Actualización Tecnológica de Sistemas de Control y Seguridad de Plantas

Autores: Daniel Petin, Carlos Fernandez, Diego Caprarelli
Compañías: Total Austral, Tecna SA

1. Introducción

El proyecto tuvo por objeto realizar la Actualización Tecnológica de los Sistemas de Control y Seguridad de las Plantas de Proceso de Cañadón Alfa, Tierra del Fuego, propiedad de Total Austral S.A.
El sistema de seguridad se encontraba en una plataforma híbrida que no respondía a los estándares de la compañía, en cuanto a los niveles de seguridad requeridos (grado SIL), por lo que se decidió su reemplazo, uniformizando todo en una única plataforma. Por otra parte, el sistema de control existente estaba desactualizado en sus versiones, lo cual dificultaba la integración confiable con los sistemas a instalar, por lo que, previo a la puesta en servicio del mismo, se le realizó un upgrade de firmware / software.
El cambio se ejecutó con planta en operación lo cual impone consideraciones especiales a la ejecución. Los resultados obtenidos comprenden la mejora de los niveles de seguridad y mejores herramientas de diagnóstico y operación.

2. Marco Conceptual de Sistemas de Seguridad

En esta sección se revisan los conceptos fundamentales que deben tomarse en cuenta a la hora de diseñar un ***Sistema de Paradas de Emergencias***, al cuál haremos referencia como ***ESD (Emergency Shut Down)*** desde ahora. Se describe lo que se debe considerar como Riesgo Aceptable, los elementos que afectan a un lazo de control o de bloqueo, y las diferentes estadísticas y factores que afectan a dicho diseño.

2.1. *Definición de Riesgo Aceptable*

Nada es absolutamente seguro. Toda operación por sencilla que sea, por rutinaria que sea, o por *"segura"* que sea, envuelve un riesgo.

Este riesgo depende de una acción, u ocurrencia, por lo que debemos definir riesgo, como: ***Las posibilidades estadísticas de que lo peligroso ocurra.***

Entonces, riesgo en este contexto es una cifra o un número que representa la probabilidad de ocurrencia de un evento peligroso.

En la industria en general, todas las operaciones envuelven riesgo, bien sea riesgo de daño a los equipos, la producción o, lo que es peor, a la integridad física de quiénes operan el proceso. No existe operación que no envuelva riesgo, y la única manera de que el riesgo sea nulo, es el no realizar la operación.

En la industria en general, y muy en especial en la industria petrolera y petroquímica, el Riesgo Aceptable es determinado por las normativas de cada país y por las políticas propias de las compañías.

El riesgo se determina en término del número de accidentes por unidad de tiempo, o en número de ocurrencias por año. Ejemplo: Un accidente cada 1.000, 10.000, 100.000, 1.000.000 etc. de años, ó 0,1, 0,01 etc. por año.
Una vez determinado el riesgo aceptable (Ejemplo: que ocurra un derrame cada millón de años), debemos determinar las medidas a tomar para que dicho nivel de riesgo se cumpla.
La ecuación que regula este comportamiento es simple y lógica. Para un lazo de control, el Riesgo Aceptable o Tasa de Peligro es igual a la Tasa de Demanda o frecuencia con que el lazo va a demandar una parada de emergencia, multiplicado por las probabilidades estadísticas de que el lazo del ESD falle en demanda, para ese mismo lazo.

Tasa de Peligro = Tasa de Demanda x PFD

Esto nos conduce a definir varios parámetros, como los que veremos en las próximas secciones, pero lo importante es visualizar que podemos tomar medidas para disminuir la Tasa de Peligro.

2.2. *Probabilidad de Falla en Demanda*

La Norma ISA, S 85.01, define la ***PFD*** (***Probability Of Failure on Demand***), como la probabilidad estadística de que un sistema falle en forma peligrosa. En otras palabras: un sistema puede no fallar, y las probabilidades de que no falle, es lo que se conoce con el nombre de Disponibilidad del sistema, pero también ese sistema puede fallar. Ahora bien, si el sistema falla, esta falla puede producirse de dos maneras. Existe la posibilidad de que falle en forma segura (PFS), por ejemplo que una válvula se cierre aunque no haya habido un derrame (lo que se conoce como Tasa de Molestia o "Paradas en falso"). En este caso, la válvula se cerró sin razón, y la producción es parada sin motivo.
Sin embargo también el sistema puede fallar en forma peligrosa (PFD), es decir, se produce un derrame y la válvula no cierra. La Figura 1, nos muestra esquemáticamente estos conceptos.

Las PFD, son utilizadas por el comité de la S84.01, para la fijación y determinación de los ***Niveles SIL***, (***Safety Integrity Levels***) ó ***Niveles Integrales de Seguridad***, donde se toman estas estadísticas o sus inversas (Factor de Reducción de Riesgo - FRR = 1/PFD), para determinar estos niveles discretos.

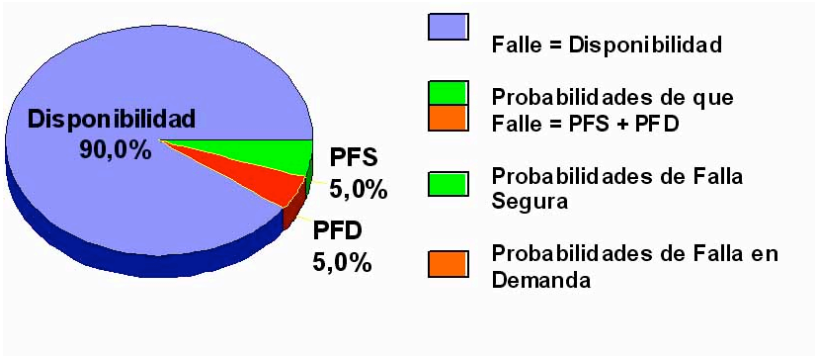


Figura 1

Para Alcanzar un Nivel de Seguridad SIL	Necesitamos una PFD (Promedio)	Necesitamos un FRR
1	0.1 - 0.01	10 - 100
2	0.01 - 0.001	100 - 1000
3	0.001 - 0.0001	1000 - 10000

2.3. *Los Niveles SIL y las Capas de Protección*

En general las medidas que se toman para disminuir el riesgo consisten en el diseño de Capas Individuales de Protección, en las cuales se envuelve al proceso para protegerlo. Por estar conceptualizadas dichas capas en forma similar a una cebolla, donde cada hoja de la cebolla corresponde a una capa individual e independiente de las demás, este concepto se conoce como el de "La Cebolla". La figura 2 nos muestra este concepto.

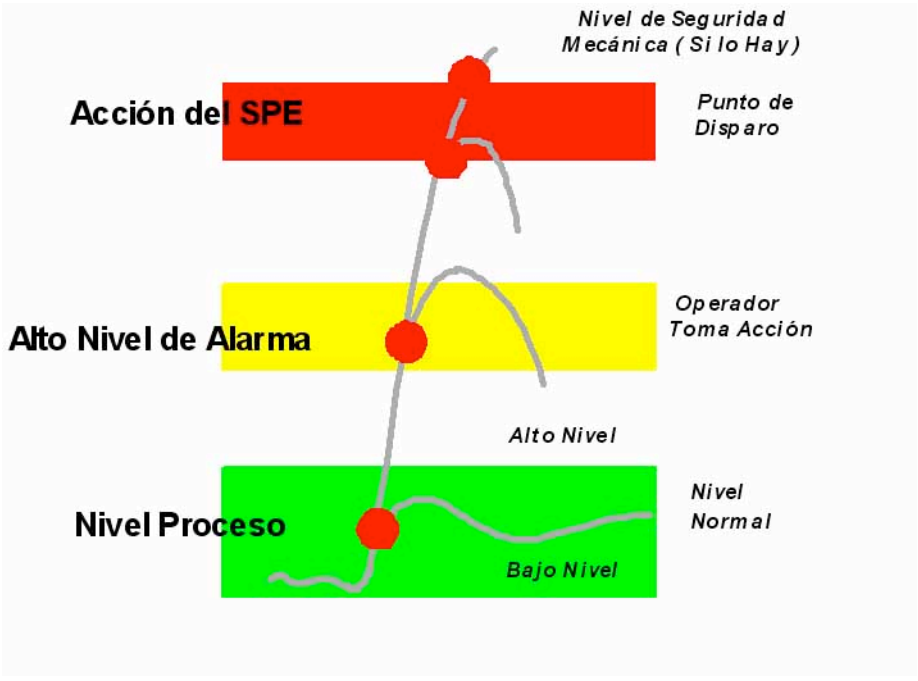


Figura 2

La primera protección del proceso se realiza en el controlador y el lazo de control. Si por cualquier razón éste fallara, existe una capa superior, completamente independiente, identificada en Figura 2 como el nivel de alarma. Por supuesto, con la tecnología moderna, es posible colocar en el controlador alarmas de todo tipo, pero si queremos

considerarlas otra capa de protección, las alarmas deben ser parte de otro equipo completamente independiente.

Más arriba se nota una segunda capa de protección, para el caso de que el controlador y las alarmas fallaran, o el operador de las alarmas fracase a colocar la variable en el nivel normal. Estamos refiriéndonos a la capa que contempla un ESD.

La figura 3 nos muestra el concepto de protección con capas.

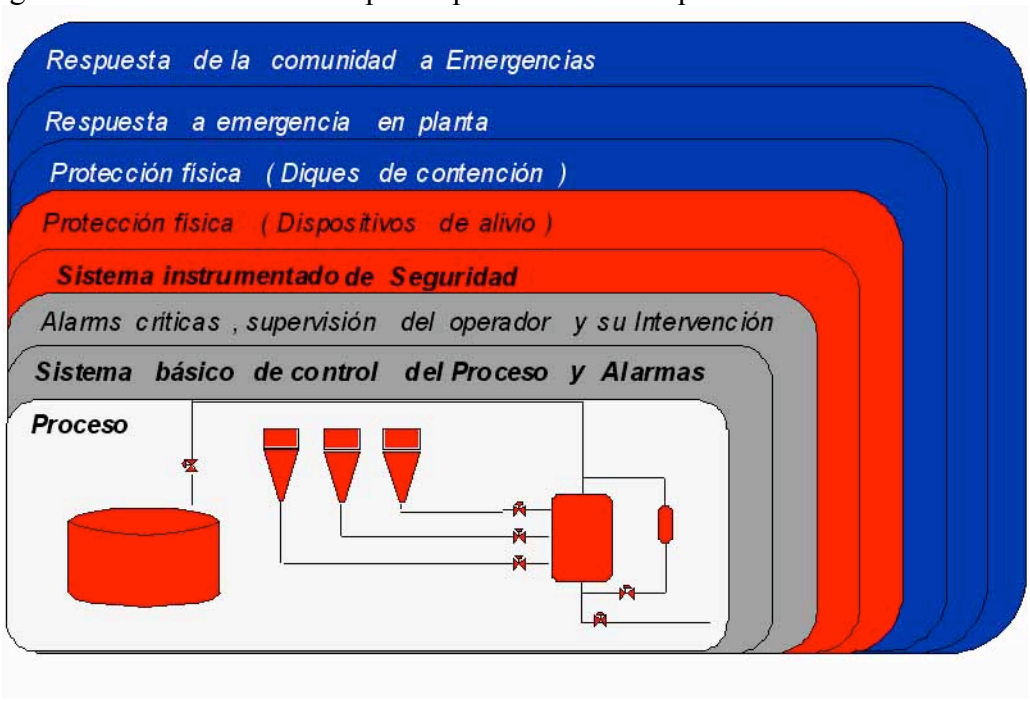


Figura 3

Aquí podemos observar más capas de protección. La inexistencia de personal alrededor de un lazo de control debe de influenciar la definición de ***Riesgo Aceptable*** y por ende del Nivel SIL requerido. Así se deduce como el número de capas de protección debe afectar la decisión de aplicación de un SIL. En la figura 4 vemos este efecto.

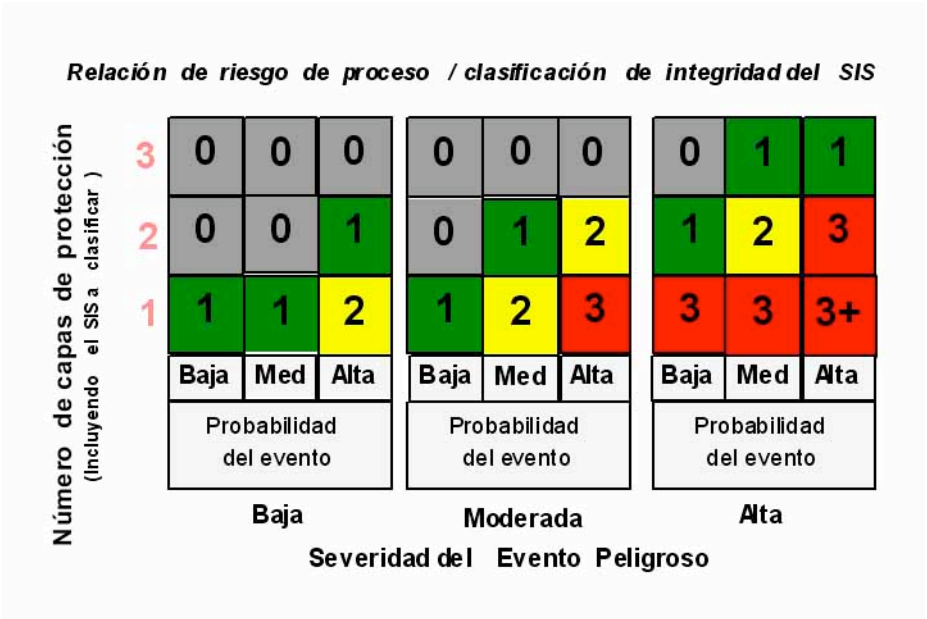


Figura 4

Aquí vemos como si un evento es ***altamente peligroso***, o sea por ejemplo, daños severos a las instalaciones y al medio ambiente, y con accidentes fatales, con probabilidades de ***ocurrencia baja***, es decir, por ejemplo, de menos de 1 vez cada 10.000 años o con una frecuencia de menos de 0,0001 veces por año; el SIL requerido para el ESD de ese lazo en específico es 3 con una capa de protección; 1 con dos capas de protección; pero no se requiere ESD (SIL 0) si se le colocan tres capas de protección.

Nota: Según lo definido por la S84.01, existen tres niveles SIL, pero debe tenerse en cuenta que para ciertas aplicaciones, se considera el nivel ***SIL 4***, aunque este no es aplicable a la industria que nos interesa, sino a las aplicaciones nucleares, militares, aviación, etc.

2.4. *Definición de un ESD*

Definidos los niveles integrales de seguridad, estadísticas que los respaldan y riesgo aceptable, trataremos de aplicar estos conceptos a los problemas más comunes encontrados en nuestras industrias.

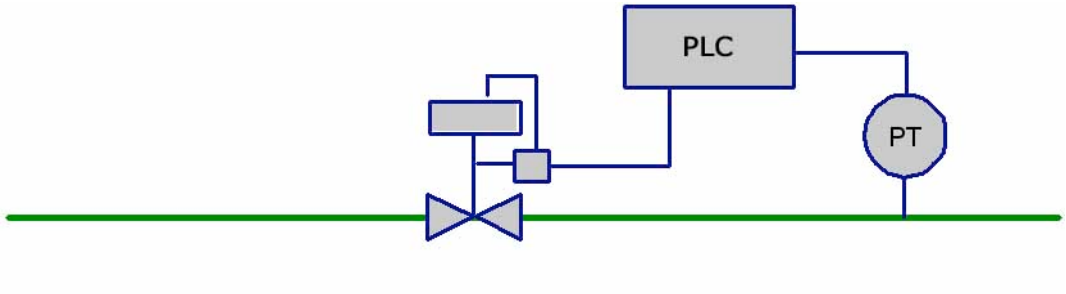


Figura 5a

Consideremos por un momento un lazo de control típico, como el mostrado en la figura 5a, donde tenemos tres elementos:

- Un elemento sensor (PT)
- Un elemento final de control
- Un sistema básico de control de proceso , BPCS (Basic Process Control System)

Cada uno de estos elementos tendrá una estadística de falla, o un tiempo medio entre fallas, que obligará a un ESD a reaccionar para colocar la variable, en este caso presión, bajo control. La figura 5b nos muestra como actuaría dicho ESD. (Ejemplo combinado de falla del lazo 0,35 veces por año)

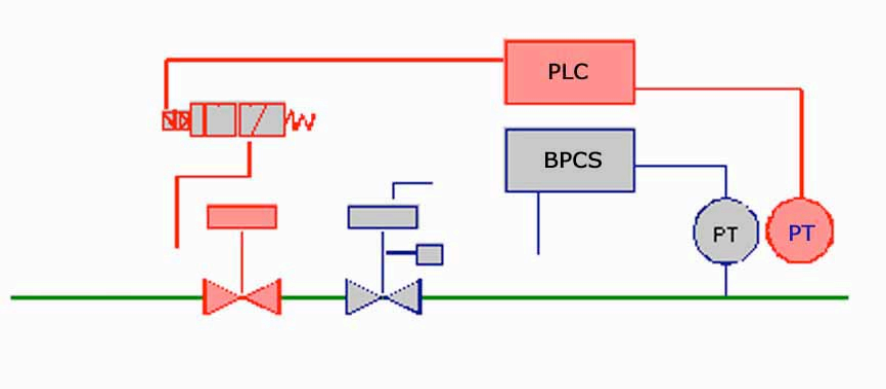


Figura 5b

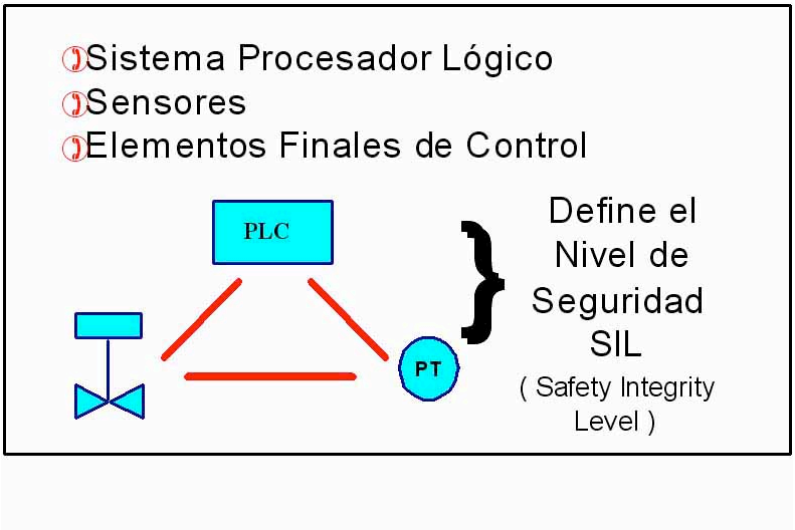
Si por alguna causa la presión se saliera de control, digamos por ejemplo que la válvula de control se trabara, que el BPCS fallara, o que el sensor se descalibrara seriamente, inmediatamente el sensor del ESD detectaría la anomalía, el sistema de procesamiento lógico (PLC) cortaría el suministro a la válvula solenoide, y la válvula del ESD se cerraría, evitando el evento peligroso. Sabiendo el riesgo aceptable, es fácil de la fórmula 1 calcular las PFDavg., y obtener el SIL adecuado de la tabla en la Figura 4.

2.5. ***Los Tres Elementos de Un ESD***

El último detalle que se quiere resaltar de la figura 5b, es el hecho de que el ESD del ejemplo, y en general, está compuesto por tres elementos:

- ***Los sensores***
- ***El PLC***
- ***Los elementos finales de control***

No es posible ni lógico entonces el alcanzar un alto nivel SIL, simplemente colocando un PLC de alta disponibilidad como un 1oo2 D ó 2oo3, si colocamos un solo sensor y un solo elemento final de control.



Por lo general colocando un sensor, un PLC y un elemento final de control, como en el ejemplo de la figura 5b, podremos alcanzar un SIL 1, siempre y cuando los equipos seleccionados sean los adecuados.
Sin embargo, es posible que con equipos especiales, con un PLC, un sensor y un elemento final, se alcance el Nivel SIL2. Tal es el caso de la utilización de un PLC con arquitectura 1oo1D, un sensor con diagnóstico que tenga la potestad de influir en la señal (1oo1D) y una válvula de doble bloqueo y purga (1002). (Ver Punto 6)

Para alcanzar un Nivel SIL 3, sin embargo, es necesario al menos duplicar, y en algunos casos triplicar, los elementos de un ESD. La figura 6, nos da una idea de lo expuesto, aunque no será hasta la próxima sección que lo abordaremos en detalle.

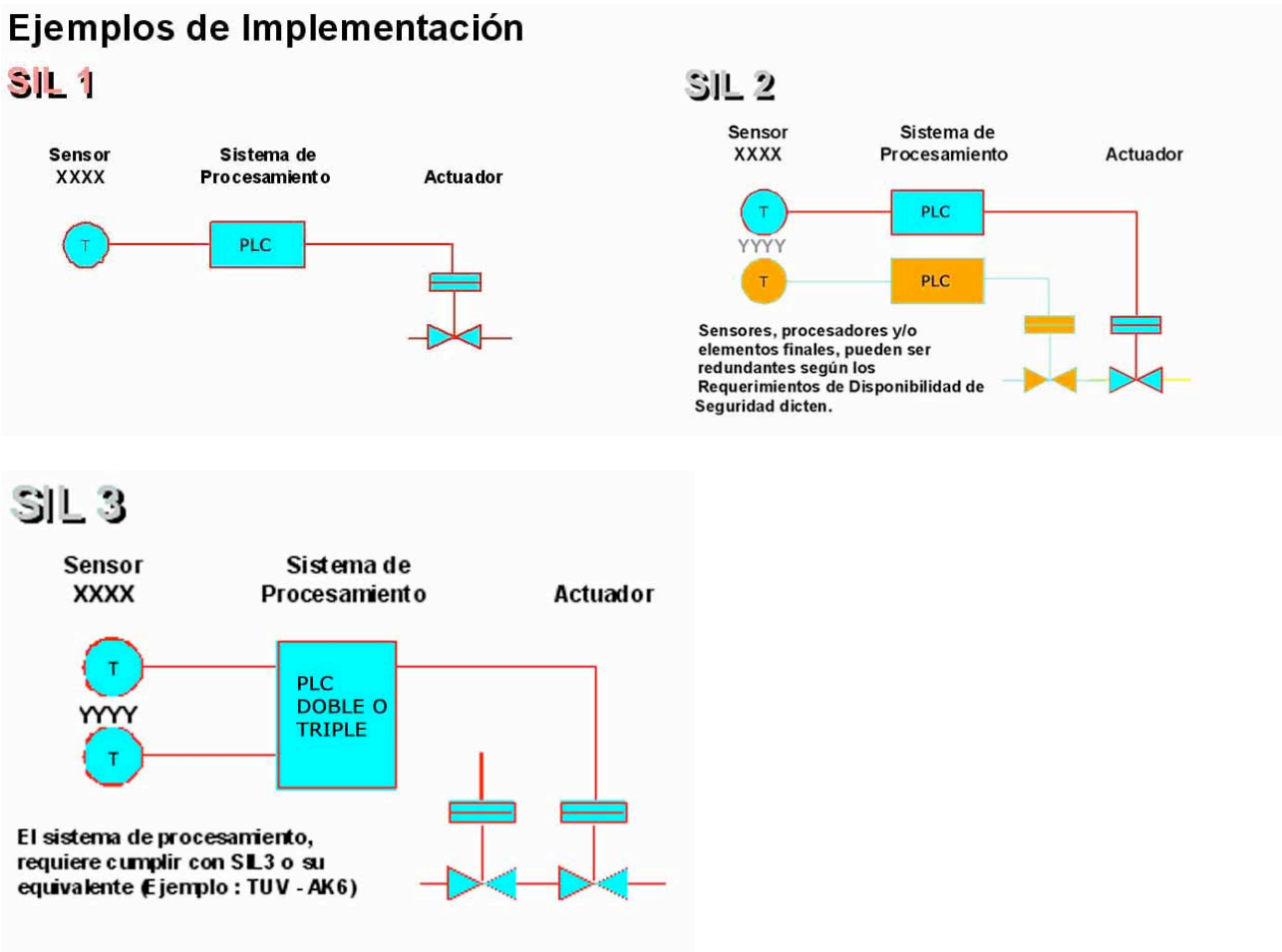


Figura 6

2.6. *Arquitecturas*

Las diferentes arquitecturas afectan los cálculos de disponibilidad.
Las diferentes arquitecturas para los tres elementos son:

- 1oo1 ó uno de uno (1 Out Of 1)
- 1oo2 ó uno de dos (1 Out Of 2)
- 2oo2 ó dos de dos (2 Out Of 2)
- 2oo3 ó dos de tres (2 Out Of 3)
- 1oo1D ó uno de uno con Diagnóstico (1 Out Of 1 Diagnostics)
- 1oo2D ó uno de dos con Diagnóstico (1 Out Of 2 Diagnostics)

Siendo estas dos últimas los más recientes aportes del mundo tecnológico al problema de los ESD. Aquí la D denota que no sólo el PLC tiene diagnóstico, sino que el mismo está como un circuito independiente dentro del mismo con veto, directo e independiente sobre la salida del PLC.

La figura 7, compara las soluciones diferentes de un lazo de un ESD, utilizando arquitecturas tradicionales, con estas nuevas arquitecturas, utilizando electrónica de alta confiabilidad. En ambos casos los diseñadores requerían que el lazo de control tuviera un Nivel SIL 2.

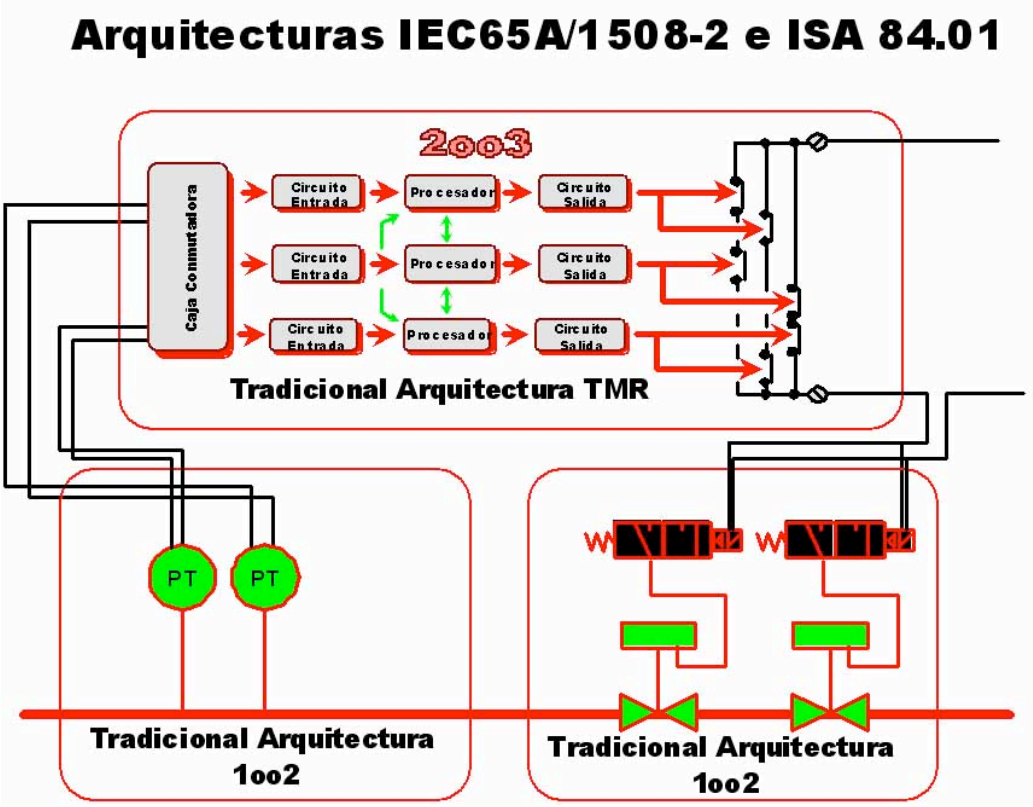


Figura 7a

En la figura 7a, se muestra la solución tradicional, de colocar dos sensores, dos válvulas, comandadas por un PLC TMR (Triple Modular Redundante) ó 2oo3. El PLC realiza un proceso de votación, donde en caso de estar dos de los procesadores de acuerdo en cerrar las válvulas, la línea de fluido será bloqueada. Como se explicó, este sistema tiene un SIL 2, es decir un FRR entre 100 y 1.000.

Por otra parte, la figura 7b, nos muestra otra solución a este problema. Aquí el diseñador ha utilizado un solo sensor con aprobación **TÜV** 4, o lo que es igual SIL 2. También el diseñador ha elegido utilizar una válvula de "doble bloqueo y purga", con un tiempo entre inspecciones acorde (cada dos meses), y un PLC con arquitectura 1oo2D.

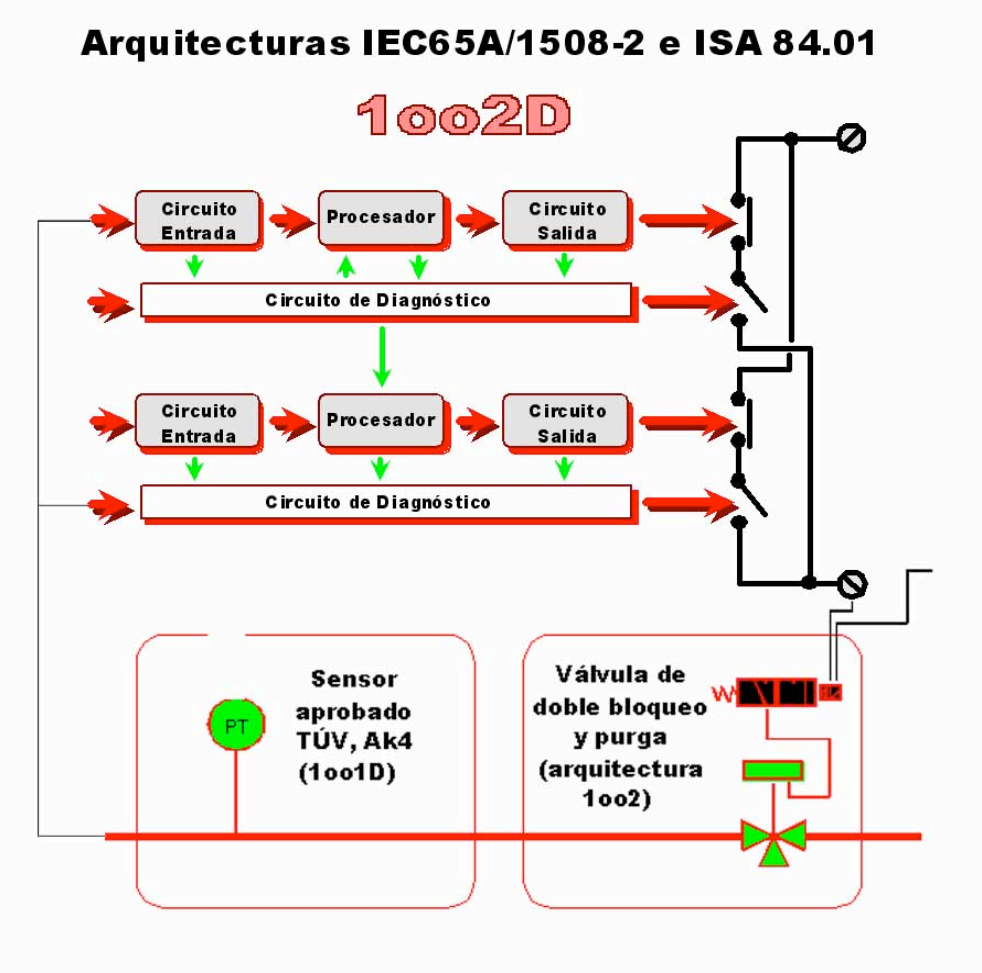


Figura 7b

3. Niveles de Shutdown

3.1. *Objeto de los ESD*

Sistema de ESD denota un sistema genérico que realice funciones de shutdown de equipos de procesos (SD) y funciones de shutdown de emergencia (ESD).

3.1.1. Filosofía General

Un sistema de shutdown contiene diferentes niveles (proceso, emergencia, Fire & Gas y shutdown de último nivel) cada uno de los cuales involucra un conjunto de lazos de seguridad. En general, como se explicó anteriormente, un lazo está formado por sensores, actuadores y Logic Solvers (en general, un dispositivo electrónico que resuelve múltiples lazos, como un PLC)

El propósito principal de los sistemas de ESD es:

• Limitar o evitar los derrames, asilando las áreas de producción y almacenamiento de hidrocarburos
• Proteger al personal, por ejemplo con detectores de humo y gas en los sistemas de ventilación
• Ejecutar procedimientos de control o remediación, manuales o automáticos después de la detección de situaciones peligrosas
• Prevenir incendios evitando la aparición de Fuentes de ignición
• Reducir el almacenamiento de productos inflamables o tóxicos por medio de despresurización, cuando sean aplicables

3.1.2. Consideraciones adicionales de diseño

El diseño del sistema ESD deberá tener en cuenta las necesidades resultantes de la operación normal y deberá satisfacer los requerimientos que puedan surgir durante otras posibles configuraciones anormales o degradadas (probables de ocurrir).
Los siguientes puntos deberán ser adecuadamente abordados cuando sea relevante:

• El shutdown de un equipo o unidad NO necesariamente elimina todas las fuentes de peligro.
• Pueden aparecer nuevos peligros como consecuencia de la pérdida de suministros esenciales, tales como: energía esencial, aire, hidráulica, etc. Estos nuevos peligros serán identificados, mitigados, y los riesgos asociados serán evaluados.
• Todas las configuraciones de operación generadas por el sistema ESD serán seguras, estables y reversibles. Todas las transiciones relacionadas al ESD, desde una configuración de operación a otra, serán seguras.
• El ESD será compatible con la filosofía de re-arranque. Todas las operaciones de la secuencia de re-arranque desde el estado total de shutdown al estado de producción completo, serán seguras, estables y reversibles. Se identificarán las inhibiciones inevitables de los sistemas de control y seguridad durante la secuencia de re-arranque, y serán limitadas en número, tiempo y duración.

3.1.3. Operaciones particulares

Se debe poner especial atención a condiciones de operación no rutinarias y a la conveniencia del sistema ESD, en combinación con el sistema EDP, para tratar con ellas. Los principales escenarios contemplados serán:

• Situaciones anormales degradadas, servicios de pozo, desviación de la especificación del producto durante un corto período, mantenimiento de un sistema de seguridad, etc.
• Operaciones simultáneas: perforación/instalación y producción, construcción y producción, mantenimiento y producción, etc.
Cada operación será segura pero se pondrá atención específica a la combinación resultante de sus simultaneidades (ej: mantenimientos simultáneos sobre dos sistemas)

En algunos casos, condiciones particulares de operación pueden requerir una lógica de shutdown diferente de aquella, o de la combinación de aquellas, aplicables bajo circunstancias normales. Por ejemplo:
• Una lógica de ESD específica puede ser activada cuando un trabajo de pozo se inicia o cuando los operadores vienen de una plataforma de perforación no manejada permanentemente.
• Una lógica temporaria de EDS mejorada puede demostrar beneficios simultáneos para construcción/puesta a punto principal y producción.
• Una instalación puede operar bajo condiciones diferentes, esto es: alta, media o baja presión.

Cada condición puede requerir una lógica de ESD diferente, pero las diferencias estarán limitadas a procesos de shutdown. Shutdowns de emergencia resultarán en las mismas acciones independientemente de la condición. Antes de conmutar entre diferentes lógicas de ESD, se necesita verificar el equipamiento aguas arriba y el estado de las válvulas. Esta operación particular será abordada en el CONCEPTO DE SEGURIDAD y en la FILOSOFÍA DE OPERACIÓN.

3.2. *Definición de la matriz de shutdown*

3.2.1. Definición de los niveles de shutdown

Es una práctica común dentro de la COMPAÑÍA definir un máximo de 4 niveles típicos de shutdown con criticidad decreciente, numeradas de 0 a 3 y que afectan a:

- todas las instalaciones con un área simple restringida (nivel-0) = ESD-0
- una zona de fuego dada dentro de la instalación (nivel-1) = ESD-1
- una unidad dada dentro de una zona de fuego dada (nivel-2) = SD-2
- un equipo individual o paquete dentro de una unidad dada (nivel-3) = SD-3

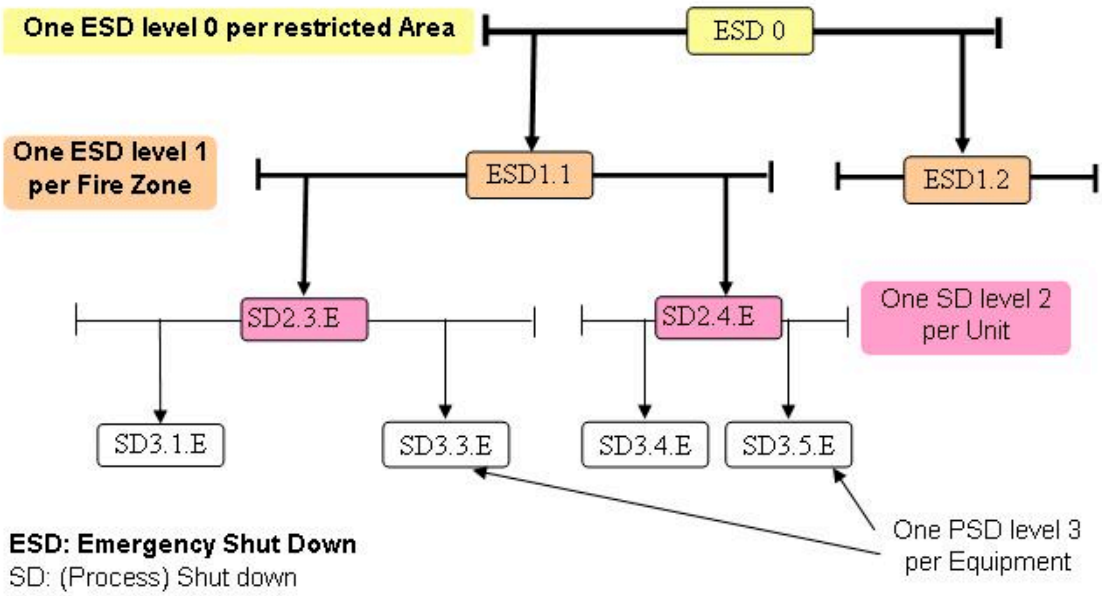
El nivel 0 y el nivel 1 serán llamados **niveles ESD** debido a que ellos involucran detección tanto de fuego/gas en ambiente no confinado (y por lo tanto una situación sujeta a posibles escaladas) como una acción manual de emergencia.

El nivel 2 y el nivel 3 serán denominados **niveles SD** porque ellos corresponden tanto a un mero proceso fuera de control como a la detección de fuego y gas confinada (suficientemente bien contenida) sin amenazar inmediatamente la seguridad del personal y de la instalación.

El sistema de seguridad de shutdown de una instalación, que consiste en un grupo de lazos de seguridad y dispositivos, comprende diferentes subsistemas organizados como barreras complementarias al Sistema de Control de Procesos.

Para cada instalación se deberá definir y representar una lógica ESD/SD en un diagrama lógico ESD/SD. La lógica está basada en la jerarquía de niveles ESD y SD, el nivel N que activa el nivel N+1.

El diagrama lógico ESD/SD cubrirá todas las facilidades de una instalación de petróleo. Las causas y acciones serán descriptas a nivel funcional (tipo y locación de detección, cierre/apertura de válvula, shutdown de equipos, etc.)



Definiciones

Area (restringida)
Área dentro de los límites de la instalación y bajo el control de la Compañía, la cual se encuentra afectada permanentemente por la operación normal de las instalaciones y puede sufrir excepcionalmente una situación de emergencia por una falla importante.

Zona de Fuego

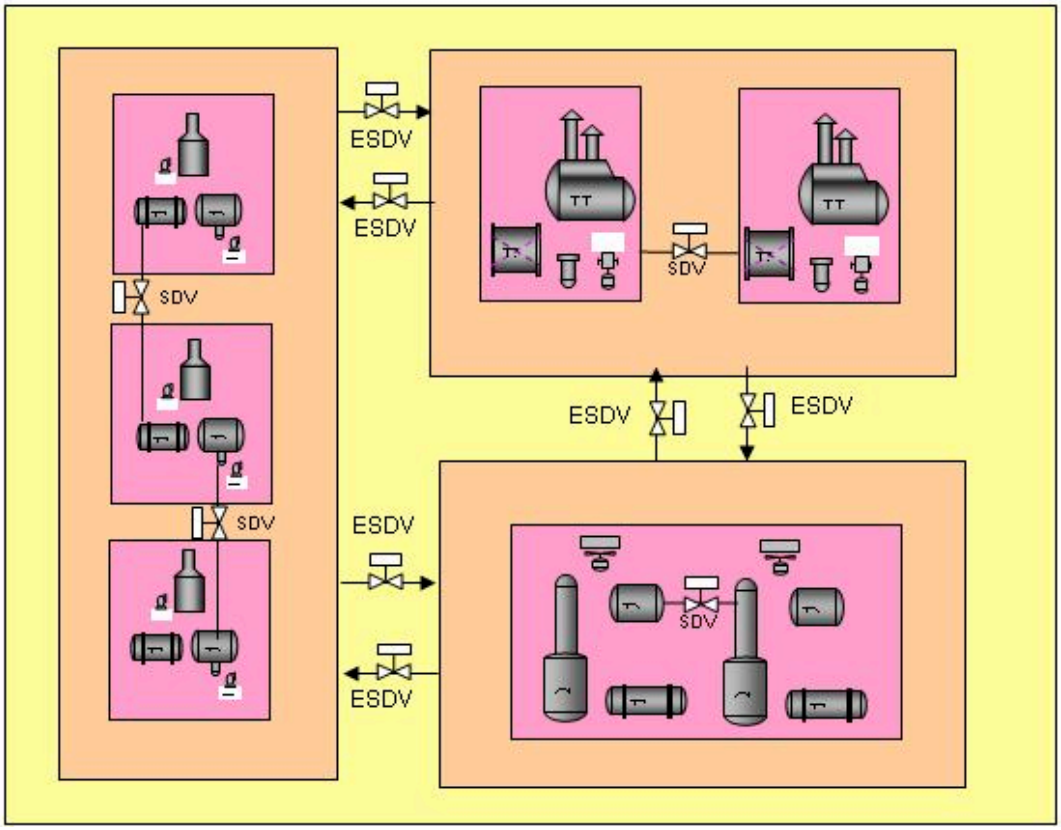
Area dentro de una instalación en la cual se agrupan los equipos de acuerdo a su naturaleza y al nivel de riesgo que important. La separación en zonas de fuego es tal que una situación peligrosa en dicha zona purde ser confinada sin causar daños o riesgos potenciales a otras zonas de fuego.

Unidad

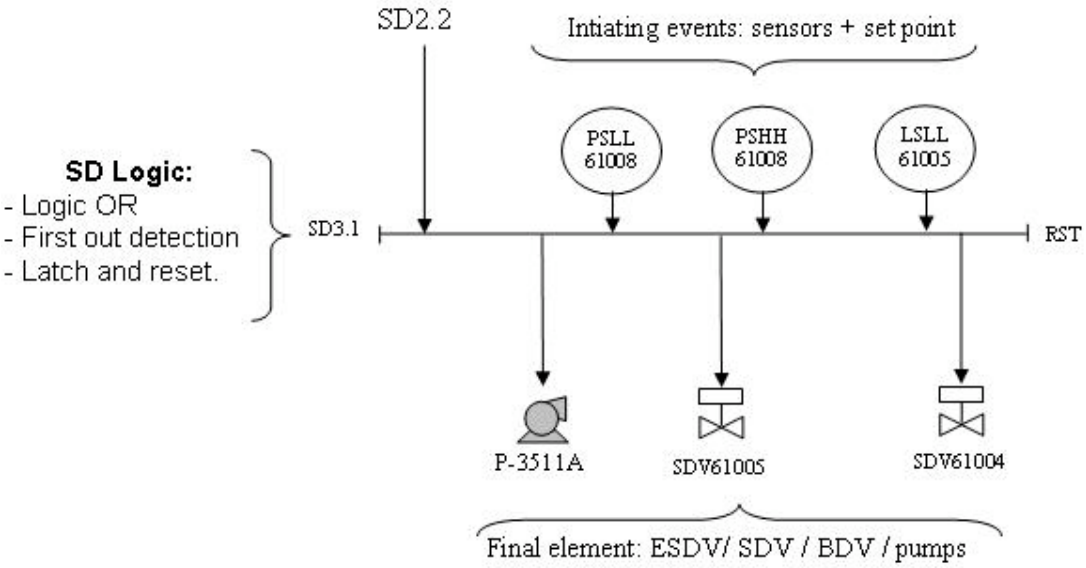
Área dentro de una instalación que resulta de particionar las instalaciones en zonas geográficas y funcionales conteniendo equipos del mismo tipo (hidrocarburos, presiones, almacenaje, etc) y niveles de riesgo (alto, medio, bajo).

Equipo
Cualquier componente o grupo de elementos identificado en los P&ID.

Typical plant layout structure



Typical structure of one shut down level



4. Sistemas Existentes

Se describen a continuación los sistemas existentes involucrados en el revamping de las instalaciones.

La Planta de Cañadón Alfa se encontraba protegida por tres diferentes PLCs: dos Triconex y un PLC5 A&B, dedicados a las unidades de compresión de LP/LPG, generación de energía y plantas de gas LTS 1/2 respectivamente.

4.1. *"LTS1/2" PLC5 Allen & Bradley (ESD 400)*

Este PLC5 A&B con CPU redundante fue instalado en 1995, para proveer funciones de ESD y Fire&Gas a las siguientes unidades de proceso:

- LTS-1 (tratamiento de gas, ajuste de punto de rocío)
- LTS-2 (tratamiento de gas, ajuste de punto de rocío)
- MP Compression (3 turbocompresores existentes más el agregado de un cuarto durante el 2007)

Adicionalmente el EDS 400 implementa las siguientes funciones:

- Fire water system (fire pumps)
- ESD1.0 level
- Telemetría de Baterías remotas 1, 2, 3, 4 y Alfa Sur. Toda la información de monitoreo, control y seguridad se conectaba a través de radioenlaces al sistema INTOUCH existente. Como parte del presente trabajo, toda esta información fue migrada al sistema BPCS.

4.2. *"LPG" Triconex*

Este PLC de seguridad, instalado en 1999, protege las siguientes instalaciones:

- LPG Units:
- LP compression units
- Servicios misceláneos y válvulas de shutdown

El PLC se conecta a través de un enlace Modbus serial con el BPCS, el cual sirve como interfase de operación.

4.3. *"Power generation" Triconex*

Este PLC protege las unidades de generación de energía y no sufrió cambios durante el revamping de los sistemas.

4.4. *Fire & Gas Architecture*

El sistema de Fire&Gas estaba basado en un sistema analógico marca Cerberus que realizaba las siguientes funciones:

- Adquisición de las señales de los detectores de Fuego, Gas y pulsadores de incendio ubicados en diferentes lugares de la planta

- Procesamiento de las señales por medio de tarjetas analógicas y generación de alarmas y señales de disparo por medio de contactos de salida
- Interconexión de los contactos generados con el sistema ESD 400 para ser usados en la matriz de Fuego y Gas

5. Tecnología Utilizada

Como se dijo, el objeto de la actualización tecnológica fue reemplazar la tecnología convencional utilizada en el ESD basada en PLCs estándares por un PLC de seguridad con certificación SIL que responda a los estándares de la compañía.

La anterior tecnología además de no ajustarse a los estándares de Total se encontraba en un grado de obsolescencia y sobrecarga que hacían imposible su expansión futura.

Como parte del proceso se adaptaron las interfases gráficas, se realizó una estandarización de los módulos básicos de programa y se realizó el upgrade a las nuevas versiones del sistema de control de procesos (BPCS).

Para la implementación del sistema ESD y de Fire and Gas se adoptó la tecnología basada en el PLC Triconex™ que responde a una arquitectura TMR 2oo3.

El BPCS basado en el sistema IA Series™ fue actualizado en la versión de software y cantidad de estaciones de operación.

Como síntesis la implantación de la nueva tecnología contempló las siguientes actividades principales:

- Diseñar, construir, realizar los tests de aceptación, instalar y poner operativos los nuevos gabinetes conteniendo el sistema ESD basado en Triconex™
- Diseñar e instalar los nuevos detectores de fuego y gas
- Diseñar e instalar los nuevos gabinetes de interconexión de las señales de campo, por medio de los cuales se efectuará la migración par por par de todas las señales correspondientes al sistema ESD
- Desarrollar, implementar, realizar las pruebas de aceptación y comisionar todas las aplicaciones correspondientes al sistema ESD
- Desarrollar, implementar, realizar las pruebas de aceptación y comisionar todas las nuevas interfases gráficas correspondientes al sistema ESD. Toda la interfase gráfica tanto de operación como de mantenimiento fue rediseñada e integrada al sistema BPCS. El sistema anterior utilizaba una interfase gráfica separada para el sistema de seguridad, basada en un paquete de software INTOUCH™ de propósitos generales
- Desarrollar los procedimientos detallados de transferencia de lazos (Switch Over Procedures)

5.1. *Detalle de las actividades*

El PLC correspondiente al sistema ESD 400 debe ser decomisionado y reemplazado por el nuevo PLC Triconex™. Todas las funciones de seguridad, Emergency Shut Down y Fire and Gas deben ser implementadas en el Nuevo equipamiento en base a la matriz de Shutdown aprobada por la Compañía.

Los gabinetes de cruzadas existentes deben ser mantenidos y nuevos gabinetes de interconexión con las señales de campo deben ser agregados para permitir la interconexión de un cierto número de nuevas señales al nuevo PLC.

Las funciones de telemetría implementadas en el PLC5 A&B deben ser transferidas al BPCS por medio de una nueva interfase de conexión agregada al hardware existente del equipamiento. De esta manera, todas las funciones de control y monitoreo de información remotas quedan segregadas del sistema del seguridad.

El sistema de Fire and Gas Cerberus™ debe ser decomisionado. El gabinete debe ser mantenido para realizar la interconexión de las señales de campo con el nuevo PLC de seguridad, el cual realizará todas las funciones correspondientes a alarmas y paros. Todas las señales de Fire and Gas son segregadas en tarjetas de IO y chasis separados del resto de las señales de seguridad y ESD. Como parte de los trabajos a realizar sobre el subsistema de F&G se reemplazan los detectores de Gas y Fuego por detectores nuevos, con salida 4-20 mA los cuales se conectan directamente a las entradas del sistema Triconex™. Los detectores de humo se mantienen, aunque se realizan modificaciones agregando divisores resistivos para convertir las salidas de contacto a entradas de 4-20 mA del nuevo sistema, lo cual permite no solamente detectar alarma sino también dar una indicación de cable cortado (falla).

El sistema INTOUCH™ debe ser decomisionado y la interfase de operación rediseñada e implementada a través de la interfase gráfica del BPCS. Esto permite contar con una única interfase de operación, consistente en características operativas con las existentes en el resto de los sistemas de Planta.

El diseño de los gabinetes de cruzadas y la estructura de la configuración debió ser hecha teniendo en mente que el proceso de cambio de las señales se realizaría en caliente, es decir con planta en operación. Durante todo el proceso el sistema EDS 400 y el nuevo Triconex deberían “convivir”, con un mínimo de complicaciones operativas y minimizando los riesgos. Las funciones evaluadas como criticas serían migradas en frío durante un paro de planta cuya duración no podría extenderse por un período superior a 24 hs. Este paro se realizaría aprovechando el paro programado para la integración del 4to Compresor al resto de las unidades.

5.2. *Dimensionamiento de los sistemas*

El nuevo sistema debe contener entradas salidas suficientes para:

- Señales existentes
- Nuevas señales correspondientes al 4to Compresor
- Señales del sistema de Fire and Gas correspondientes a los nuevos detectores con salida analógica

I/O Sistema EDS existente

I/O type	Quantity
AI (Two wires)	31
DI (Triplex)	128
DI (Simplex)	262
DO (Triplex)	162
DO (relays)	10

I/O correspondiente al 4to Compresor

I/O type	Quantity
AI (Two wires)	17
DI (Triplex)	3
DI (Simplex)	22
DO (Triplex)	20
AI (three wires)	10

I/O para Fire and Gas

I/O type	Quantity
AI (Two wires)	21
AI (Three wires)	94
DI (Triplex)	26
DI (Simplex)	
DO (Triplex)	17
DO (relays)	
DO (Supervised)	17

6. Fases del Proyecto y sistemas involucrados

El planeamiento de las diferentes actividades se realizó teniendo en cuenta que se contaría con un paro programado de planta de cómo máximo 2 días en Enero del 2007.

Se prestó especial atención a aquellas actividades que sólo podrían realizarse durante el paro de planta, como por ejemplo:

- Reubicación de cables correspondientes a señales críticas
- Interconexiones entre los sistemas de ESD
- SAT y comisionado de señales críticas
- Transferencia de los niveles de shutdown críticos

6.1.1. Preparación del trabajo

La preparación de las actividades es una tarea de ingeniería que fue realizada en diferentes etapas, con un grado de precisión creciente. Se definieron tres etapas principales: en la primera se definieron los procedimientos de trasferencia por cada Unidad/Planta y equipo, luego se definieron los procedimientos detallados para cada señal involucrada y finalmente se construyeron los paquetes de trabajo que permitieron definir los recursos y cronogramas de la migración.

6.1.2. Ejecución de la Transferencia

La transferencia de las señales se realizó bajo responsabilidad de Total, por un equipo formado por personal de Total y TECNA y de acuerdo al programa acordado con el área de operaciones.

6.1.3. Desmantelamiento del equipo obsoleto

Como último paso de los trabajos, todo el equipamiento antiguo fue removido e ingresado a depósitos de la Compañía.

7. Transferencia Paso a Paso

7.1. *Paso 1*

En esta etapa un equipo interdisciplinario formado por técnicos de la GP (Gerencia de Proyectos) de Total y de TECNA analizó y definieron la filosofía general con que se realizaría la transferencia. Se definieron aquellos lazos que deberían ser migrados en caliente (Hot Transfer) y aquellos que requieren paro de planta (Cold Transfer), teniendo en cuenta la seguridad de las instalaciones y los requerimientos operativos.

7.2. *Paso 2*

Durante esta etapa, se realizó la ingeniería de detalle: asignación de Tags, listas de cables, diagramas de conexionado y los nuevos diagramas de lazo.

Simultáneamente, se desarrollaron los procedimientos de migración específicos para cada "Tipo" de lazo, procedimientos que servirían como modelo a aplicar para el total de las señales.

Varias funciones críticas requirieron la implementación de conexiones temporarias "Hardwired" entre el PLC5 A&B y el nuevo PLC Triconex, a fin de posibilitar la transferencia manteniendo el nivel de protección en todo momento.

7.3. *Paso 3*

La última etapa fue la definición de los paquetes de trabajo, definidos como:

7.3.1. Paquetes de ESD/F&G

Se desarrolló un paquete de trabajo por cada nivel de Shutdown, conteniendo la siguiente información:

- Lista de señales a ser transferidas
- Display de INTOUCH and Foxboro para el nivel de shutdown específico
- Procedimiento paso a paso (uno por señal).
- Diagrama de Lazo existente
- Nuevo diagrama de Lazo
- Diagramas de conexionado

La tabla resume los niveles de Shutdown implementados por Planta:

Planta	ESD level 1	SD level 2	SD level 3
LTS 1	4	4	11
LTS 2	1	3	

7.3.2. Paquetes de trabajo para señales de Control y Monitoreo

Se desarrolló un paquete por cada display de proceso, conteniendo:

- Lista de señales a ser transferidas
- Display de INTOUCH and Foxboro
- Procedimiento paso a paso (uno por señal).
- Diagrama de Lazo existente
- Nuevo diagrama de Lazo
- Diagramas de conexionado

La siguiente tabla resume los displays involucrados en cada Planta:

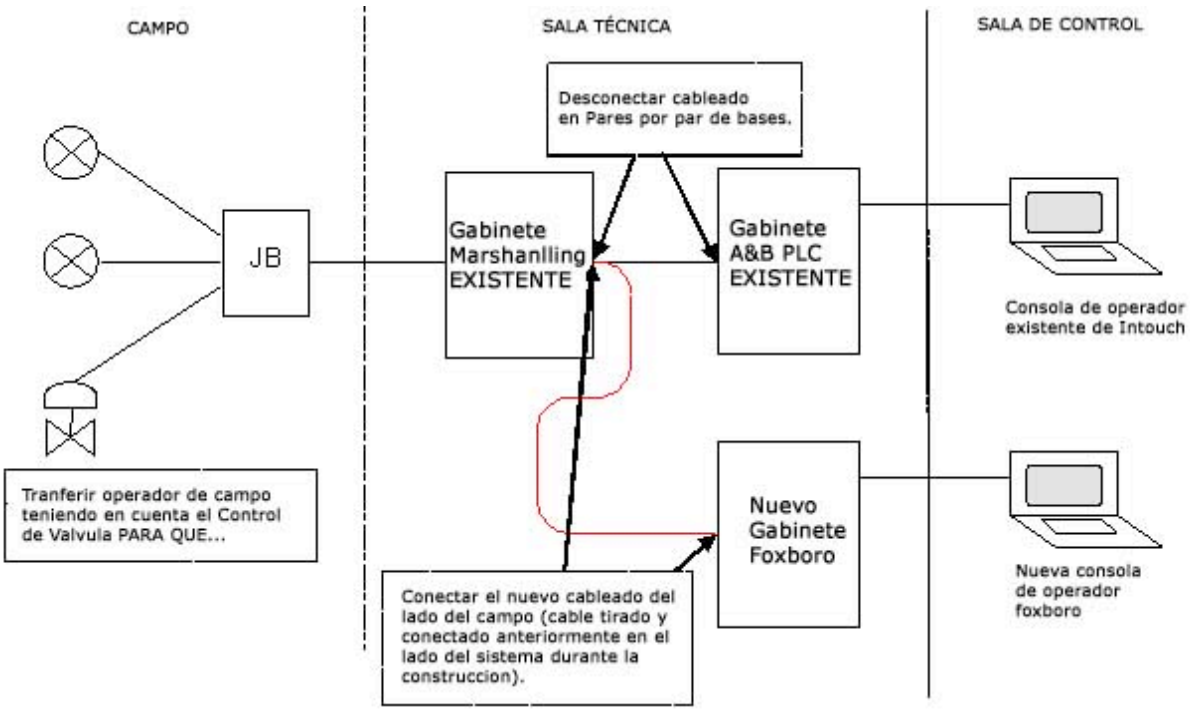
Plants	Process displays
LTS 1	9
LTS 2	24

8. Ejecución de la transferencia

8.1. *Transferencia en caliente de funciones de Control y Monitoreo*

La trasferencia se realiza en sala de control, donde cada par se desconecta desde su posición original y se reconectan a su nueva posición. Para cada señal a trasferir se ha especificado las acciones que deben tomarse a nivel de campo para permitir la trasferencia segura. Estas acciones pueden incluir la operación de bypasses, bloqueos, forzados manuales, etc.

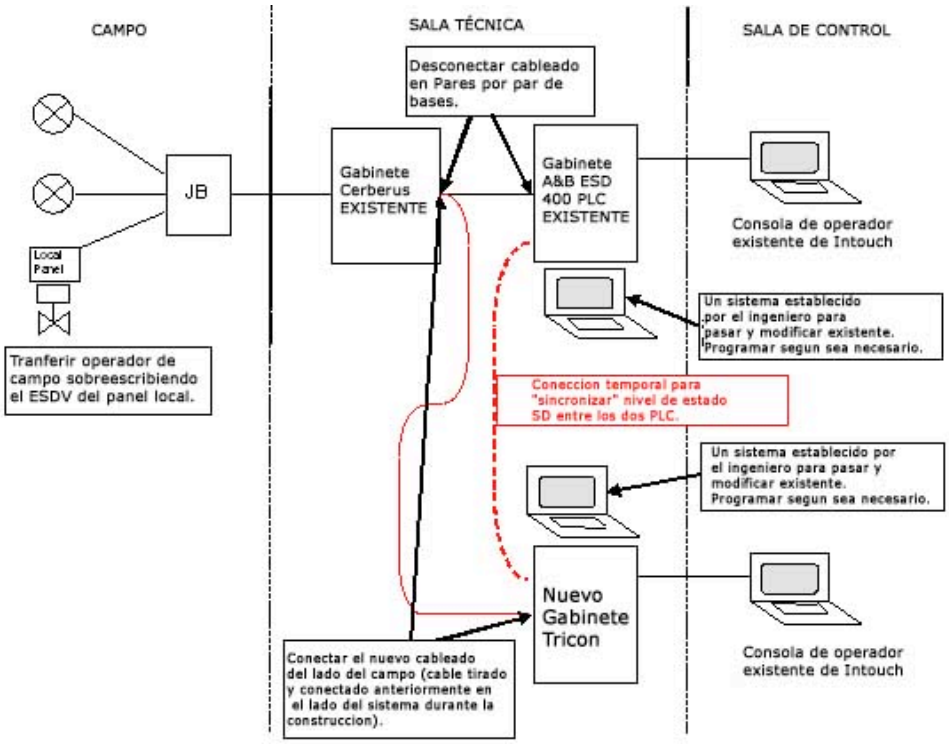
Typical DCS point transfer



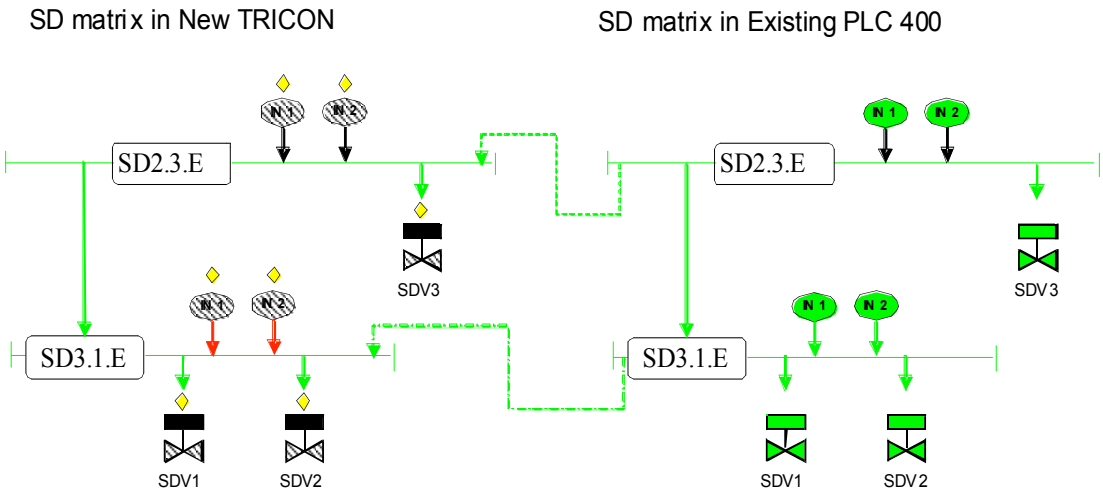
Los lazos trasferidos al sistema Foxboro™ IA (BPCS) fueron borrados del sistema INTOUCH, a fin de facilitar la coexistencia durante el proceso y atenuar el impacto sobre la operación, ya que durante toda la migración el operador debería convivir con lazos que se operaban desde el antiguo sistema mientras que otros se operarían desde las nuevas interfases.

8.2. *Transferencia en caliente de funciones de ESD*

Este es el tipo más crítico de transferencia, considerando que durante el proceso de cambio de las señales, la planta quedará protegida por dos equipos separados, en los cuales los correspondientes niveles de shutdown deberán estar “sincronizados”.



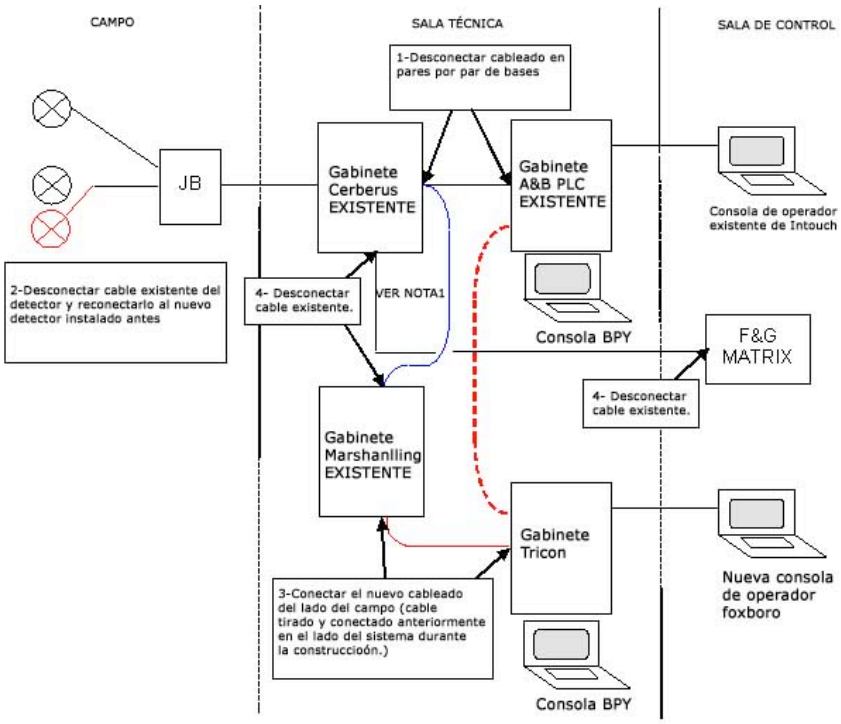
El concepto de sincronización de las matrices de SD de ambos PLCs se obtiene por medio de una conexión cableada que refleja el estado de la barra de SD en un equipo (Master ESD 400) como una entrada de Trip hacia el otro equipo (Slave Triconex)



8.3. *Hot Transfer of Fire and Gas detection*

Esta transferencia involucra cambios en sala, donde las señales provenientes de los detectores son conectadas al Nuevo sistema, a la vez que en campo se reemplazan los viejos detectores de Fuego y gas por los nuevos.

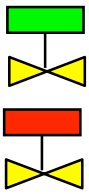
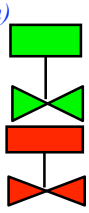
Typical Fire and Gas point transfer



Se muestra un ejemplo de procedimiento paso a paso para transferencia de una válvula ESDV, que se han mantenido en inglés que fue el idioma oficial con el que se manejó el proyecto. Para cada tipo de elemento se implementó un procedimiento similar.

9. Procedimiento Típico paso a paso para válvula ESDV

STEP	ACTIVITY DESCRIPTION	BY
1	*Select the relevant process displays from the Intouch and Foxboro operator's consoles (See graphic marked on ESD Work pack).*	Panel Operator
2	*Record the present status for the valve from the Intouch console, in appropriate column on the IO-Migration list (Closed/Open/Override active...Etc.).*	Panel Operator

STEP	ACTIVITY DESCRIPTION	BY
3	*Confirm that the SD bar associated to the valve have the same status in both systems.*	Panel Operator
4	*Confirm on the new screen that the valve has the following status for:* - *Case 1: Bar level in Normal State (Green)* *Open command from New System -------* *Discrepancy Status ----------* - *Case 2: Bar level in Tripped State (Red)* *Close command from New System -------* *Discrepancy Status ----------* 	Panel Operator
5	*From the local panel switch the valve to override in order to keep the actuator pressurized. The field operator shall confirm by radio to the control room that the valve is perfectly blocked and ready to be transferred.* *Note: If during this step a cause of shutdown appears, the valve actuator can be depressurized by the field operator, using the local close pushbutton, located on valve local panel.*	Field Operator
6	*Remove fuse or open knife in the existing ESD400 cabinet, The electrician will verify with an appropriate instrument (multimeter) that the solenoid is de-energized, and then disconnect the wires corresponding to the solenoid valve (SOV) in the existing ESD marshalling cabinet. Refer marked terminal blocks on existing loop part of ESD work pack.*	Electrician
7	*Check that all the causes which could trip the ESDV have been By Passed in the new system.*	System engineer
8	*In the new marshalling verify that the knifes corresponding to the relevant SOV are open, then connect the corresponding wires from the new marshalling cabinet to the existing terminal strip (refer appropriate annex in ESD work pack), close the knifes and verify presence of 24 VDC*	Electrician
9	*Open knife in the existing ESD400 cabinet, then disconnect the wires corresponding to the limit switches (ZSC & ZSO) in the existing ESD marshalling cabinet. The electrician will verify with an appropriate instrument (multimeter) that the switch is open (value=0) or closed (value=1) depending of the present status, see marked terminal block on existing loop.* *Note: in order to avoid errors and interpretations about the future status of the valve in the new system, not activated limit switch should be transferred first. (ZSC if valve is open, ZSO if valve is closed)*	Electrician
10	*In the new marshalling verify that the knifes corresponding to limits switches are open, then Connect the corresponding wires from the new marshalling cabinet on the existing terminal strip (see new loop on ESD work pack), close the knifes and verify switch status by checking presence or not of 24 VDC.*	Electrician
11	*Confirm on the new screen that the valve has the following status for:* - *Case 1: Bar level in Normal State (Green)* *Open command from New System -------* *Open Status ----------* - *Case 2: Bar level in Tripped State (Red)* *Close command from New System -------* *Close Status ----------*  *Record process values from the Foxboro screens (it shall be "identical" to the value recorded in step 2) in appropriate column on the IO-Migration list.*	Panel Operator
12	*Open knifes in the existing ESD400 cabinet, then disconnect the wires corresponding to the field reset (PB_____) in the existing ESD marshalling cabinet. The electrician will verify with an appropriate instrument (multimeter) that the PB is open (value=0).*	Electrician

STEP	ACTIVITY DESCRIPTION	BY
13	*In the new marshalling verify that the knifes corresponding to the field reset are open, then Connect the corresponding wires from the new marshalling cabinet on the existing terminal strip (see new loop on chapter 2), close the knifes and verify presence of 24 VDC.*	Electrician
14	*Open knife in the existing ESD400 cabinet, then disconnect the wires corresponding to the override valve (PSL_____) in the existing ESD marshalling cabinet. The electrician will verify with an appropriate instrument (multimeter) that the circuit is open (value=0).*	Electrician
15	*In the new marshalling verify that the knifes corresponding to the override valve are open, then Connect the corresponding wires from the new marshalling cabinet on the existing terminal strip (see new loop), close the knifes and verify presence of the yellow diamond on the new DCS display*	Electrician and Panel Operator
16	*Keep the local override valve active and test the available command and signals from the new system (Example: force from panel monitor (on Triconex) the output signal to de-energized the SOV in order to confirm that is working correctly; push on the local panel the reset button and verify the status change in the Triconex.*	System engineer; Panel Operator and Field Operator
17	*From the local panel remove the override valve and checking that the SDV remains in its position. Verify DCS screen (no yellow diamond)*	Field Operator and Panel operator
18	*Cancel or Delete point from Intouch system*	System engineer
19	*Stamp and sign off the new loop diagram to acknowledge transfer of the loop. Update the Operation master shut down matrix.*	Team leader System Engineer
20	*End of transfer*	

10. Conclusiones

- Los trabajos de actualización tecnológica implican riesgos que pueden evitarse o mitigarse por medio de una cuidadosa planificación de las actividades, adoptando la tecnología que mejor se ajusta en cada caso y realizando una ingeniería detallada y un exhaustivo conjunto de pruebas para cada sistema a implementar
- El valor agregado adicional de estas actividades subyace en la adecuación y revisión de las estrategias de control y seguridad implementadas, es decir, no simplemente cambiar la tecnología para implementar lo mismo sino aprovechar la inversión para dejar mejores y más eficientes sistemas de protección para personas e instalaciones
- Es de vital importancia la conformación de equipos de trabajo bien comunicados, donde estén involucrados todos los sectores que tienen intereses en las instalaciones: ingeniería, mantenimiento, operaciones y calidad, a fin de garantizar el cumplimiento de los estándares de la compañía y la trazabilidad de los equipos y desarrollos implementados.
- Los procedimientos de configuración basados en típicos que han sido testeados exhaustivamente antes de su propagación a todos los lazos del sistema han demostrado ser de crucial importancia en el desarrollo de los trabajos. La clave es trabajar antes, sobre los estándares y luego configurar sobre seguro.
- La elaboración de procedimientos típicos para cada tipo de lazo, con secuencias paso a paso garantizaron la mitigación y el manejo de los imprevistos a la hora de

realizar los cambios en caliente, evitando la pérdida de confianza que producen las tareas que presentan grandes inconvenientes durante las primeras etapas.

11. Referencias

1- Seguridad en Sistemas de Parada de Emergencia, *Luis Garcia – Solution Specialist – Siemens Energy & Automation Inc*
2- GS-EP-SAF-253 , Safety, General Specification, Total
3- GS-EP-SAF-261, Emergency Shutdown and Emergency Depresurization, General Specification, Total
4- SP-CAF-00595-06-J-034, ESD Hot Transfer, General Procedure, project document, Total/Tecna
5- SP-CAF-00595-06-J-035, Process Signal Transfer, General Procedure, project document, Total/Tecna