HASIL, UN PROTOTIPO PARA EL DESARROLLO DE HAZOP/SIL

Nicolás Scenna* ^, María del Carmen Real* y Néstor Rodríguez+

* INGAR: Instituto de Desarrollo y Diseño, Avellaneda 3657 – 3000 Santa Fe
+ UTN- FRRo: Universidad Tecnológica Nacional, Facultad Regional Rosario,
Zeballos 1341 – 2000 Rosario.
^ nscenna@ceride.gov.ar

Resumen

La adopción del estándar IEC 61511 introdujo un nuevo desafío a los proyectos ingenieriles. La determinación de los niveles SIL (Safety Integrity Level o nivel de integridad en seguridad).

En la industria de procesos, en general, esta determinación se lleva a cabo luego de realizar un HAZOP u otro método de análisis de riesgo equivalente.

Mientras que la práctica de análisis HAZOP está bien establecida no sucede lo mismo con el relativamente nuevo estudio SIL, o los análisis relacionados como el LOPA (Layer of Protection Analysis o análisis de capas de protección). En general, varios procedimientos usan una combinación de herramientas para determinar el SIL.

La forma tradicional de desarrollar el análisis HAZOP y la evaluación SIL es tratarlos como tareas separadas. Primero un equipo experimentado realiza el HAZOP. Se identifican aquí los escenarios y sus riesgos asociados usando una matriz para cuantificarlos, documentándose los resultados generalmente en una planilla Excel específicamente diseñada o con algún software comercial.

Luego debe convenirse otra sesión para completar la evaluación SIL, por ejemplo utilizando la metodología de Análisis de capas de protección (LOPA) u otra. Un equipo multidisciplinario conducido por un líder experimentado en el método completa la evaluación SIL.

Por último se lleva a cabo una tercera etapa llamada Validación SIL que es entonces elaborada usando un conjunto distinto de herramientas.

El resultado final del proceso es típicamente un conjunto de tres reservorios de datos conteniendo aquellos provenientes de los tres diferentes estudios o etapas.

El objetivo de este trabajo es presentar un prototipo (software) llamado SIAR (sistema integrado de análisis de riesgos) para la documentación y el apoyo en la ejecución de análisis cualitativos de Riesgos (HAZOP, WHAT IF; FMECA) y los semicuantitativos (como LOPA), al igual que la determinación de los niveles SIL.

En particular, se hará hincapié en una herramienta específica del software SIAR (llamado HASIL) que tiene por objeto permitir la evaluación de los niveles SIL para las funciones instrumentadas de seguridad (FIS); integrando esta actividad con la del HAZOP clásico.

Introducción

Desde hace tiempo, en función de la experiencia obtenida por el grupo de Análisis de Riesgos del INGAR (UTN-CONICET) y el GIAIQ (UTN-FRRo) en la realización de diversos estudios de Riesgos (identificación de escenarios, evaluación de las consecuencias), ante la necesidad de contar con una herramienta adecuada de almacenamiento de datos y elaboración de informes de los resultados obtenidos, se comenzó con el desarrollo del software SIAR. El mismo básicamente se construye a partir de una base de datos que contiene la información adecuadamente codificada del

análisis de Riesgo efectuado, identificando caso, plantas, fechas, tipo de estudio y todo otro dato relevante que identifique el objeto de estudio y sus resultados.

La forma de presentar los informes, (planillas en formato Word o pdf), dependerá del tipo de estudio realizado (WHAT IF, HAZOP, FMECA, etc.).

En función de la creciente masificación del estándar IEC 61511 en nuestro medio, y la consecuente necesidad del desarrollo de análisis de niveles SIL, o del tipo LOPA, se ha incorporado al software SIAR, un programa (HASIL), que permite la evaluación del nivel SIL, integrado a la realización del Análisis HAZOP. Obviamente, en su desarrollo se ha utilizado toda la arquitectura y elementos disponibles en SIAR para el desarrollo del HAZOP convencional.

Por último, SIAR puede realizar análisis LOPA, a través de un programa incorporado, cuyo desarrollo ha seguido los mismos lineamientos que para el programa HASIL.

A continuación, se comentan brevemente los fundamentos del análisis HAZOP y LOPA, para facilitar la comprensión del presente trabajo. Además, se explicarán brevemente algunos conceptos del análisis SIL, en particular resaltar las principales metodologías existentes para el cálculo de niveles SIL; a los efectos de luego presentar sucintamente las características del software HASIL, sus alcances y limitaciones.

I- Análisis HAZOP

Como es conocido, el análisis HAZOP consiste en una metodología sistemática desarrollada por un grupo multidisciplinario que permite identificar todos los escenarios de riesgos y analizar sus consecuencias, cubriendo todo el proceso / planta / procedimiento bajo análisis. Para ello se separa el proceso en nodos, y a cada uno de ellos se los analiza utilizando un conjunto de palabras guías (entre ellas: nada de, más de, menos de, otro de, etc.) aplicadas a parámetros fundamentales del proceso (por ejemplo: temperatura, caudal, presión, etc.), a los efectos de generar desviaciones sobre el comportamiento normal (como pueden ser: más caudal, menos temperatura, etc.). Para un proceso transitorio debe agregarse la variable temporal a esta estrategia (nuevas palabras guía que cubren la variable temporal).

Es responsabilidad del grupo multidisciplinario encontrar todas las causas (escenarios) que dan lugar a estas desviaciones. A cada una de ellas, se le evalúa las consecuencias. En general, también se evalúa cualitativamente el Riesgo, utilizando una matriz de riesgo como la se indica en la figura 1. Este es solo un ejemplo, dependiendo del criterio y objetivos de gerenciamiento de riesgo que se tenga en la empresa, la forma de expresar los elementos de la misma. En ella se discretiza (aquí en 4 niveles), el rango numérico de valores de la frecuencia y la severidad. El resultado (Riesgo = Frecuencia x Severidad) obviamente resulta discretizado en el mismo rango.

Frecuencia \ Severidad	B	M	A	E
B	B	B	M	M
M	B	M	M	A
A	M	M	A	E
E	M	M	A	E

B: bajo, M: Medio, A: Alto, E: Extremo

Figura 1-Matriz de Riesgo HAZOP

Los hallazgos del grupo HAZOP se vuelcan en una planilla como la indicada en la figura 2. Debe remarcarse que existen otras formas (planillas) de presentar los resultados, según la manera en que se recorra el proceso (por palabras quía, por parámetros, etc.) o en la forma que se desee agrupar la información. No obstante, salvo en la presentación de los datos, en general contienen la misma información, y son conceptualmente equivalentes. El formato de la figura 2 es el que genera SIAR.

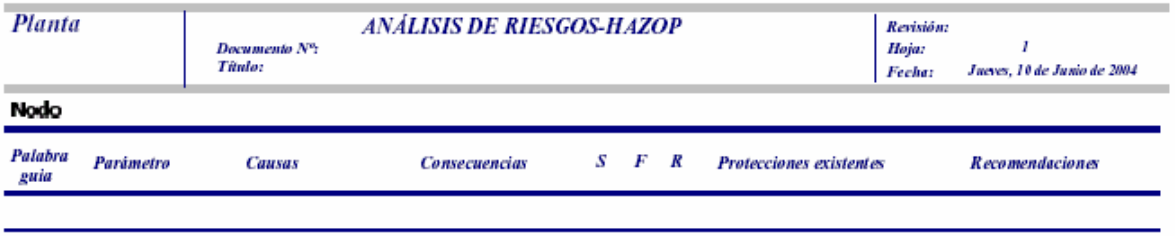

Figura 2-Planilla HAZOP convencional

Según puede observarse en la figura 2, existe una columna de protecciones existentes (salvaguardas) y otra de recomendaciones. En la primera de ellas, se enumeran todas las capas de protección que existen frente al evento iniciador, en función de las consecuencias observadas. Sin embargo, no existe un formalismo para analizar su independencia, modos comunes de falla, etc. El contenido de la columna Recomendaciones surge de realizar un "balance" entre las "protecciones existentes" con el riesgo asociado al escenario. No existe por ejemplo, una metodología para especificar (una vez recomendada su necesidad), una Función Instrumentada de Seguridad (FIS). Dada esta subjetividad, con el advenimiento de sistemas computarizados cada vez más complejos (PLC, etc.), la norma IEC 61511 sistematiza dicho análisis, para formalizar las "recomendaciones", en particular en los casos de mayor riesgo.

Aquí conviene realizar un alto y evaluar ciertas características del análisis HAZOP. La variante más utilizada (y aconsejada) es determinar la frecuencia del evento iniciador (o causa) independientemente de las protecciones existentes. La consecuencia igualmente. Es decir, el riesgo se evalúa en función del evento iniciador y su desarrollo, cristalizado en la Severidad de las consecuencias, independientemente de las protecciones existentes. Luego se explicitan éstas (considerando además de las alarmas, los enclavamientos, los indicadores o medidores, controladores, acciones posibles del operador, el mantenimiento y su nivel si existiese, etc.). Del balance entre el riesgo y las protecciones surgen las recomendaciones que propone el grupo HAZOP.

En otras filosofías de desarrollo del análisis HAZOP, se evalúa el riesgo, contemplando las salvaguardas o protecciones, y en función del resultado (si es "aún así" inaceptable), entonces se realizan recomendaciones. Esta metodología consideramos aquí que no es aconsejable, en particular si se requiere integrar luego el análisis HAZOP a la determinación de los niveles SIL o con un análisis LOPA posteriormente al HAZOP.

Otra variante realiza, luego de las recomendaciones, una nueva evaluación de la frecuencia y severidad para determinar el riesgo contemplando ahora las salvaguardas y las recomendaciones. Este procedimiento es más exacto, pero consume mayor tiempo, y como se verá más adelante, aquí consideramos preferible dedicar este tiempo a integrar el HAZOP con la determinación de los niveles SIL, ya que es un procedimiento menos subjetivo para la especificación de las FIS.

Por último, debe aclararse que se supone en el desarrollo del HAZOP, la ocurrencia de una sola falla (la que da origen al escenario bajo análisis). Por lo tanto, todos los demás elementos del sistema se suponen funcionan normalmente.

Al plantear las capas de protección y analizar las recomendaciones, sin embargo, existen problemas tales como: ¿existen fallas de causa común con el escenario planteado? , ¿qué sucede si falla una capa de protección? ¿y sus consecuencias ante un escenario de riesgo muy alto? ¿cómo evaluar en forma objetiva la necesidad de agregar elementos de protección nuevos al sistema? Es

evidente que el método HAZOP no nos proporciona, desde este punto de vista, metodológicamente, una forma adecuada para especificar nuevas capas de protección (o eliminarlas si es necesario o conveniente). Tampoco nos da una metodología sistemática para analizar las potenciales fallas de los elementos de seguridad que se introducen en las recomendaciones ya que ellas no aparecen como causa asociada en las desviaciones, ya que no forman parte del proceso.

Estas limitaciones, son inherentes a la metodología HAZOP, por ello se recomienda la evaluación de los niveles SIL, para las Funciones Instrumentadas de Seguridad, o la evaluación LOPA, para determinar más precisamente la Probabilidad de Falla ante Demanda (PFD) del sistema de protección o mitigación en su conjunto ante cada escenario.

Esta limitación del método no debe extrañarnos ya que el HAZOP naturalmente está planteado para detectar todos los posibles escenarios de riesgo; nos provee una forma de evaluarlos cualitativamente al utilizar la matriz de riesgo, pero no puede pedírsele además, una manera sistemática y eficiente de resolver la especificación de las capas de protección necesarias en cada caso. En el ámbito del análisis HAZOP, este hecho dependerá de la experiencia del grupo de análisis (y por lo tanto, es una solución subjetiva).

II- Análisis de capas de protección (LOPA)

El procedimiento LOPA es un intento de analizar el número de capas de protección necesarias (introducido por la CCPS Center for Chemical Process Safety) en 1993 con título “Guidelines for Safe Automation of Chemical Processes”.

LOPA es una técnica semi-cuantitativa de análisis de riesgos que aún cuando en forma usual genera un valor numérico conservador para el riesgo, utiliza usualmente órdenes de magnitud bastantes aproximados. Una tabla indicativa de los resultados de un análisis LOPA es la siguiente. Para lograr una mayor aproximación sería necesaria la realización de un Análisis de Árbol de Fallas. En la tabla indicada, agregamos aquí la columna del SIL, el cual se calcula según información disponible en las otras columnas, y criterios estándar, incluido el target o valor deseado por la empresa para el riesgo, si los hubiese. Si existiese ya la FIS, el SIL se calcula como valor de referencia, para compararlo con el diseño adoptado.

Evento de inicio (Causa)	Consecuencia	S (Severidad)	Capas de Protección Independientes Probabilidad de falla ante demanda (PFD)				(PFD) Sistemas de protección	Frecuencia de la consecuencia mitigada lyr. F_i^C	SIL necesario según estándares
			Capa 1	Capa 2	Capa 3	FIS			

Figura 3-Planilla LOPA

Los métodos para la determinación de los niveles SIL se describirán más adelante.

La severidad de la consecuencia se estima usando técnicas apropiadas las cuales van desde simples tablas hasta sofisticadas herramientas informáticas de modelado. Uno o más eventos iniciales (causas) pueden desencadenar una consecuencia particular. A cada causa-consecuencia se denomina escenario. LOPA estudia un escenario a la vez. La frecuencia de los eventos iniciales es un valor estimado. Notar la diferencia con HAZOP. Cada salvaguarda identificada se evalúa para dos características claves.

- ¿La salvaguarda es efectiva para prevenir los alcances de la consecuencia?
- Y, la salvaguarda, ¿es independiente del evento de inicio y de otras capas de protección independientes (CPI)?

Si la salvaguarda satisface ambas cuestiones entonces es una capa independiente de protección (CPI). LOPA estima la probabilidad de consecuencias indeseables mediante la multiplicación de la

frecuencia del evento inicial por el producto de las probabilidades de falla ante demanda (PFD) para las CPI usando la ecuación:

$$f_i^C = f_i^I * \prod_{j=1}^{J} PFD_{ij} = f_i^I * PFD_{i1} * PFD_{i2} * ... * PFD_{iJ}$$

donde:

f_i^C = *frecuencia para la consecuencia C para el evento i*

f_i^I = *frecuencia para el evento de inicio i*

PFD_{ij} = *probabilidad de falla ante demanda de la j−ésima CIP que protege de la consecuencia C para el evento de inicio i*

El resultado del LOPA es la estimación del riesgo para el escenario considerado. También se estima la frecuencia mitigada, mitigación que es lograda a través de las capas independientes de protección. El riesgo estimado puede compararse con los criterios tolerables de riesgos en una compañía. Así, si se requiere una reducción del riesgo deben agregarse más capas independientes de protección al diseño o rediseñarse las existentes. En algunos casos puede llegar a ser necesario rediseñar el proceso (pudiendo hacerse uso de diseños inherentemente seguros).

En la bibliografía se resalta que es importante considerar escenarios que tengan una sola causa y una sola consecuencia, ya que el no hacerlo es una fuente común de equivocaciones al plantear esta técnica.

Además, se debe comprender el significado de una capa de protección independiente (CPI). Esta es un dispositivo, sistema o acción que es capaz de evitar las consecuencias indeseadas de un evento inicial independientemente de la acción de cualquier otra capa de protección asociada con el escenario. La efectividad e independencia debe ser certificable. Todas las CPI son salvaguardas, pero no todas las salvaguardas son CPI. Un punto crítico para el análisis LOPA es la determinación no sólo de las CPI sino también de su independencia del evento inicial o de cualquier otro. La metodología LOPA se basa en la asunción de dicha independencia. Si existen modos de fallas comunes entre los eventos iniciales y las CPI, los resultados del análisis LOPA subestimarán el riesgo de dicho escenario.

En general los procedimientos e inspecciones no pueden ser considerados como CPI ya que no tienen la capacidad de detectar al evento inicial, no pueden tomar una decisión o realizar una acción para evitar las consecuencias. Las inspecciones y pruebas tampoco se consideran CPI ya que no afectan a la PFD (Probabilidad de falla ante demanda) de la CPI.

Por último, una CPI puede evitar las consecuencias identificadas para el escenario pero a través de su acción podría generar otra consecuencia menos severa aunque todavía indeseable. Un disco de ruptura de un recipiente es un buen ejemplo.

El mismo protege al recipiente de una sobrepresión (aunque no en un 100% de las veces, el disco de ruptura tiene una PFD). Sin embargo, la acción correcta del disco de ruptura resulta en una pérdida del contenido del recipiente hacia el medio ambiente hacia un contenedor o sistema de tratamiento. La mejor forma de tratar con esta situación es realizar otro escenario LOPA para estimar la frecuencia de escape a través del disco de ruptura, sus consecuencias y entonces determinar si el mismo alcanza un criterio de riesgo aceptable.

III- Determinación de los niveles SIL

Como se ha mencionado, para cada Función Instrumentada de Seguridad (FIS), se debe asociar un nivel de seguridad (SIL) que la caracteriza. En otras palabras, los requerimientos de funcionamiento (PFD) que deberán lograrse con el diseño (arquitectura) adecuada.

Existen varios métodos propuestos para la evaluación de los niveles SIL, dependiendo por ejemplo del tipo de industria, del nivel de rigurosidad exigida, etc. A continuación se desarrollan las más comunes. Una de las formas, como se ha visto, es a través de un análisis LOPA.

El estándar internacional IEC 61508 ha sido ampliamente aceptado como base para el diseño y especificación de los sistemas instrumentados de seguridad (SIS). El estándar hace uso de análisis de riesgos para decidir el (SIL) necesario para cada FIS que sea contenida en un dado SIS.

Los niveles SIL se enumeran de 1 a 4 en donde 4 representa el máximo nivel de integridad. La velocidad de falla objetivo se asigna a cada SIL tanto en términos de probabilidad de falla ante demanda como en fallas por hora (en casos de procesos de operación continua). Estos valores se reproducen en la tabla siguiente:

SIL	Probabilidad de falla por hora	Probabilidad de falla ante demanda
4	10^{-9} a $< 10^{-8}$	10^{-5} a $< 10^{-4}$
3	10^{-8} a $< 10^{-7}$	10^{-4} a $< 10^{-3}$
2	10^{-7} a $< 10^{-6}$	10^{-3} a $< 10^{-2}$
1	10^{-6} a $< 10^{-5}$	10^{-2} a $< 10^{-1}$

Figura 4

Una vez que el diseñador ha seleccionado el SIL apropiado las nomas IEC 61508 contienen toda la información necesaria para que dicho nivel de integridad pueda ser alcanzado. Algunos puntos a considerar son:

- Las categorías se relacionan directamente con la fiabilidad,
- Las fallas sistemáticas se consideran en forma explícita,
- La importancia de la garantía de calidad del diseño que asegure la seguridad funcional se reconoce y abarca con detalle,
- Sin embargo el estándar es complejo, nada fácil de aplicar y parece ser un tanto burocrático.

En general, para la industria química el SIL 4 no es recomendable. Ante esta situación se requiere un rediseño del sistema. A continuación se detallan algunas de las formas habituales del cálculo de los niveles SIL. No se pretende hacer una descripción detallada, ni menos aún precisa del cálculo de tales niveles. Se los menciona a modo de ejemplo. Cada compañía a través de los estándares definidos por la misma; y las normas específicas, son la guía a seguir para la determinación de dichos niveles.

III. 1 IEC 61508 (International Electrotechnical Commision)

El IEC 61508 adopta para el cálculo del SIL el uso de una gráfica de riesgo. Se usan 4 parámetros para seleccionar el SIL. Al incluir la probabilidad de anulación y la frecuencia de exposición al evento indeseado combinado con la frecuencia y severidad del evento, el cálculo se complica en cuanto al tiempo empleado y los datos necesarios.

III. 2 DEF STAN 00-56/Issue 2

Se trata esta de una familia de estándares desarrolladas por el Ministerio de Defensa de los EE. UU. (MOD) tomando en cuenta normas internacionales de estandarización. Este estándar está dividido en 2 partes. En la primera se describen los requerimientos para el manejo de la seguridad incluyendo análisis y estudios de riesgo mientras que en la segunda parte se provee información genérica y guía para el manejo de la seguridad necesaria en los sistemas relacionados.

El concepto de riesgo y sus consecuencias se describen en la parte 1 sección 7,4 de este estándar el cual introduce una técnica interesante para la selección del SIL. La matriz está basada en 2 parámetros como se aprecia en la siguiente tabla (una simplificación).

Probabilidad del evento de origen	Severidad del accidente			
	Catastrófica	Crítica	Marginal	Despreciable
Frecuente	Nivel SIL 4			
Probable		Nivel SIL 3		
Ocasional			Nivel SIL 2	
Remota				
Improbable			Nivel SIL 1	

Figura 5

III: 4 Método basado en la controlabilidad del evento.

El principal concepto detrás de ésta técnica es la introducción de heurísticos para la determinación del SIL. Por ejemplo según el concepto de controlabilidad. En efecto, entre una falla y un accidente hay una cierta pérdida de control y es esta pérdida de control lo que se clasifica. Cada riesgo es estudiado por el grado de control remanente después de que la falla ha ocurrido. En la Fig. 6 se detalla una posible organización de las categorías de controlabilidad que podrían seleccionarse. De esta forma se define el SIL requerido para la velocidad de falla aceptable.

Nivel de controlabilidad	Velocidad aceptable de falla	Nivel de integridad
Incontrolable	Extremadamente improbable	4
Difícil de controlar	Muy remota	3
Fluctuante	Remota	2
Ruido que supera la banda normal de operación	Ocasional	1

Figura 6 – Posible asignación de SIL de acuerdo a los niveles de controlabilidad

Se ha descrito arriba, a modo de ejemplo, algunas variantes para el cálculo del SIL. En un trabajo (Summers, 2003) describe un repaso de tales técnicas. Se destaca que la técnica más simple y conservadora que puede utilizarse es una selección cualitativa de un SIL basada solamente en la consideración de las consecuencias.

III. 5. Método basado en la consecuencia del evento

Con frecuencia es muy difícil hacer estimaciones realistas de las probabilidades de los escenarios, así que esta técnica puede ser la más apropiada. Esta es la "*técnica de consecuencia sola*", por ejemplo puede adoptarse la tabla de la Fig. 7

SIL	Consecuencias
4	Riesgo de muerte entre miembros de la comunidad (público)
3	Riesgo de numerosos muertos (sólo entre los empleados)
2	Riesgo de daños serios e incluso con algún muerto
1	Riesgos de daños menores

Figura 7

III. 5 SIL por política corporativa.

Otra técnica menos adoptada, en especial plantas de especialidades químicas que no desean un empleo extensivo de mano de obra en la selección del SIL, se refiere a '*SIL por política corporativa*". En esta técnica es la compañía la que fija el nivel (usualmente SIL 3) para todos los

niveles de seguridad. De esta forma se encausan los recursos que se emplearían en el estudio del SIL a garantizar un diseño y validación de alta calidad.

III.6 Método basado en el análisis cuantitativo

La técnica cuantitativa que es más rigurosa y en consecuencia más consumidora de tiempo. En el "*análisis cuantitativo*" el SIL se asigna mediante el modelado de las causas del incidente determinando la frecuencia a través de técnicas QRA (Quantitative Risk Analysis) tales como el análisis de árbol de fallas (TFA). El valor del SIL apropiado se selecciona dividiendo la frecuencia del riesgo considerado tolerable por la frecuencia calculada ante demanda en la función de seguridad. Esto da la probabilidad tolerable de falla ante demanda y por lo tanto el SIL. Este método es recomendable en los casos en donde es muy limitado el registro histórico tal que haga que la estimación de la probabilidad sea difícil de estimar. Aparentemente, por lo tanto, sería apropiado para los casos de sistemas de control nuevos en el área industrial. Sin embargo esta técnica requiere una comprensión completa de cómo el sistema puede fallar y las probabilidades o frecuencias para los eventos de inicio lo cual es muy difícil de estimar. El tiempo requerido por esta técnica es probablemente prohibitivo. Una variante simplificada es la utilización del análisis LOPA, como se ha visto en la sección II.

Sin embargo la técnica con más apoyo dentro de la industria es la de la "*matriz de riesgo*". Esta es una extensión de la "técnica de consecuencia sola" que permite la selección del SIL teniendo en cuenta la frecuencia del evento peligroso.

Es ya un requerimiento de OSHA que "el análisis de riesgo de un proceso sea usado para determinar las medidas de protección necesarias para proteger a los trabajadores, la comunidad y el medio ambiente". HAZOP es una técnica ampliamente empleada en la industria de procesos químicos para la identificación de peligros potenciales. Es, por lo tanto, un candidato obvio para una modificación que incorpore la selección del SIL tomando la ventaja del hecho de que la gente con el conocimiento y la experiencia apropiados están ya disponibles en el grupo. Esta es la técnica de "*HAZOP modificado*". Una vez que se ha identificado los requerimientos para el sistema instrumentado de seguridad entonces el SIL debe ser asignado en forma cualitativa basado en el conocimiento exhaustivo que tiene el equipo acerca de las operaciones del proceso, riesgos del mismo y la política de tolerancia de riesgo de la compañía. En esencia el equipo selecciona un SIL que crean apropiado de acuerdo a su estimación del riesgo. (Summers, 2003) hace una consideración importante: "puesto que la asignación es muy subjetiva, es necesario que el personal encargado de la selección del SIL sea consistente en cada uno de los proyectos." La pregunta obvia que salta a la mente es ¿cómo hacer para asegurar la consistencia a lo largo de la industria?

III.7 Integración con el análisis HAZOP. HAZOP/SIL

En este caso, para la determinación de los niveles SIL se propone un método que integra el número de capas de protección independientes con la frecuencia y severidad del evento.

Es el método básico que se adoptará en este trabajo, con matrices de riesgo discretizadas en 4 niveles en lugar de tres (ver sección I, Fig. 1).

Como se ha visto, dado que la matriz de riesgo y el número de capas de protección para cada falla o evento se realizan naturalmente durante un estudio HAZOP, surge luego la posibilidad de determinar el SIL mediante un HAZOP extendido o "HAZOP/SIL".

Una solución integrada sólo requiere de un equipo multidisciplinario liderado por un experto tanto en HAZOP como en análisis SIL. Mediante el uso de un software adecuado (en nuestro caso se propone un prototipo llamado HASIL) los detalles de ambos análisis (HAZOP/SIL) se introducen en la base de datos en una única sesión mientras que la etapa de validación SIL del proyecto se realiza mediante una herramienta complementaria a posteriori, utilizando la misma fuente de información. Para ello debe lograrse una herramienta informática robusta para almacenar los datos y realizar integralmente la tarea HAZOP/SIL metodológicamente en forma conveniente.

IV- HAZOP/SIL

En este trabajo se propone una metodología para el desarrollo de un HAZOP/SIL y un prototipo de software (HASIL) para el soporte de dicha actividad. Se basa en las propuestas publicadas previamente en la literatura abierta. Se trata de formular un método que sea práctico, seguro, y fácil de utilizar.

Como base de documentación de los resultados se propone la planilla indicada en la figura 9. Como se observa, se agregan a las columnas existentes de un HAZOP convencional (palabra guía, variables analizadas o parámetros, causas de la desviación, consecuencias de la misma, frecuencia del evento, consecuencias, valor del riesgo (calculado mediante una matriz de riesgo), salvaguardas existentes, recomendaciones); aquella del SIL y se reordena agregando información la clásica columna “protecciones existentes”. Ahora, además de la descripción de las mismas, se solicita al grupo HAZOP-SIL que determine el número de capas de protección independientes; y además, se estimen, si es posible, las probabilidades de falla de cada una de ellas (PDF).

Como se ha mencionado, dado que normalmente se utiliza, durante un HAZOP, una matriz de riesgos con 4 niveles de discretización (ver figura 1), resulta necesario adaptar el procedimiento a la determinación de los niveles SIL (0,1,2,3) -generalmente en la industria química no se estila la adopción del nivel 4, en este caso se recomienda un rediseño -.

En nuestro caso, se propone el siguiente esquema de cálculo. Dada la matriz de riesgo, la determinación del nivel SIL se realiza a través de las matrices indicadas en la figura 8. En las mismas, dados el nivel de riesgo (que tiene en cuenta frecuencia y severidad) y el número de capas de protección independientes, se determina el nivel SIL. Debe aclararse nuevamente, que las matrices indicadas para el cálculo, son solo una propuesta; los valores dependerán de la política que la empresa/usuario asigne a la determinación de los niveles SIL. Es obvio que para minimizar la subjetividad del método deben establecerse criterios para delimitar las fronteras de discretización entre los niveles de probabilidad o frecuencia de ocurrencia y en los niveles de consecuencias, abarcando el impacto a la salud, las instalaciones, al ambiente, y también a la imagen de la empresa. Queda claro también, que la asignación de los niveles SIL en las matrices de la Fig. 8, al igual que la determinación de las fronteras de discretización mencionadas, muestran el grado de sobreestimación adoptado en la medición del riesgo y determinación de los niveles SIL de la empresa que los adopte.

	NCI	4	4	4
4		0	0	1
0		0	0	1
0		0	1	1
0		0	1	1
0				
		3	3	3
		0	0	1
3		0	1	2
0		0	1	2
0		1	2	2
0				
0		2	2	2
		0	1	2
		1	1	2
2		1	2	3
0		2	3	3
0				
1		1	1	1
1		1	1	2
		1	2	3

	2	3	3
1	2	3	4
0			
1			
1	B	B	B
1	M	M	M
	A	A	A
	E	E	E

B			
M	**Prob.del evento**	**Prob.del evento**	**Prob.del evento**
A			
E			

Prob.del evento

Severidad Baja **Severidad Media** **Severidad Alta** **Severidad Extrema**

B: bajo
M: Medio
A: Alto
E: Extremo
NCI: número de capas independientes
SIL = 0 : no requerido

Figura 8 – Matrices SIL

V- HASIL. Un prototipo para la determinación de HAZOP-SIL

Mediante el uso de bases de datos relacionales es posible la incorporación progresiva de la información requerida para un análisis de riesgos. Existen numerosos paquetes comerciales basados en esta filosofía. En este trabajo se describe un prototipo que se basa en una base de datos relacional implementada en Access 2000 (al igual que el software principal SIAR). A través de formularios especialmente diseñados, se va introduciendo la información requerida, que se desarrolla durante la actividad del grupo de Análisis de Riesgo.

En una primera etapa, el HAZOP requiere la introducción de la palabra guía con sus respectivos parámetros. Una vez que el grupo HAZOP-SIL determina causas y consecuencias para cada evento o desviación (también llamado escenarios), se ingresa en los campos correspondientes la información respectiva.

Luego de introducidos los datos de frecuencia y severidad del evento, un procedimiento se encarga de evaluar el riesgo (matriz de riesgo HAZOP, según la figura 1). A partir de allí, el grupo HAZOP-SIL deberá describir todas las salvaguardas existentes. Considerando los requisitos que deben cumplir las CPI, deberá determinar el número de las mismas. Ingresado ese dato, HASIL calcula el nivel SIL automáticamente mediante las matrices indicadas en la figura 8.

La información ingresada a los respectivos campos, se presenta en el informe o planilla HAZOP-SIL según se indica en la figura 9 la cual fue generada por un informe incorporado en el mismo Access seleccionando los campos que se desean reportar.

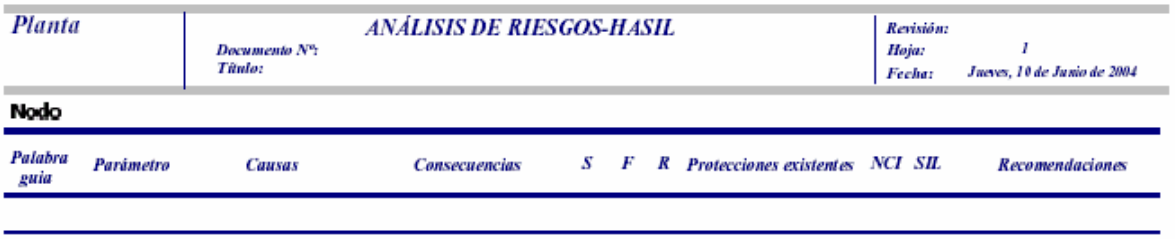

Figura 9 – Planilla HAZOP/SIL

V.1 Comparación de tiempo y costo entre la forma tradicional y la integrada.

Uno de los problemas más renombrados al realizar estudios de análisis de riesgo es el tiempo que insumen. En particular, luego del análisis HAZOP, si resulta necesario realizar una evaluación los niveles SIL, este problema se potencia.

Usando los métodos y herramienta apropiados el tiempo y el costo de desarrollar análisis de riesgos y operabilidad (HAZOP/SIL) pueden reducirse fácilmente en un 30% con un significativo mejoramiento de la integración y manejo de la información, según lo indica la experiencia propia y lo reportado por la bibliografía.

Según mencionamos, tradicionalmente los análisis HAZOP y SIL constituyen dos fases separadas las cuales producen 2 fuentes de datos diferentes. Si además consideramos la etapa de validación SIL, se produce una tercera fuente de datos. Una plataforma integrada permitiría realizar las tres tareas con una única base de datos. Esta es la ventaja de organizar en una base de datos con una organización adecuada, toda la información que se genera en el grupo HAZOP-SIL.

En una plataforma integrada sólo se requiere de una sesión de análisis HAZOP/SIL produciendo una sola base de datos la cual se empleará en la tercera etapa, la validación SIL.

Los beneficios de una solución integrada son:

- Un ahorro en tiempo y costo.
- Se hace uso de una única base de datos tanto para el análisis HAZOP como la evaluación/validación SIL.
- Se puede fácilmente realizar cambios a los fines de mantenimiento y verificación (optimización SIL) usando la misma base de datos.
-

El ahorro real comienza en el hecho de reducir el número de miembros del equipo multidisciplinario a la mitad (con respecto a ambos en forma separada).

El proceso de análisis HAZOP junto con la evaluación/validación SIL permite hasta un 30% de ahorros en los costos frente a la forma tradicional (actividades realizadas en serie).

El HAZOP consume el mismo tiempo. En el caso de la determinación de los niveles SIL, se reduce el tiempo total, y el correspondiente a cada tarea, debido al ahorro que se produce en función de la integración de las tareas.

VI- Ejemplo de Aplicación

En la figura 10 se indica el diagrama de flujo de un proceso consistente en un horno de coquización, del cual emanan gases que deben tratarse. Para bajar la temperatura se inyecta agua de un circuito específico del proceso en (A), de acuerdo al esquema adjunto. En la figura 11 se indica la planilla HAZOP del análisis del nodo correspondiente a dicho circuito de enfriamiento.

Se aprecia que el nivel del decantador D1 se controla con el controlador LIC-1. Cuando el flujo al tubo de descarga (que se controla con FIC-1) baja a un valor indeseable, entra en funcionamiento la bomba B (en paralelo) a través de un sistema de disparo automático. A más bajo flujo se dispara un circuito de enfriamiento auxiliar.

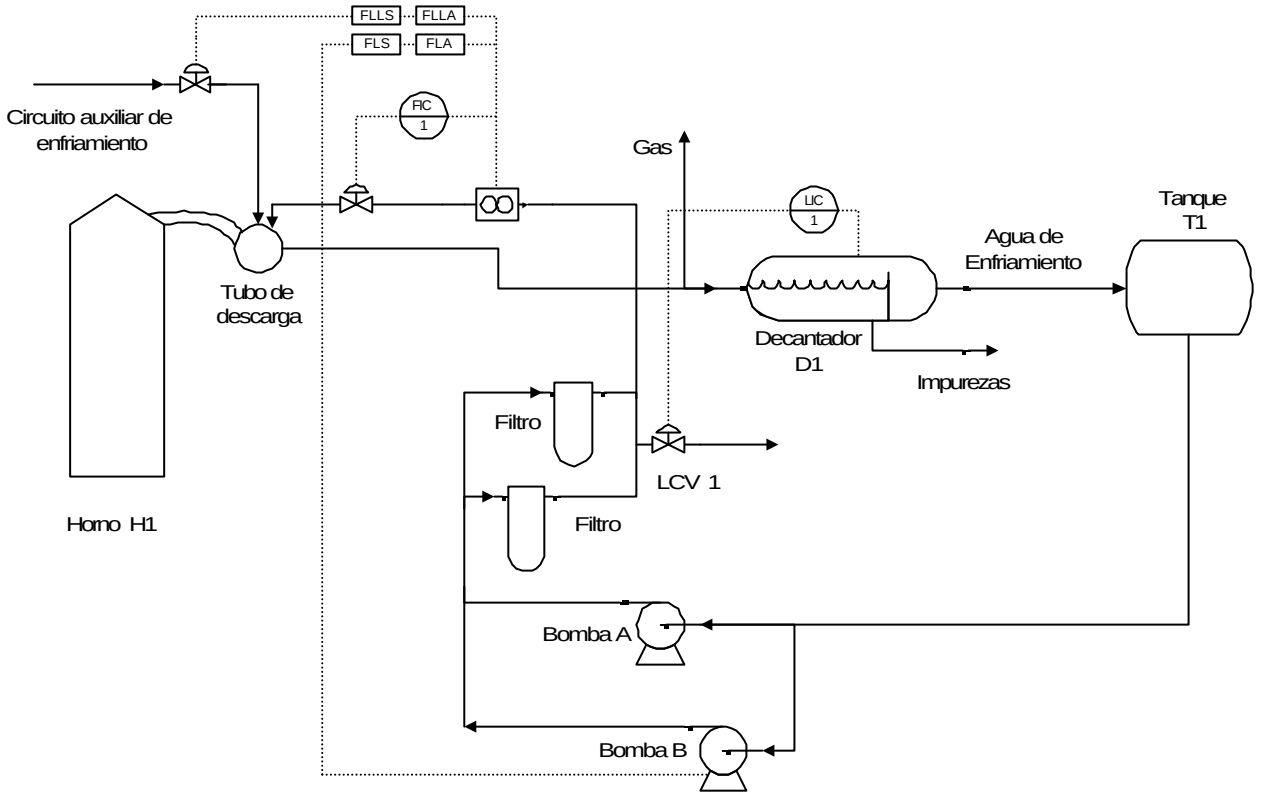

Figura 10 Esquema del Proceso

En la figura 12 se muestra la planilla HAZOP/SIL correspondiente al mismo nodo. Del diagrama de flujo y la planilla HAZOP se aprecia que sólo hay una capa de protección independiente. En efecto, en caso de fallar la señal de nivel del controlador, no actúa la bomba B ni el circuito auxiliar de enfriamiento por tener un modo de falla común.

Conclusiones

Se desarrolla un software prototipo (HASIL) para la realización de estudios de riesgo (HAZOP) y simultáneamente, la determinación de los niveles SIL las funciones instrumentadas de seguridad (FIS). La herramienta resulta ser flexible, amigable, y lo más importante, permite fácilmente determinar niveles SIL, extendiendo la tarea HAZOP en forma natural. Esto redunda en una ventaja importante, debido a la familiarización que existe en la industria química con dicha metodología.

HASIL adopta una metodología de cálculo por medio de matrices de riesgo, y la consideración de los niveles o capas de protección independientes, para la determinación del SIL, en su versión de cálculo más sencilla. No obstante, contiene funciones de verificación que utilizan diversos criterios para la determinación de niveles SIL. Dadas las frecuencias de fallas ante demanda de las distintas capas, e ingresando el nivel de riesgo aceptable por la compañía, (si se dispone como dato) el sistema calcula un nivel SIL correspondiente a dicho criterio, y reporta un mensaje de inconsistencia si el nivel SIL determinado por medio de las matrices arriba mencionadas difiere del cálculo de chequeo.

También puede, a requerimiento del usuario, utilizar criterios más simples, por ejemplo basados en la consecuencia solamente.

El programa ha sido relativamente fácil de implementar, ya que se utilizó como base la arquitectura existente y el software desarrollado (SIAR) para la realización del análisis HAZOP, WHAT IF y FMECA.

En la actualidad se está trabajando en el desarrollo de estrategias basadas en inteligencia artificial para asesorar al líder/escriba del grupo HAZOP en inconsistencias de los resultados que se generan, al cubrir las líneas/nodos del proceso bajo estudio (por ejemplo en nada de flujo, advertir al usuario si no aparecen fallas en controladores, bloqueos por error humano, etc.). Esto obligaría a que el programa codifique cada escenario registrado por tipo, y luego genere estadísticas, alertando al usuario de las situaciones potencialmente anómalas. Obviamente, dependerá del tipo de proceso que la situación bajo análisis (por ejemplo las citadas arriba) tenga relevancia o no. Se trata simplemente de un nivel de advertencia, que obligaría a chequeo de la información registrada durante el análisis HAZOP. Lo mismo podría desarrollarse para un análisis SIL. Es evidente que existen diversas metodologías de cálculo. Ante un resultado dado, y la información disponible sobre el escenario (y los objetivos de seguridad de la empresa, si se ingresan como datos), se reportan inconsistencias o discrepancias en los resultados según el método que se utilice, para alertar al líder/escriba sobre esta situación.

Por último, cabe aclarar que en la poca experiencia desarrollada hasta el presente respecto a la realización del estudio HAZOP/SIL en forma integrada, puede advertirse que se verifica claramente la ventaja de complementar ambas tareas en cuanto al tiempo consumido, ya que se aprovecha sinérgicamente , e “in situ”, el conocimiento del grupo HAZOP-SIL. Se corrige además la “subjetividad” mencionada en la sección I al realizar las recomendaciones.

Como desventaja puede comentarse que la constitución del grupo HAZOP/SIL debe ser cuidadosamente seleccionada para lograr cubrir las necesidades y/o habilidades necesarias para ambas tareas. Esto, algunas veces impone un número mayor de personas para el grupo HAZOP/SIL respecto del recomendable para la evaluación HAZOP. Una vez que un grupo multidisciplinario supera las 7 personas, comienza a incrementarse exponencialmente la tarea del líder para conducir eficientemente la reunión. Este hecho atentaría contra la ventaja ganada al integrar las tareas, pues tendería a incrementar el tiempo ocioso de trabajo, anulando la ventaja de ahorro de tiempo que se logra integrando ambas tareas.

Otra aparente desventaja (trivial en este caso) es la del incremento del tiempo respecto al HAZOP convencional, ya que ahora se agrega la evaluación SIL. Dado que el HAZOP de por sí consume tiempo, se trata de separar las tareas ya que la “segunda” (evaluación SIL) podrá realizarse más adelante, generando un “aparente” ahorro de tiempo presente, atentando contra la complementación de tareas, dada la “permanente” carencia de tiempo disponible frente a las necesidades comunes de toda empresa. Ante esta situación resultará conveniente que la evaluación SIL sólo se realice en los escenarios en los cuales el riesgo es el mayor, o en los 2 mayores niveles, para ahorrar tiempo de cálculo.

Literatura Citada

1- TECHNIQUES FOR ASSIGNIN A TARGET SAFETY INTEGRITY LEVEL, Angela E. Summers, ISA Transactions 37 (1998-2003) 95-104

Planta	ANÁLISIS DE RIESGOS-HAZOP	Revisión:
	Documento Nº Título:	Hoja: 1 Fecha: Sábado, 28 de Agosto de 2004

Nodo 2 *Circuito de enfriamiento*

Palabra guia	Parámetro	Causas	Consecuencias	S	F	R	Protecciones existentes	Recomendaciones
Flujo	Nada de	Falla en la bomba A, falla intrinseca.	No enfria los gases en tubo de descarga. -Deformación severa del tubo de descarga. -Detiene la producción. -Problemas operativos. -Apertura de antorcha. -Problemas ambientales. -Posibles daños a equipos de aguas abajo.	1	2	I	Bomba B (automática) en paralelo. -Circuito auxiliar de enfriamiento a válvulas rociadoras. -Mantenimiento predictivo-preventivo. Alarma de bajo y muy bajo caudal y presión. A bajo caudal arranca la bomba B y a muy bajo caudal emplea agua del circuito auxiliar de enfriamiento.	Analizar el nivel SIL y las CPI.

Figura 11- Planilla HAZOP convencional aplicada al ejemplo

Planta:	ANÁLISIS DE RIESGOS HAZOP/SIL	Revisión:
	Documento Nº Título:	Hoja: 1 Fecha: Sábado, 28 de Agosto de 2

Nodo 2 Circuito de enfriamiento

Palabra guia	Parámetro	Causas	Consecuencias	S	F	R	Protecciones existentes	NCI	SIL	Recomendaciones
Flujo	Nada de	Falla en la bomba A, falla intrinseca.	No enfria los gases en tubo de descarga. - Deformación severa del tubo de descarga. - Detiene la producción. - Problemas operativos. - Apertura de antorcha. - Problemas ambientales. - Posibles daños a equipos de aguas abajo.	1	2	I	Bomba B (automática) en paralelo. -Circuito auxiliar de enfriamiento a válvulas rociadoras. - Mantenimiento predictivo-preventivo. Alarma de bajo y muy bajo caudal y presión. A bajo caudal arranca la bomba B y a muy bajo caudal emplea agua del circuito auxiliar de enfriamiento.	1	3	Diseñar el SIS correspondiente.

Figura 12 – Planilla HAZOP/SIL aplicada al ejemplo