Sistema de Protección de Planta en ISOMAX

Fabian Verdun
Repsol-YPF

1.- Introducción

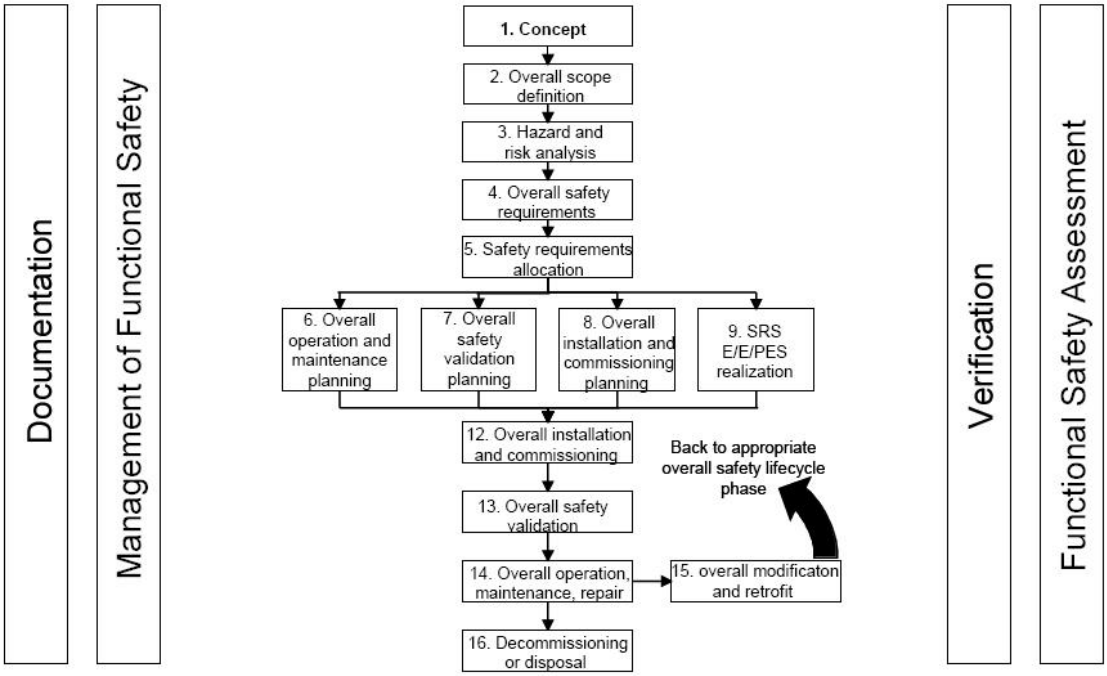
A partir de la norma alemana DIN V VDE 0801 y con el advenimiento de los microprocesadores en los sistema de protección, y por ende del software relacionado con estos sistemas, surge un estándar internacional que está dirigido a las funciones Eléctricas/Electrónicas/Programación de los sistemas de seguridad para toda clase de industria IEC 61508. Particularmente este estándar, a diferencia de los anteriores, basa sus requerimientos en la performance requerida para el sistema. Dicha performance se encuentra íntimamente relacionada con el nivel riesgo, lo cual significa que cuanto mayor sea el riesgo que se necesite disminuir, mayor serán los requerimientos exigidos al sistema de protección para alcanzar tal performance. El parámetro utilizado para medir estos requerimientos de performance de los sistemas de protección es el nivel de seguridad integrada o comúnmente conocido por sus siglas en inglés SIL. La IEC 61508 usa el nivel SIL para prescribir los requerimientos cuantitativos como así también cualitativos para desarrollo y uso del sistema de protección.

Este trabajo intenta dar al lector una pequeña introducción en la norma internacional IEC 61508, mencionando el concepto de ciclo de vida y se intentará contestar la pregunta de cuanta seguridad es suficiente**.** Por otro lado se mencionarán los detalles de implementación del sistema de protección de Isomax, el estudio de validación del SIL y sus consecuencias en relación al proyecto.

2.- Desarrollo

2-1.- Ciclo de Vida

Uno de los mayores avances introducido por la norma IEC 61508 es que su espectro no solo abarca los requerimientos técnicos del sistema de protección, sinó que tiene en cuenta el trabajo de selección, desarrollo, uso y administración de dicho sistema. Esto se ve plasmado en el concepto "Ciclo de Vida", el cual ordena todas las actividades relacionadas con el sistema de protección de manera sistemática.



CICLO DE VIDA

El ciclo de vida concretamente ayuda al usuario final a:

1) Entender el proceso desde el punto de vista de peligro y riesgo.
2) Trasladar estos peligros y riesgos a funciones de seguridad apropiadas.
3) Incluir estas funciones de seguridad dentro de sistemas de protección
4) Planear la realización, instalación, comisionado, validación, operación, mantenimiento y relación del sistema de seguridad.
5) Actualizar diseños y seleccionar los elementos que componen un sistema de protección para construirlo.
6) Instalar y comisionar, validar, operar, mantener y repara el sistema de protección
7) Decomisionar el sistema de protección cuando el mismo a llegado al fin de su vida útil.

2-2.- ¿Cuánta seguridad es suficiente?

La norma IEC 61508 define requerimientos específicos para la integridad de los sistemas de protección como lo puede ser la seguridad, y que se representa cuantitativamente en el nivel de integral de seguridad (SIL) para una función de seguridad específica y por ende para el sistema de protección. Hay cuatro niveles de requerimiento los cuales se pueden expresar de la siguiente manera:

SIL	PFD	Safety Availability	Risk Reduction
4	0.0001 – 0.00001	0.9999 – 0.99999	10000 – 100000
3	0.001 – 0.0001	0.999 – 0.9999	1000 – 10000
2	0.01 – 0.001	0.99 – 0.999	100 – 1000
1	0.1 – 0.01	0.9 – 0.99	10 – 100

TABLA DE SIL

El SIL en si mismo expresa la probabilidad de falla del sistema ante una demanda. Cuanto mas alto sea el valor de SIL, menor será la probabilidad de falla en demanda del sistema. Otra forma de expresar esto es la disponibilidad segura del sistema y la reducción del riesgo lograda.

Para contestar la pregunta realizada anteriormente nos debemos introducir primero en quien debe determinar cuanta seguridad es suficiente. No existe ninguna ley internacional que pueda ser usada para ser usada para decidir cuanta seguridad es suficiente, algunos países pueden tener algunas leyes nacionales que puedan ser usadas como una ayuda para determinar esto. Como así también se puede usar alguna guía que surja de las compañías aseguradoras. En definitiva quien debe decidir cuanta seguridad es suficiente es el dueño de la compañía.

Para ello debe determinar cual es su nivel de riesgo base alcanzado contemplando las primeras tres capas de protección que son el diseño de la planta, el sistema de control y los operadores. Se realizan análisis de peligro y riesgo dentro del cual se contemplan factores tales como ubicación física de la planta, los materiales usados, el proceso de producción, el nivel de entrenamiento de los operadores y así con muchos otros factores.

Una vez establecida esta línea base de riesgo, la compañía necesita tener en cuenta cualquier leyes nacionales, locales o cualquier estándar de la compañía para determinar el nivel de riesgo aceptable. En caso de que nuestra línea base no alcance el nivel de riesgo aceptable, se deberán incorporar capas de protección.

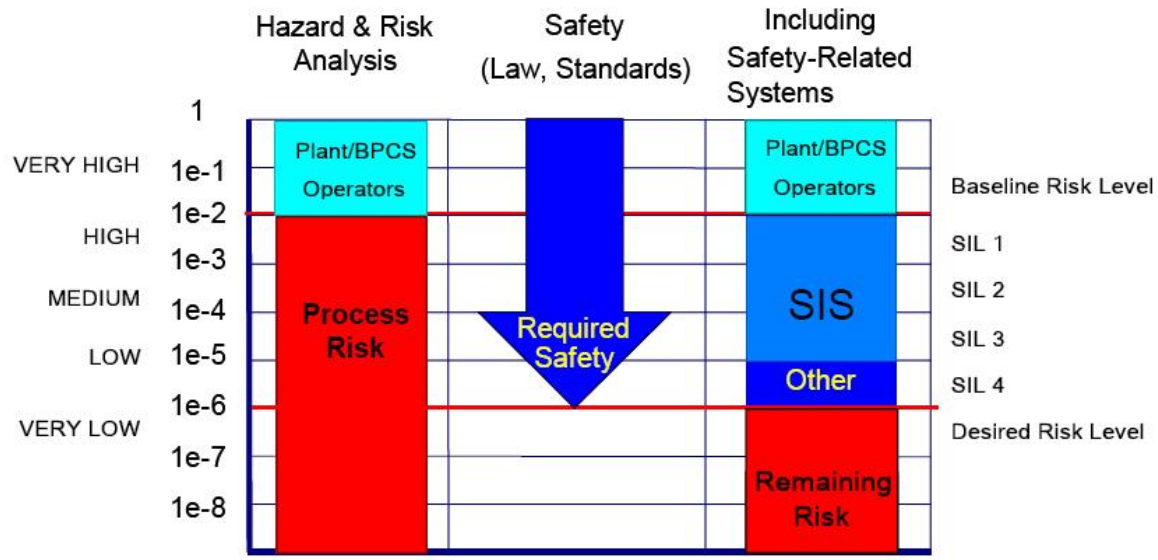


GRAFICO DE REDUCCION DE RIESGO

2-3.- Implementación

La implementación del sistema de protección de la planta de Isomax de Luján de Cuyo consistió en un sistema de protección basado en PLC de seguridad, situado en un nivel por encima de los sistema de protección individuales de equipo.

Se determinaron las distintas funciones de seguridad y sus correspondientes requerimientos de seguridad (SIL) en base a estándares conocidos por el licenciatario del diseño de la planta (UOP).

Las funciones de seguridad determinadas fueron:

Unicracking Process - Achieved SIL - Figure 2

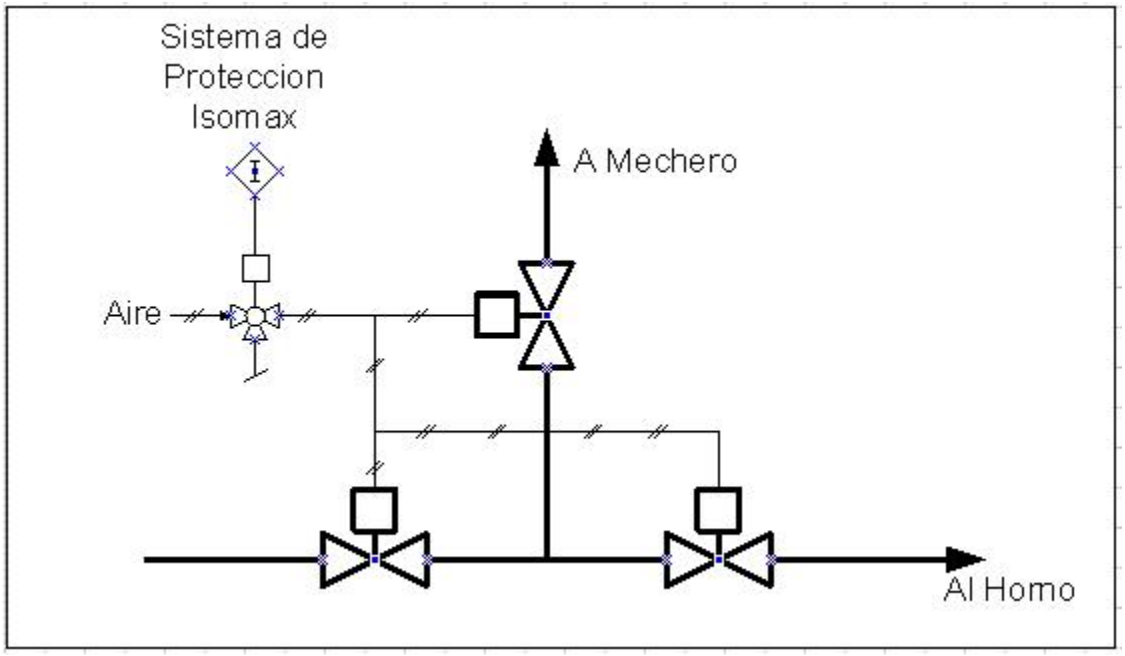
							Service	Charge Pumps	LXH1-A-Heater Pilot Gas Shutoff Valves	LXH1-A-Heater Fuel Gas Shutoff Valves	LXH1-A-Heater Fuel Oil Shutoff Valves	LXH1-A-Heater Fuel Oil Bypass Valve	LSH1-B-Heater Pilot Gas Shutoff Valves	LSH1-B-Heater Fuel Gas Shutoff Valves	LSH1-B-Heater Pilot Oil Shutoff Valves	LSH1-B-Heater Pilot Gas Bypass Valve	High Rate Depressuring	Low Rate Depressuring	Recycle Gas Compressor	Wash Water Pumps	Wash Water to Condenser	Makeup Gas
	Req'd			Voting	Sensor Component PFD		Tagname	LX-P1A/B	MV-7041/7043	MV-7044/7046	MV-7050/7051	MV-7052	MV-7341/7043	MV-7344/7046	MV-7350/7051	MV-7352	UV-9901	UV-9903	LX-C1	LX-P2A/B/C/D	UV-9904	PV-0186
SIF #	SIL	Tagname	Service	Required	(*E-03)																		
1	1	TSHH-xxxx (several)	Reactor Bed	1oo1	16.9			S		C	C	O		C	C	O	O		S	S	O	O
2	1	TSHH-xxxx (several)	Reactor Bed	1oo1	16.9			S		C	C	O		C	C	O	O		S	S	O	O
3	2	FSLL-7080A/B/C	Recycle Gas to Combined Feed Exch	2oo3	0.033			S		C	C	O		C	C	O		O	S	S	O	O
4	2	PSLL7040A/B/C	LXH1-A Heater Pilot Gas	2oo3	0.024				C	C	C	O										
5	2	PSLL7340A/B/C	LXH1-B Heater Pilot Gas	2oo3	0.024								C	C	C	O						

Tabla causa efecto

La implementación del sistema fue realizada por la empresa Honeywell bajo la supervisión de la Dirección de ingeniería de ABB (DIABB). La construcción del sistema de protección demandó la instalación de nuevos sensores, adecuación de otros, instalación de un PLC seguridad e instalación de nuevos actuadores. Se desarrollaron pantallas de visualización específica para dicho sistema, que están siempre visibles desde la estación de trabajo del operador.

Una vez finalizada la implementación del sistema, se realizó un estudio de validación de SIL a fin de corroborar que lo construido alcanzaba el nivel de SIL especificado en la etapa de diseño. Sin embargo, el estudio (realizado por un tercero) no arrojó los resultados esperados. Las funciones de seguridad diseñadas no alcanzaron el nivel de SIL requerido, en la mayoría de los casos solo alcanzaron SIL 0 y en otros alcanzaron marginalmente SIL 1.

En el estudio se señala que los sensores y el programador de lógica (PLC de seguridad) son apropiados para encontrar los requerimientos de SIL. Los mayores inconvenientes para alcanzar SIL 2 están relacionados con el arreglo de solenoides – válvulas; en la mayoría de los casos múltiples válvulas son manejadas por una simple solenoide. A continuación se muestra gráficamente el arreglo mencionado:



La experiencia de quien realizó el estudio indica que un arreglo de este tipo no alcanza SIL 2, a menos que se implementen las siguientes modificaciones:

a) Realizar una configuración redundante con el fin de que con cualquiera de las válvulas que actúe se alcance el estado seguro.
b) Realizar testeos mas frecuentes, 12 meses. Esto no se corresponde con la frecuencia de testeo planteada (48 meses) en el diseño.

También sugiere instalar Partial Stroke. Esta alternativa es la de menor costo ganando además en seguridad. Sin embargo el efecto de estas alternativas en cuanto al SIL no se ha calculado.

3.- Conclusiones

Mas allá de implementar las soluciones sugeridas para lograr el nivel SIL requerido es importante detectar cuales son los puntos importantes que impidieron lograr una construcción exitosa:

1) El estudio de validación se basó en una revisión de la norma y la especificación realizada en otra.

2) falta de experiencia en implementación de estos sistemas. Un estudio de validación una vez finalizada la ingeniería de detalle hubiera permitido detectar las anomalías que pudieran existir y decidir su re-diseño.

3) Falta de experiencia en el uso de las herramientas utilizadas para el cálculo del SIL.

La experiencia resultó muy positiva para el complejo. Se logró capacitar al personal en un tema tan nuevo como lo son estos estándares. Se está analizando la implementación de las modificaciones propuestas.

4.- Bibliografía

a) Safety Integrity Level Selection, Ed Marszal y Eric Scharpf (ISA)
b) IEC 61508, An Introduction To The Safety Standard For End Users, Dr. Michel J.M. Houtermans.
c) Reporte Validación SIL, James Halle.
d) Control Systems, Safety Evaluation & Reliability, William Globe, (ISA)