridad PESS estará en estado expectante en tanto la planta opera normalmente, listo para ejercer su acción protectora en caso de que alguna variable crítica del proceso se escape de sus límites de seguridad.

Pero puede suceder que se produzca una falla en cualquiera de las plataformas de protección (y a veces en más de una en efecto cascada) reduciendo o perdiendo su efecto protector y modificando drásticamente la curva de reducción de riesgos. En el peor de los casos puede llegar a fallar totalmente el Sistema de Regulación y como consecuencia (daba la complejidad del proceso) puede hacer casi nula la posibilidad de que el personal operativo pueda controlarlo con la ayuda del sistema de alarmas.

En este caso el proceso se descontrola, se escapa, la curva de riesgo se mueve del punto "B" al punto "B1" y allí, una vez superados los límites de seguridad, irrumpe el PESS o SIS para contener el peligro y conducir el proceso a condición segura (punto "F" de la curva, Reducción de Riesgo RRf).

Ninguna duda cabe respecto de la enorme responsabilidad del PESS o SIS de tener la "obligación" de actuar como última barrera supersegura de contención del riesgo dentro del proceso (las etapas o plataformas posteriores implican protecciones donde el proceso busca alivio o mitigación escapando hacia el exterior, debiendo preverse en este caso los riesgos consecuentes).

De allí la exigencia ineludible de que el PESS/SIS tenga garantizado el nivel de integridad segura (aprobación SIL) que le permita cumplir con su propósito de proveer (con muy baja probabilidad de falla) la protección requerida para evitar el siniestro, llevando el proceso a condición de bajo o despreciable nivel de riesgo.

Es importante además asegurarse de que cada plataforma de protección sea debidamente diseñada e implementada.

Esto es obvio y fácil de ver. Una deficiente capacitación del personal puede no permitir la complementación esperada en la reducción del riesgo y lo que es peor, puede ser la causante de un serio incremento del riesgo. Es conocida la facilidad con la que una maniobra indebida puede conducir a un desastre, en particular cuando el operador debe actuar bajo situaciones apremiantes o de pánico.

De igual manera el Sistema de Regulación deberá ser adecuadamente diseñado e implementado para lograr el control óptimo. Un diseño insuficiente o uno sobredimensionado no alcanzarán a producir el óptimo funcionamiento del proceso resultando en pérdidas de eficiencia productiva y de seguridad.

Por su parte un diseño incorrecto de este sistema que no ha sido advertido a tiempo puede conducir (o inducir) a nuevas situaciones de peligro no previstas.

Es por esta razón que existe una fuerte recomendación para que se realice un nuevo HAZOP a posteriori de la incorporación de todas las plataformas de protección en la etapa de diseño.

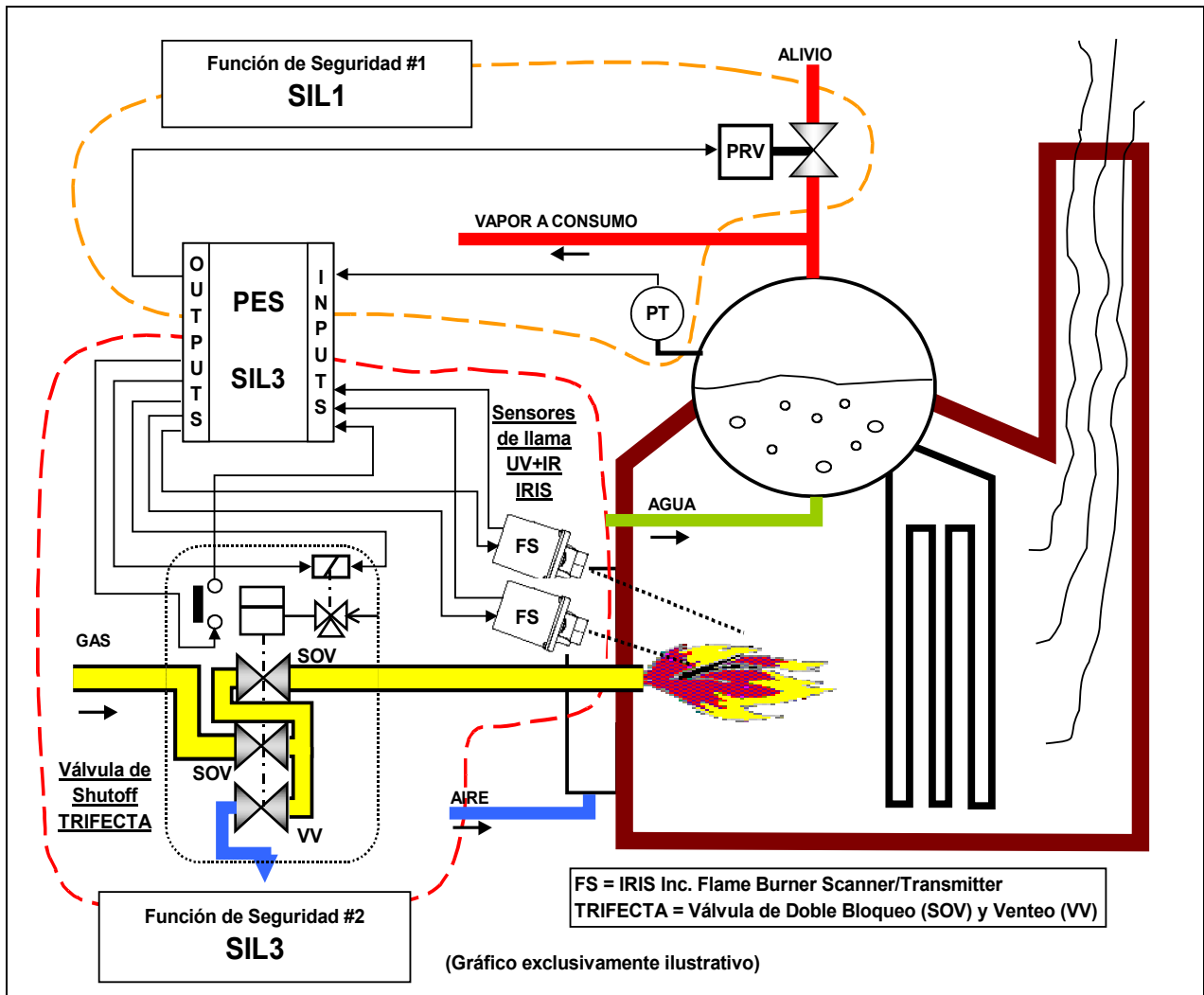
8- SISTEMA INSTRUMENTADO DE SEGURIDAD (SIS)

El Sistema de Seguridad actúa como una cadena de seguridad que “tracciona” desde su primer eslabón (el detector de la variable que alcanza niveles de peligro) y va trasladando su efecto a través de los restantes eslabones que la componen hasta el último de ellos cuya función es la de accionar el elemento final de protección.

Esta representación del Sistema de Seguridad SIS permite ver que así como “una cadena es tan fuerte como su eslabón más débil”, así también “un Sistema de Seguridad es tan seguro como su componente más débil”.

Es importante comprender que cada situación de peligro determina una específica necesidad o “función de seguridad” que reclamará una adecuada reducción del riesgo.

Un proceso peligroso muy probablemente va a requerir más de una función de seguridad donde cada una de ellas tendrá a su vez un menor o mayor nivel de exigencia definido por el respectivo SIL.



Esto significa que no se debe tratar de determinar el Nivel SIL de todo el proceso sino el de “cada función de seguridad” aunque obviamente el equipo PES-Logic Solver del sistema de protección que abarque a todos ellos quedará definido por el mas alto de los Niveles SIL obtenidos (ver gráfico).

Cada función de seguridad compone-en verdad-una cadena de “demandas” que viajan desde el proceso hasta el actuador final a lo largo del Sistema PESS/SIS.

La “demanda” inicial (variable en situación peligrosa) emana del proceso e “ingresa al detector”, el que a su vez emite una señal representativa que viaja e “ingresa como demanda” al equipo PES-Logic Solver que ejecuta la lógica.

Este equipo PES-LS elabora la acción protectora a ejecutar y emite una señal de accionamiento que ingresa como “demanda” al elemento final de control para que este provoque el efecto protector buscado (por ejemplo el bloqueo de alguna parte del proceso).

Un caso común y muy conocido es el de una caldera con múltiples quemadores.

Si en uno de esos quemadores se apaga la llama, la falta de fuego impone una “demanda de protección” al detector de llama, la que pasará a ser procesada por el PES-Logic Solver para finalmente “demandar” el disparo de la válvula de bloqueo de la línea de envío de combustible a ese quemador para evitar una acumulación explosiva en el hogar de la caldera.

9- MODOS DE FALLA (Failure Modes)

El Sistema de Seguridad PESS o SIS constituye una plataforma de protección en estado de permanente vigilancia, aparentemente quieto pero ininterrumpidamente atento y expectante tal como se supone que lo está la guardia real del Palacio de Buckingham para proteger a la Reina frente a situaciones de riesgo.

De ambos (tanto del SIS como de la guardia) se espera que “no estén dormidos cuando deban actuar ni que actúen cuando no deban hacerlo”.

Si protegen a la Reina cuando no hay riesgo, la incomodan (Nuisance Protection) y si no la protegen cuando hay peligro (Inhibited Protection) la Reina corre serio riesgo.

Y de ambos casos el segundo es el más preocupante.

El núcleo del Sistema de Seguridad es el PES-LS (Programmable Electronic Safety-Logic Solver) que es el que contiene la lógica y el que interpreta la “demanda” (señal de peligro) que recibe del detector para elaborar una adecuada señal de accionamiento del elemento de protección final.

Al igual que en el caso de la Guardia del Palacio, el PES-LS puede sufrir dos tipos de fallas:

- **FALLA POR ACCIONAMIENTO ESPURIO (NUISANCE TRIP)**

En ésta el equipamiento PES-LS (o el SIS) activa la protección del proceso sin que haya existido “demanda” o necesidad alguna.

Este tipo de travesuras del SIS por falla en el Logic Solver y/o en algún otro componente del lazo de seguridad, es muy fastidioso toda vez que detiene o reduce innecesariamente la producción.

Una parada intempestiva de este tipo, arbitrariamente decretada por el SIS, lleva a crear un clima de desconfianza respecto de su capacidad de proteger adecuadamente el proceso y es común que, de repetirse, los operadores terminen by-passeando, ignorando y/o anulando, el Sistema de Protección, quedando así expuestos a los riesgos de un siniestro.

- **FALLA POR INACCION (INHIBITED FAILURE)**

En este caso el PES-LS (o el SIS) recibe 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.

Lo más grave de este tipo de falla es que es totalmente invisible al operador, el que continuará operando la planta confiadamente, ignorante de la insospechada situación de alto riesgo a la que tanto él como el proceso han quedado expuestos.

Tomemos el ejemplo de la caldera de múltiples quemadores mencionado al final del punto 8.

“Si el detector de llama de un quemador comunica al PES-LS la falta de fuego (apagado de la Llama y-como consecuencia-combustible sin quemar) y éste sufre una falla por inhibición que le impide emitir el comando de bloqueo del ingreso de combustible al quemador, casi seguramente se producirá una explosión”.

Ambos modos de fallas se dan en todo tipo de Controlador Programable a microprocesadores, tanto en PLC como en DCS (Distributed Control Systems) como en PES-LS, pero la diferencia fundamental entre estos diseños es precisamente el muy diferente “grado de probabilidad” de que dichas fallas se produzcan.

- El alto grado de probabilidad de que estos modos de fallas internas se presenten en un PLC (simple o aún modificado como el que mencionamos en el punto 4, y/o en la lógica de un DCS) los hace incompatibles con las necesidades de protección de un proceso peligroso.

Es como pretender usar como cable extra de protección de un ascensor de carga el cable de seguridad de un elevador de platos de comidas de un restaurante. El requerimiento supera la capacidad del elemento de protección última.

Por su parte los PES-LS están específicamente diseñados para reducir significativamente el riesgo o probabilidad de que tales fallas se produzcan. Sus diseños incluyen redundancias, diversidades, altas coberturas de diagnósticos, máxima neutralización de causas comunes de fallas, etc.

Pero también hay diferentes modelos de PES-LS según su “menor” o “mucho menor” probabilidad de fallas internas, y se distinguen entre sí por el nivel de integridad segura de sus diseños.

El nivel de Protección o Reducción de Riesgo requerido por las Funciones SIF de Seguridad de un proceso queda definido por el Nivel SIL de cada una de ellas, por lo que un proceso que requiera Funciones de Seguridad de bajos Niveles SIL podrá ser protegido por un PES-LS aprobado como apto para dicho nivel o por uno aprobado para su uso en un Nivel SIL superior.

Pero no tendrá Ud. la debida protección si las Funciones de Protección de su proceso requieren un nivel SIL 3 y Ud. pretende protegerlo con un PES-LS aprobado para SIL 1 ó SIL 2.

Por esto es conveniente incorporar a los conocimientos técnicos el siguiente DOGMA (o reflejo condicionado):

- Solo podrá protegerse debidamente un proceso peligroso usando un PES-LS aprobado para operar (como mínimo) con el grado de integridad SIL requerido por la Función Protectora de mayor Riesgo de dicho proceso”.
- No intente resolverlo de otra manera.

Toda Norma (Code, Standard or Recommendation tal como las IEC 61508 y 61511, las NFPA, las FM, las DIN etc) no es un compendio de decretos arbitrarios sino de recomendaciones (utilizadas también por las aseguradoras de riesgos para evaluar la aplicación de sus pólizas) resultantes del análisis de muchas experiencias desagradables y catastróficas.

Estas recomendaciones – por la fuerza de los hechos – suelen ir convirtiéndose en regulaciones de aplicación obligatoria.

10- FAIL TO SAFE, FAIL TO DANGER

Se puede reducir la probabilidad de que un equipo falle pero nunca evitar la posibilidad (absoluta) de que alguna vez suceda.

En tal caso la opción deseable e indiscutible es que el SIS lleve el proceso a condición segura, esto es Fail to Safe o Failsafe.

La característica Failsafe es un requerimiento esencial para un Sistema de Seguridad.

- Es naturalmente Failsafe el disparo innecesario (Nuisance Trip) de un sistema de seguridad que provoca una acción protectora injustificada por haberse producido sin que el SIS recibiera un “pedido o demanda real” de protección por parte del proceso.

Si bien este tipo de falla es Failsafe- pues conduce al proceso a condición segura- entorpece el ritmo normal de la producción, genera pérdidas y demoras e incomoda a operadores y gerentes de producción.

Por esto el usuario exige que la probabilidad de este tipo de falla sea lo suficientemente baja como para tener en el proceso un muy largo tiempo de continuidad operativa segura (Availability, Disponibilidad Productiva con Protección)) sin paradas espurias (innecesarias).

En términos específicos se requiere que el tiempo medio hasta la próxima falla espuria sea significativamente alto (elevado MTTFs, Mean Time To Failure Spurious)

En procesos de alto costo productivo es razonable pretender un elevado valor probabilístico MTTFs (expresado en años).

- Cuando el sistema de seguridad sufre el otro tipo de falla interna (la invisible “falla por inhibición”), el PES-LS, pese a estar recibiendo una “verdadera demanda” o reclamo de protección, ha perdido la capacidad de ejecutar la acción protectora “permitiéndole al proceso continuar operando en condición peligrosa y-por ende- dejándolo expuesto a la catástrofe.

Puesto que la falla por inhibición perpetúa dicha situación de riesgo se la conoce como Fail to Danger.

Por ambas razones (por ser invisible y por inhibir la acción protectora) este tipo de falla es sumamente peligrosa y obliga a diseñar los SIS con una bien acotada y reducida “Probabilidad de Falla ante una Demanda Real” (PFD, Probability of Failure on Demand o Probability of Fail to Danger).

Es esta la cualidad realmente exigida a un SIS cuando se busca implementar el Nivel Requerido de Reducción del Riesgo en el proceso.

Cuando más alto sea el Riesgo, mas alto deberá ser el Nivel SIL de exigencia de integridad segura del SIS y, en consecuencia, mas bajo deberá ser el Nivel de PFD requerido.

El equipo PES-LS elegido (y el SIS con él implementado) debe estar diseñado para cubrir las exigencias SIL de las diferentes Funciones de Seguridad SIFs del proceso, o superarlas, y son los Approvals que emiten TÜV y FM los que garantizan tal performance y cumplimiento.

Estas instituciones emiten sus Certificados de Aprobación luego de muy rigurosas y exhaustivas pruebas (que suelen incluir requerimientos de modificación en el diseño durante las mismas), certificados que tienen alcances, limitaciones y advertencias que deben ser “cuidadosamente leídas y observadas” tanto por el integrador del sistema de seguridad como por el usuario.

11- TABLA DE APLICACIÓN SIL

Las siguientes tablas exhiben las exigencias de integridad (PFD, RRF) relativas a cada Nivel SIL con Sistemas de Seguridad SIS operando en Modo de Baja Demanda (Tabla 1,Procesos Discontinuos) y en Modo de Operación Continua y/o de Alta Demanda (Tabla 2).

TABLA 1 - SISTEMA DE SEGURIDAD EN MODO DE BAJA DEMANDA

Nivel de Riesgo	Safety Integrity Level (SIL)	Equivale a la alemana Application Class AK	Probability of Failure On Demand (PFD)	Risk Reduction Factor RRF=1/PFD
ESPECIAL	SIL 4	AK-7/AK-8	menos de 10^{-4}	más de 10.000
ALTO	SIL 3	AK-5/AK-6	10^{-3} a 10^{-4}	1.000 a 10.000
MEDIO	SIL 2	AK-4	10^{-2} a 10^{-3}	100 a 1.000
BAJO	SIL 1	AK-2/AK-3	10^{-1} a 10^{-2}	10 a 100

TABLA 2 - SISTEMA DE SEGURIDAD EN MODO DE ALTA DEMANDA o EN PROCESO DE OPERACIÓN CONTÍNUA

Nivel de Riesgo	Safety Integrity Level (SIL)	Equivale a la alemana Application Class AK	Probability of Failure on Demand per hour or Probability of Fail to Danger per hour (PFD per hour)	Industrias
ESPECIAL	SIL 4	AK-7/AK-8	menos de 10^{-8}	Nuclear, Aerotransporte, Ferrocarril
ALTO	SIL 3	AK-5/AK-6	10^{-8} a 10^{-7}	Calderas de Generación, Procesos Químicos, Gas, Refinación de Petróleo, Calderas Industriales
MEDIO	SIL 2	AK-4	10^{-7} a 10^{-6}	Calderas Industriales, Procesos Químicos, Gas, Petróleo
BAJO	SIL 1	AK-2/AK-3	10^{-6} a 10^{-5}	Procesos de Menor Riesgo

12- SINOPSIS

El "SIS" puede dar lugar a tres situaciones que resumimos sintéticamente en el cuadro que sigue:

- ON - Operación Normal	Ante la existencia de una "demanda" por condición peligrosa en el proceso, el PES-LS/SIS ejecuta la correcta acción protectora.
- FS - Fail to Safe	Sin la existencia de una "demanda" por condición peligrosa en el proceso, el PES-LS/SIS ejecuta una innecesaria acción protectora.
- FD - Fail to Danger	Ante la existencia de una "demanda" por condición peligrosa en el proceso, el PES-LS/SIS no ejecuta la debida acción protectora.

Los diferentes niveles de protección de un equipo "SIS" programable a microprocesadores quedan reflejados en el gráfico que sigue (las dimensiones de las gráficas son puramente ilustrativas).

Corresponde recordar una vez más que el PES-LS es tan sólo un eslabón en todas las Cadenas o Funciones de Seguridad (SIFs, Safety Instrumented Functions) del Sistema PESS o SIS completo y que el requerimiento exigido por el Nivel SIL definido para cada SIF se va incorporando a la totalidad de dicho Sistema SIS.

Comportamiento del Equipo		Tipo de Logic Solver	Nivel de Integridad Segura	Aplicaciones Industriales
Zona de Probabilidad de Fallas	Zona de Operación Normal			
		PLC	NO APTO para Protección Segura	Extenso campo en aplicaciones de bajo riesgo (inherentemente seguros, with negligible and tolerable risk)
FRONTERA DE APLICACIONES SEGURAS				
		PES-LS	SIL 1 (AK-2/3)	
		PES-LS	SIL 2 (AK-4)	Calderas Industriales y de Generación a Gas, Carbón Pulverizado, Fuel Oil y otros.
		PES-LS	SIL 3 (AK-5/6)	Procesos Químicos y Petroquímicos. Industrias de Gas. Refinerías de Petróleo, etc.
Referencias: ■ FD (Fail to Danger) ■ FS (Fail to Safe) ■ ON (Operación Normal)				

13- EPÍLOGO

Las exigencias de integridad para tener una garantía de protección segura en un proceso imponen el uso de un Sistema SIS exclusivo, independiente, dedicado y debidamente aprobado como apto para producir la necesaria Reducción de Riesgo que la peligrosidad del proceso requiere.

J. A. Cabrera 4621 Tel (54) (11) 4833 0020
Buenos Aires (C1414BGI) Fax (54) (11) 4833 0019
Argentina E-mail: dacs@dacs.com.ar

SistemasDACS S.A.

Quien tenga la responsabilidad de decidir el tipo de protección del proceso peligroso deberá preguntarse si bajaría con su familia por un angosto y escarpado camino de cornisa manejando un automóvil cuyos frenos fueran simplemente aceptables para circular por una llana y tranquila ciudad, o si se pararía con su familia delante de un proceso de alto riesgo indebidamente protegido.

Creemos que Ud. va a poner especial cuidado en usar un automóvil con frenos adecuados al mayor riesgo a enfrentar y a asegurarse que cuenten con la mayor garantía posible de que su probabilidad de falla sea decididamente muy baja.

No deje de hacer lo mismo con el Sistema de Protección de su Proceso.

Recuerde el “posible vagón desprendido” mencionado en el punto 2.

Ing. ROBERTO FERNÁNDEZ BLANCO

ISA & FUNCTIONAL SAFETY EXPERT ENGINEER

rblanco@dacs.com.ar

SISTEMAS DACS S.A.

ESPECIALISTAS EN SISTEMAS DE SEGURIDAD

PARA PROCESOS PRODUCTIVOS DE ALTO RIESGO

Septiembre 2001