Risk Software S.A de C.V.

# Análisis de Capas de Protección (LOPA)

Preparado por: Victor Machiavelo Salinas

Numero de Reporte:29032011

# Resumen ejecutivo

## Objetivo

El objetivo del presente reporte es mostrar los diferentes métodos que existen para determinación del Nivel de Integridad de Seguridad -NIL- (Safety Integrity Level -SIL-). Esta determinación es un requerimiento establecido en el punto numero 4 en el ciclo de vida de seguridad de la norma IEC-61508 y en el punto numero 2 en en ciclo de vida de seguridad de la norma IEC-61511/ANSI-ISA-SP84-2004, el presente estudio esta basado en la Tesis doctoral desarrollada por Christopher A. Larsen en la Universidad de Ciencias y Tecnología Noruega (NTNU) presentada en Junio del 2008, y ha sido complementada con la experiencia practica de quien prepara el presente trabajo.

## Objetivo Particular

Como objetivo particular justificaremos en este reporte la necesidad de utilizar un método Cuantitativo en la determinación del SIL Objetivo. En los últimos años se ha estado utilizando métodos Cualitativos para la determinación de los niveles de integridad de seguridad en proyectos de alto riesgo y críticos para la producción de energéticos en Mexico. Si bien normas internacionales sugieren que los métodos cualitativos pueden ser utilizados para la determinación del SIL Objetivo, no se ha profundizado en las consecuencias al utilizar un método poco analítico, por esta razón el siguiente reporte tiene como objetivo demostrar la necesidad de utilizar un método Cuantitativo y la implementación de una metodología basada en el análisis del proceso, del la peligrosidad de este y del nivel de riesgo basado en el desempeño de los sistemas de seguridad.

## Metodología

El reporte estará basado en el análisis de las diferentes metodología existentes para la determinación del SIL Objetivo recomendadas en diferentes normas y al final presentaremos un caso real de la determinación del SIL Objetivo y las diferencias, pros y contras de los diferentes métodos.

### 1) Método Cuantitativo descrito en la norma IEC 61508

Este método parte del establecimiento del nivel de riesgo tolerable aceptado por la organización, el cual esta basado en las estrategias corporativas o legales de la empresa, país o estado en el cual se encuentra la empresa que determinara el nivel SIL Objetivo. Existen tres criterios para el establecimiento del nivel de riesgo tolerable, 1) Riesgo Individual, 2) Riesgo Social y 3) Riesgo Corporativo (analizaremos a detalle los conceptos de riesgo tolerable en un siguiente reporte). Básicamente el riesgo tolerable es el numero de veces que una Función Instrumentada de Seguridad (SIF) puede fallar, también podemos definirlo como de veces por año que una consecuencia no deseada ocurre en el proceso. Generalmente se obtienen estos valores de tablas o matrices que muestran la frecuencia de un evento y sus consecuencias. La matriz #1 muestra un ejemplo de esta determinación. Es común encontrar diferentes matrices dependiendo del país, compañía, tipo de industria, criterios corporativos, la determinación del nivel de riesgo tolerable requiere de un profundo conocimiento de los peligros y riesgos en la industria y contar con grupos corporativos dedicados a fijar los criterios de frecuencia y consecuencia, esto depende directamente de la localización del proceso, la interacción con la sociedad y ciudades y los materiales y productos

utilizados, desafortunadamente en Mexico no existe una legislación ni un criterio corporativo que fije los riesgos tolerables para las empresas publicas y privadas, generalmente utilizamos criterios establecidos en normas o compañías extranjeras.

| Frecuencia | Consecuencia | | | |
|---|---|---|---|---|
| | Catastrófico | Critico | Marginal | Despreciable |
| Frecuente | I | I | I | II |
| Probable | I | I | II | III |
| Ocasional | I | II | III | III |
| Remoto | II | III | III | IV |
| Improbable | III | III | IV | IV |
| Increíble | IV | IV | IV | IV |

MATRIZ #1 CLASIFICACION DEL RIESGO DE ACUERDO A IEC 61508

El siguiente paso es la determinación del riesgo del Equipo Bajo Control (EUC). El riesgo es una medida que utiliza la probabilidad y la consecuencia. El riesgo para un equipo bajo control consiste en la medida de la consecuencia no deseada y la relación de demandas del sistema sin considerar medidas de protección. La forma de calcular este valor es por medio de técnicas cuantitativas como son los Análisis de Arboles de Fallas (FTA) o los Diagramas de Bloques de Confiabilidad (RBD) (IEC 61508, 2003).

El paso final es el calculo de la Reducción de Riesgos Necesarios para cumplir con el riesgo tolerable. Este se obtiene al dividir el numero de veces por año que la Función Instrumentada de Seguridad (SIF) falla entre el numero de Demandas por Año. El resultado obtenido es el “Numero Aceptable de Veces que la SIF puede Fallar por Año” que viene siendo la Probabilidad de Falla sobre Demanda (PFD), el nivel SIL es fijado de acuerdo a la matriz #2, y bajo los criterios de un experto.

| Nivel de Integridad de Seguridad NIL (SIL) | Probabilidad de Falla Sobre Demanda Promedio (PFDave) |
|---|---|
| 4 | $<=10^{-5}$ a $<10^{-4}$ |
| 3 | $<=10^{-4}$ a $<10^{-3}$ |
| 2 | $<=10^{-2}$ a $<10^{-3}$ |
| 1 | $<=10^{-1}$ a $<10^{-2}$ |

MATRIZ #2 NIVELES DE INTEGRIDAD DE SEGURIDAD

Si bien este método utiliza cálculos cuantitativos para la determinación del riesgo del equipo bajo control, al final la selección del nivel SIL es un método de aproximación ya que se requiere de un buen juicio para seleccionar exactamente en que rango se seleccionara el SIL.

## 2) Método de Matriz de Riesgo

El método de la matriz de riesgo o matriz de peligros es uno de los mas populares ya que es muy simple de utilizar, este utiliza la frecuencia y la consecuencia para determinar cualitativamente el nivel SIL, fijando una categoría para cada relación existente en la matriz. La matriz #3 muestra esta relación.

| Frecuencia | Consecuencia (Severidad) | | |
|---|---|---|---|
| | Menor | Serio | Extenso |
| Alta | SIL2 | SIL3 | SIL3 |
| Media | SIL1 | SIL2 | SIL3 |
| Baja | NR | SIL1 | SIL3 |

MATRIZ #3 MATRIZ FRECUENCIA CONSECUENCIA

Las consecuencias pueden ser expresadas en términos de perdidas humanas, económicas, ambientales o de imagen a la empresa, y la frecuencia puede ser expresada en términos de la frecuencia en que se presenta el evento indeseable, alto, mediano o bajo. El problema con las matrices de riesgo es que la selección del SIL Objetivo esta basada en términos de una evaluación cualitativa, algunas empresas han calibrado sus matrices de acuerdo a su experiencia y tipo de aplicación y pueden proveer una guía rápida en la evaluación del nivel SIL Objetivo, sin embargo dejar a criterio de personas la selección del SIL Objetivo podría no ser una buena idea ya que pueden perderse de vista factores externos o experiencias externas en procesos similares que puedan representar un potencial problema de presentarse combinaciones de eventos no previstas por el analista, las matrices de frecuencia contra consecuencia son muy utilizadas en el análisis de peligros y operación (HAZOP) el cual es un método analítico cualitativo para la determinación de los peligros en los procesos, tal vez por esta razón se ha extendido el uso de matrices calibradas para la determinación de los niveles de SIL Objetivo.

## 3) Método de Matriz de Capas de Seguridad.

La matriz de capas de seguridad es una matriz de seguridad a la cual se le adicionan capas de protección (PL) la matriz #4 muestra un ejemplo de matriz con capas de seguridad. Una capa de seguridad (PL) de acuerdo a la IEC 61511es un grupo de equipos y/o medidas administrativas de control que operan de forma conjunta con otras capas de protección para mitigar los riesgos de proceso. Una capa de protección (PL) debe de disminuir los riesgos en un factor de al menos de 10 y deberá de cumplir con los requerimientos establecidos por la IEC 61511, 2003 que mostramos a continuación:

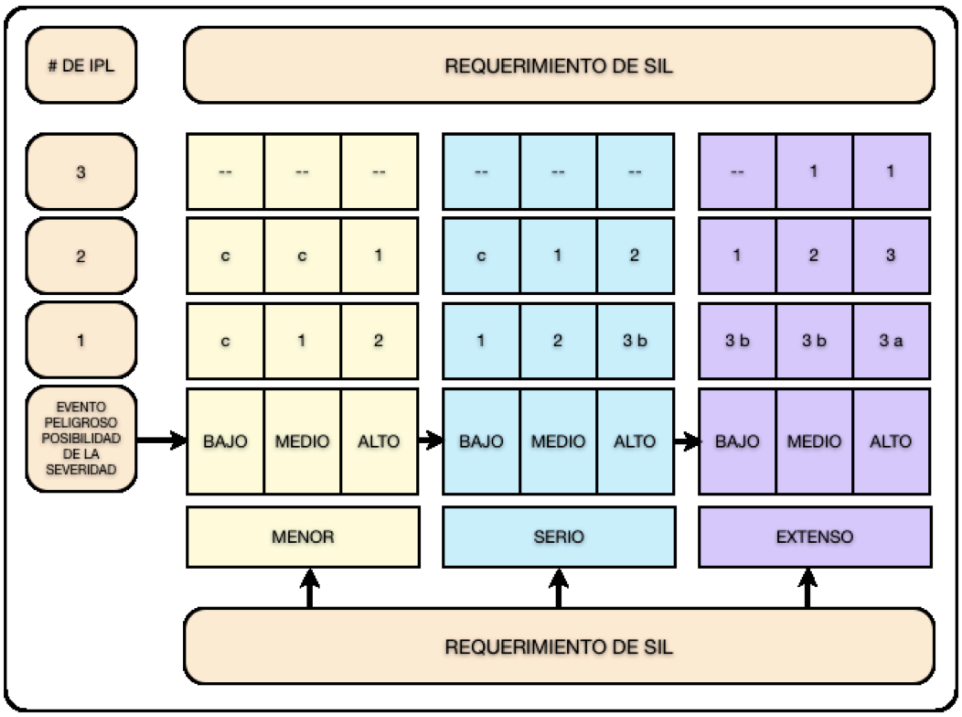
**Específicos**: Una Capa de Protección deberá estar diseñada para prevenir o mitigar las consecuencias de un evento potencialmente peligroso.

**Independiente**: Una Capa de Protección deberá ser independiente de otras capas y no deberá de tener una falla de causa común (CCF).

**Confiable**: Una Capa de Protección deberá actuar de acuerdo a la intención de su diseño.

**Auditable**: Una Capa de Protección deber estar diseñada para que pueda ser validada.

Un Sistema Instrumentado de Seguridad (SIS) es considerado como una capa de protección (IEC 61511. 2003).




a) Un solo SIL3 no provee del nivel de reducción de riesgo requiere modificaciones
b) Un solo SIL3 podría no proporcionar el nivel de reducción de riesgo requiere revisión
c) Probablemente no se requiere de un SIS

MATRIZ #4 MATRIZ CON CAPAS DE SEGURIDAD

La clasificación de la frecuencia de los eventos peligrosos adaptada de la IEC 61511 se muestra en la tabla #1

| Tipo de Evento | Posibilidad/ Rango Cualitativo |
|---|---|
| Eventos como múltiples fallas en diversos instrumentos, válvulas, múltiples errores humanos en un ambiente libre de tensiones o fallas en equipos de proceso. | Bajo |
| Eventos como fallas en instrumentos y válvulas en redundancia, o liberación de productos en áreas de carga y descarga de productos | Medio |
| Eventos como fugas en proceso, fallas de instrumentos y válvulas simples o errores humanos que generan una pequeña liberación de productos. | Bajo |
| Los sistemas deberán de estar de acuerdo a normas que indican que una función de control debe de fallar con una frecuencia menor de 10 E-1 por año | |

TABLA #1 FRECUENCIA DE UN EVENTO PELIGROSO DE ACUERDO A IEC 61511

## 4) Método de Gráficos de Riesgo

El método de gráficos de riesgo fue desarrollado con la publicación de la norma Alemana DIN 19250 publicada en 1994, y es un método muy popular en la determinación del nivel de SIL Objetivo. Este método cualitativo basado en categorías.

Las categorías utilizadas son las consecuencias y frecuencias de un evento peligroso, pero también la probabilidad de que una persona se encuentre en el área afectada y la posibilidad de que esta pueda evadir el peligro. Mostramos en la figura #1 la representación de un gráfico de riesgos, los parámetros de riesgo pueden ser tomados de la norma IEC 61511.

El parámetro de Consecuencias (C) describe el resultado probable del evento peligroso, y esta compuesto por cuatro categorías, Ca es el valor menos severo y el rango de afectación esta dado por la lesión de una persona, Cb representa lesiones serias para una o varias lesiones, Cc representa muerte de varias personas y Cd fatalidad de múltiples personas.
El parámetro de tiempo de exposición (F) nos indica la fracción de tiempo que la persona expuesta al peligro se encuentra en el área del evento, Fb indica un riesgo mayor que Fa, y generalmente se selecciona Fa cuando el tiempo de ocupación es aproximadamente de 10% o menor.

La posibilidad de que el personal evite el peligro es incorporado en el parámetro (P). Este refleja los métodos y logística implementados para que el personal pueda escapar del área peligrosa, Pb representa un riesgo mayor que Pa, la norma IEC 61511 proporciona una lista de cumplimientos para que la posibilidad pueda ser tomada como Pa.

El parámetro final es la relación de demandas (W), la cual es la frecuencia por año en que se presenta la consecuencia no deseada sin la función instrumentada de seguridad (SIF). W1 indica una relación de demandas es de 0.03 por año. W2 indica entre 0.03-0.3 y W3 mas de 3 relaciones de demanda por año.

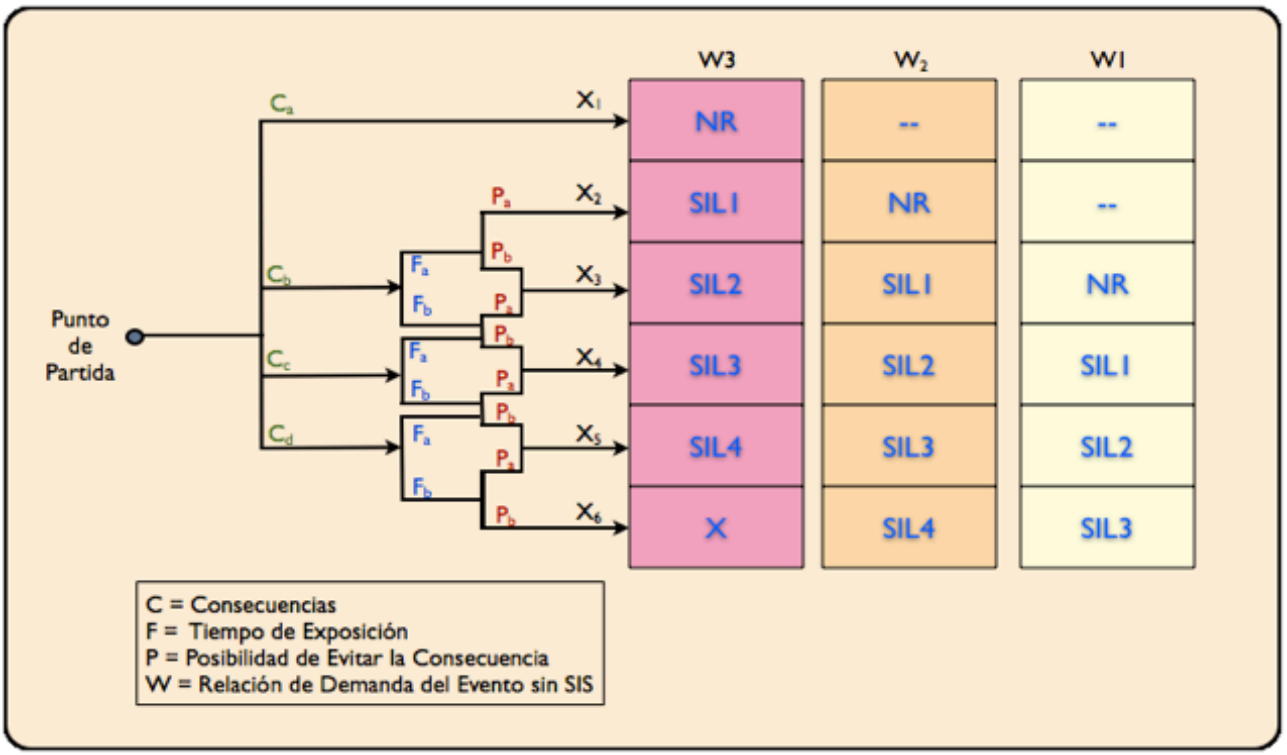



Figura #1 GRAFICO DE RIESGO

En la figura #1 observamos el flujo de decisión que va de izquierda a derecha, los valores de SIL son sugeridos en esta figura, cada empresa y cada aplicación deberá de revisar y ajustar el gráfico de riesgo de acuerdo a sus propios criterios, esto resulta particularmente difícil dado que es un método cualitativo y no seria extraño encontrar que las empresas tiendan a relajar el nivel de integridad de seguridad SIL, es por esto que se recomienda que si se ha tomado la decisión de utilizar gráficos de riesgos estos sean calibrados.

## 5) Gráficos de Riesgo Calibrados

El método de Gráfico de Riesgo Calibrado es un método Semi-Cuantitativo, y utiliza los mismos parámetros utilizados en el gráfico de riesgos.

Calibración significa asignar valores numéricos a los parámetros. Esto permite una determinación mas precisa del SIL Objetivo y una toma de decisión mas objetiva. La calibración depende de los valores que se tomen para el riesgo individual y social, así como los criterios corporativos de las empresas y regulaciones estatales y de cada país.

Los valores de consecuencias pueden ser cualificados como el numero de fatalidades, pero en muchas instancias una falla no causa una fatalidad inmediata, lo cual nos hace introducir el concepto de “Vulnerabilidad” (V) que es una función de la concentración de peligro y la duración a la exposición. Multiplicando la vulnerabilidad por el numero de personas presentes en el área expuesta, la tabla #2 muestra los valores para un gráfico de riesgo calibrados donde se muestran los valores de vulnerabilidad.

| Parámetro de Riesgo | | Clasificación |
|---|---|---|
| **Consecuencias (C)**<br>Numero de Fatalidades<br>Puede ser calculado como: Numero de personas presentes cuando el área expuesta a un peligro es ocupada. y la Vulnerabilidad dado el peligro identificado:<br>V= 0.01 (Liberación pequeña cantidad de material tóxico o explosivo)<br>V= 0.1 (Liberación grande cantidad de material tóxico o explosivo)<br>V= 0.5 (Idem al anterior pero con alta probabilidad de ignición o afectación tóxica)<br>V= 1 (Ruptura o explosión) | Ca | Daño Menor |
| | Cb | 0.01< No de Fatalidades < 0.1 |
| | Cc | 0.1 < No de Fatalidades <1.0 |
| | Cd | No de Fatalidades >1.0 |
| **Ocupación (F)**<br>Porcentaje del tiempo que el área expuesta es ocupada durante un periodo de tiempo normal de trabajo | Fa | Ocupación < 0.1 |
| | Fb | |
| **Posibilidad de Evitar el Peligro (P)** | Pa | El peligro puede ser prevenido por acciones que el operador realiza, después de que el SIS ha fallado |
| | Pb | Si no hay acciones posibles. |
| **Relación de Demandas (W)** | W1 | Relación Demandas < 0.1 por año |
| | W2 | 0.1D <Relación Demandas <10D por año |
| | W3 | Para Relación de Demandas >10D |

TABLA #2 EJEMPLO TOMADO DE IEC 61511 PARA LA CREACION DE GRAFICOS DE RIESGO CALIBRADOS.

Debemos tener en cuanta que la vulnerabilidad (V) y la posibilidad de evitar el peligro (P) son dos diferentes parámetros, V tiene que ver con la escalación y P tiene que ver con la prevención del peligro por parte del operador (IEC 61511,2003).

De acuerdo a Marszal y Scharpf (2002) los Rangos Potenciales de Perdidas de Vida (PLL) también pueden ser utilizados como una medida de las consecuencias. El valor de PLL es el numero esperado de fatalidades en una población durante un periodo de tiempo especifico (NORSOK Z-013, 2003). Hacemos notar que que hay que tener cuidado cuando se toman los valores de PLL como medida de consecuencia, por que este valor incorpora tanto la probabilidad como la consecuencia.

El parámetro F es generalmente una medición de porcentaje del tiempo que el personal puede estar expuesto en el área peligrosa y Fa deberá ser utilizada para valores menores de 0.1 (IEC 61511, 2003, Marszal y Scharpf, 2002).

Consideráremos a Pa cuando todas las condiciones requeridas por la IEC 61511-3 se cumplan y Pb si no se cumplen.

El factor de demanda W es el numero de veces por año que ocurre el evento peligroso en ausencia de las funciones instrumentadas de seguridad SIF. “D” es un factor de calibración que debe hacer que el resultado en el gráfico de riesgo se mantenga en niveles de riesgo tolerable.

## 6) Comentarios a los Métodos

Los cuarto métodos discutidos con anterioridad son utilizados en la industria de forma frecuente, su selección y utilización depende de varios factores y políticas de cada campaña, algunos puntos a considerar al seleccionar alguno de estos métodos son:

1. Se cuenta con políticas claras en la definición del riesgo y peligro en los procesos.
2. Se cuenta con personal calificado para la determinación de un evento utilizando herramientas com arboles de falla y diagramas de confiabilidad.
3. Se tiene identificado los riesgos tolerables para cada aplicación e industria.
4. Las gráficas de riesgo han sido desarrolladas para cada aplicación y consideran las diferencias en los procesos, y sus consecuencias.
5. Las matrices y los gráficos de riesgo se han verificado con los datos reales de proceso.
6. Se desarrollo una metodología clara y documentada para calibrar las matrices y gráficos de riesgo.
7. Se cuenta con personal calificado (Certificado) para evaluar las matrices y gráficos de riesgo, el personal tiene la experiencia para utilizar métodos que requieren el establecimiento de criterios en los procesos.
8. Se han desarrollado análisis y/o simulaciones para identificar la frecuencia de los eventos o se utilizan valores publicados en literatura.
9. Se han desarrollado análisis y/o simulaciones para determinar las consecuencia o se utilizan valores publicados en la literatura.
10. Se tiene una política clara y documentada respecto a que metodología utilizar, que considere la aplicación, el proceso y la ubicación de las instalaciones.

De no cumplirse con estos puntos se deberá de optar por otras formas de obtener el SIL Objetivo de preferencia utilizando métodos cuantitativos/semi-cuantitativos que permitan obtener resultados confiables minimizando juicios basados en criterios personales. La tabla #3 muestra la información mínima requerida por cada uno de los cuatro métodos de determinación de SIL Objetivo analizados.

| Características | Cuantitativo IEC 61608 | Matriz de Riesgo | Gráfica de Riesgo | Gráfica de Riesgo Calibrada | LOPA | GRAFICA DE RIESGO CON CAPAS DE PROTECCION |
|---|---|---|---|---|---|---|
| Cuantitativo | X | -- | -- | -- | X | X |
| Cualitativo | -- | X | X | -- | X | |
| Semi Cuantitativo | -- | -- | -- | X | X | |
| Riesgo Tolerable | X | -- | -- | -- | X | |
| Frecuencia del Evento | X | X | X | X | X | X |

| Características | Cuantitativo IEC 61608 | Matriz de Riesgo | Gráfica de Riesgo | Gráfica de Riesgo Calibrada | LOPA | GRAFICA DE RIESGO CON CAPAS DE PROTECCION |
|---|---|---|---|---|---|---|
| Consecuencia del Evento | X | X | X | X | X | X |
| Riesgo del Equipo Bajo Control | X | -- | -- | -- | X | |
| Reducción del Riesgo Residual | X | -- | -- | -- | X | |
| Tiempo de Exposición al Peligro | -- | -- | X | X | -- | X |
| Posibilidad de Evitar el peligro | -- | -- | X | X | -- | X |
| Relación de Demandas | -- | -- | X | X | X | X |
| Vulnerabilidad | -- | -- | -- | X | -- | -- |
| Requiere método analítico FTA/ RBD | X | -- | -- | -- | X | -- |
| % Basado en Cálculos vs Criterios | 50/50 | 0/100 | 0/100 | 20/80 | 80/20 | 60/40 |

TABLA #3 REQUERIMIENTOS DE INFORMACION PARA CADA METODO

Como podemos observar en la tabla #3 solo el método cuantitativo de la IEC 61508 toma en cuanta el riesgo tolerable, el riesgo al cual esta sometido el equipo bajo control y la reducción del riesgo. Los métodos basados en matriz y gráfico de riesgo parten de criterios establecidos por parámetros preestablecidos y no se enfocan en el calculo y determinación de frecuencias y consecuencias y condiciones dadas por el proceso, es por esta razón que de forma estricta no representan una real practica de ingeniería en la determinación del SIL Objetivo.

El uso de valores preestablecidos basados en criterios dados por las empresas o por los expertos siempre estarán sujetos a la interpretación, adicionalmente debemos también considerar las características de los procesos y la forma en que los peligros y los riesgos se presentan en cada equipo, proceso e instalación nunca son los mismos, tampoco deberían ser las

mismas las bases y criterios de la determinación de las frecuencias y consecuencias de los eventos peligrosos. Resulta también difícil de entender que se utilicen los mismos criterios para instalaciones localizadas en diferentes ubicaciones geográficas, y que ademas no se considere importante la determinación del riesgo individual/social/corporativo.

La figura #2 nos presenta un modelo de decisión para la selección del SIL Objetivo,aquí se considera que los métodos de matriz de riesgos y gráficos de riesgos son mas adecuados cuando se desea realizar una validación o verificación rápida de las funciones instrumentadas de seguridad existentes o bien se encuentra en una fase de desarrollo de ingeniería básica y no se cuenta con toda la información para utilizar un método cuantitativo mas detallado.

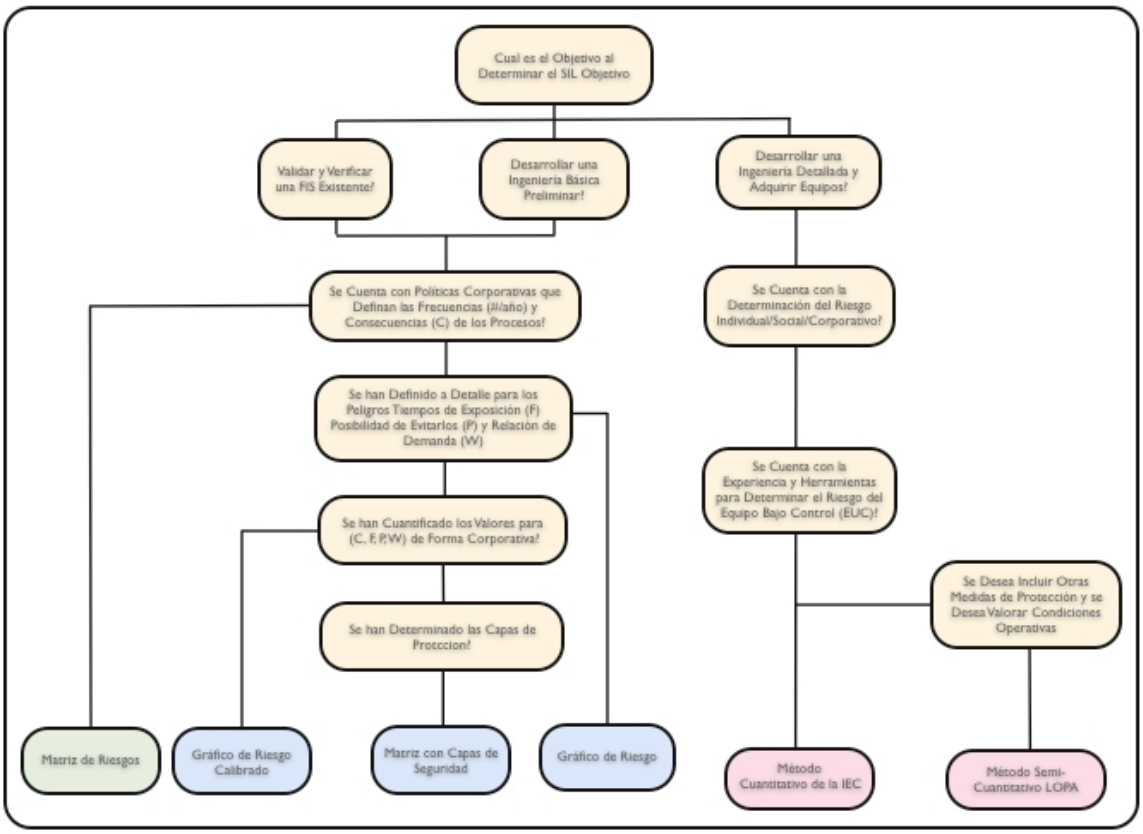



FIGURA #2 FLUJO PARA LA DETERMINACION DEL METODO SIL

Consideramos que la seguridad en los procesos industriales no debe estar basada en criterios sino en cálculos detallados y en la confirmación de forma numérica que se esta cumpliendo con los requerimientos de seguridad deseados, es muy importante aclarar que si la determinación del SIL Objetivo es clara y sustentada, no solo nos ayudara a la determinación del SIL Proporcionado por el Sistema Instrumentado de Seguridad (SIS) también nos ayudara a determinar las áreas peligrosas del proceso y los elementos que pueden generar condiciones riesgosas, la figura #2 introduce una nueva metodología llamada LOPA (Layer Of Protections Analysis) Análisis de Capas de Protección el cual es el método cuando se desea calcular el SIL Objetivo y compararlo con el SIL Proporcionado por el SIS y la ponderación que otras funciones de seguridad tienen en la reducción del riesgo así como consideraciones operativas del proceso.

## 7) LOPA Análisis de Capas de Protección.

La metodología de LOPA fue introducida a principios de los años 90´s, y ha ganado popularidad en los últimos años como técnica para la determinación del SIL. En la literatura encontramos que LOPA es referida como una técnica de valoración del riesgo y como una herramienta de análisis de riesgos. Otras aplicaciones que se han desarrollado entorno a LOPA son como herramienta de planeación de inversión, investigación de accidentes y manejo de cambios.

De acuerdo a Marszal y Scharpf (2002) LOPA puede ser visto como un tipo especial de análisis de arboles de eventos (ETA) el cual tiene el propósito de determinar la frecuencia de una consecuencia indeseada, esto puede ser evitado por medio de un juego de capas de protección. La aproximación evalúa el peor escenario/caso, donde todas las capas de protección deben de fallar para que se presente la consecuencia. La frecuencia de la consecuencia indeseada es calculada al multiplicar la Probabilidad de Falla Sobre Demanda (PFD) de las diferentes capas de protección por la demanda del sistema de protección (representada por la frecuencia). Comparando el resultado de la frecuencia de la consecuencia indeseada con la frecuencia de riesgo tolerable se identifica la reducción de riesgo necesaria y el nivel de SIL apropiado puede ser seleccionado (Marszal y Scharpf ,2002, CCPS, 2004).

LOPA es un método semi-cuantitativo que utiliza categorías numéricas para estimar los parámetros requeridos para calcular la reducción del riesgo necesario con ciertos criterios de aceptación (CCPS, 2001). En una Valoración Cuantitativa de Riesgos (QRA) los modelos matemáticos y la simulación son frecuentemente utilizados para para estimar los daños o la escalacion de estos, como son los análisis de dispersión, modelos de sobre-presión en explosiones o fuegos. En adición los Arboles de Falla (FTA) y otros métodos son utilizados para calcular la frecuencia del evento. En LOPA juicios simplificados, tablas y referencias bibliográficas son utilizadas para obtener los números deseados, pero también es posible partir de los valores simulados y calculados como en las valoraciones cuantitativas de riesgo, dando una mayor certeza a LOPA.

LOPA obtiene la información del análisis de peligros y operación (HAZOP) o de los estudios de identificación de peligros (HAZID) y puede ofrecer información para la creación de estudios mas sofisticados como QRA. La figura #2 muestra los estudios típicos de análisis de riesgos dependiendo de la fase en la que se encuentra la evaluación y muestra el evento/ accidente y la vinculación que tiene con las causas y consecuencias. La utilización de los Arboles de Eventos como herramienta en LOPA se encuentra mas enfocada en la determinación y valoración de las consecuencias y no tanto en las causas pero también por su interacción con el Hazop es normal situar la aplicación de LOPA entre los análisis del evento y sus consecuencias.

LOPA utiliza el concepto de capas de protección como es mostrado en la Figura #4, donde se muestran las diferentes capas de protección existentes y posibles en una instalación industrial, debemos entender que para definir que puede ser definido como capa de protección, su definición, aplicación y separación con otras capas de protección debe quedar claramente establecida, decimos que una salvaguarda pueda ser considerada como capa de protección cuando se cumplen las cuatro primicias (Especifico, Independiente, Confiable, Auditable)

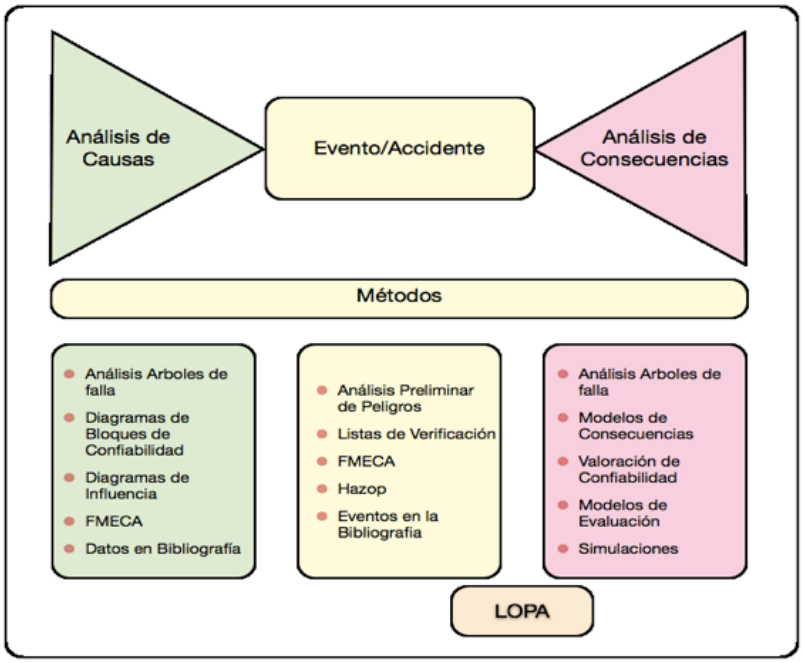



FIGURA #3 RELACION DE METODOS DE ANALISIS

LOPA utiliza el modelo de capas de protección y la efectividad de estas para la determinación del SIL.

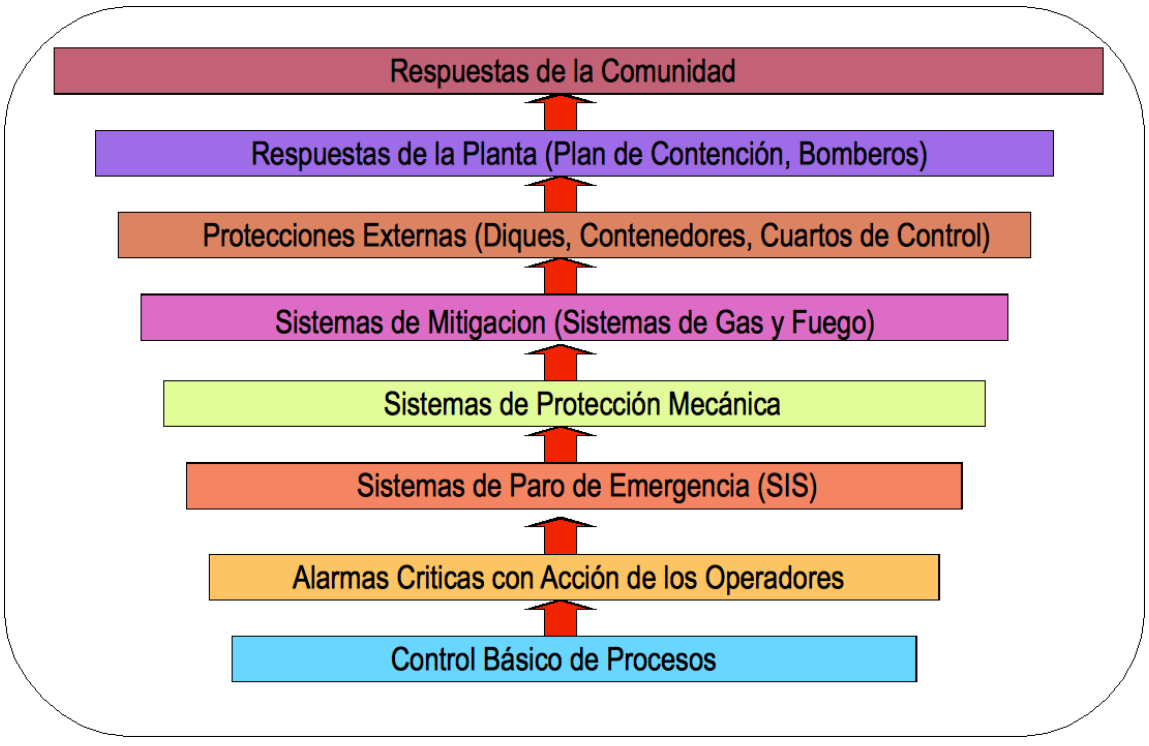



FIGURA #4 CAPAS DE PROTECCION

La metodología de LOPA ha sido interpretada y desarrollada por varios autores y compañías de forma diferente, esto ha conducido a diferencias en las definiciones y términos utilizados, a continuación explicaremos a detalle cada uno de los términos utilizados en LOPA así como la metodología de esta, también es importante aclarar que se debe revisar a detalle las definiciones y requerimientos para definir y aceptar cada una de las capas de protección mostradas en la Fig #4, situación que no abarcaremos en este trabajo y recomendamos revisar en el libro "Layer of Protection Analysis" publicado en el 2001 por "Center for Chemical Process Safety" de AIChE, uno de los objetivos en esta sección será aclarar el funcionamiento y aplicación de LOPA, partiremos de las definiciones que se generan a partir de la Fig #5.

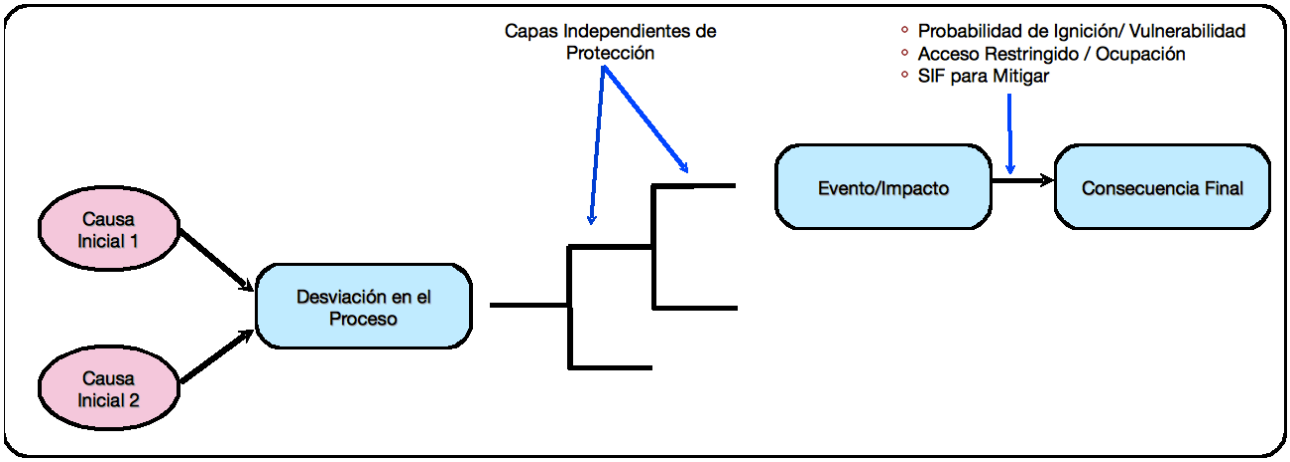



FIGURA #5 RELACION ENTRE LAS CAUSAS INICIALES, EVENTOS, DESVIACION DEL PROCESOS Y CAPAS INDEPENDIENTES DE PROTECCION

## Causa Inicial / Evento Inicial.

Las causas iniciales o eventos iniciales son las que generan una desviación en el proceso, no nos referimos a las causas raíz básicas. Las causas iniciales son resultado de las causas raíz. El CCPS nos indica que hay tres clases de causas iniciales: 1) Eventos Externos, 2) Fallas en los Equipos y 3) Fallas Humanas. Los eventos externos son huracanes, terremotos, y en general factores externos fuera de control. Las fallas en los equipos están dadas por fallas en los sistemas de control y protección así como en las fallas mecánicas de los equipos en los procesos como compresores, bombas, válvulas, etc. Las fallas humanas pueden ser por errores en el desarrollo de la ingeniería y especificación de los equipos, fallas por omisiones, fallas en las pruebas de los sistemas, fallas en operación y procedimientos de emergencia.

## Desviaciones en el proceso.

De acuerdo a la norma NORSOK Z-013 (2001) un evento accidental es definido como "Evento o cadena de eventos que puede causar la perdida de la vida, daños a la salud o daño al medio ambiente". Otra definición es " La primera desviación significante de una situación normal que puede causar consecuencias indeseadas" (Rausand y Hoyland,2004). En la norma IEC 60300-3-9 (1995) se utiliza el termino evento peligroso en lugar de evento accidental. En los estudios de Hazop el evento accidental es referido como desviación del proceso.

## Evento/Impacto.

La CCPS (2001) define como impacto: “El resultado ultimo potencial resultado de un evento peligroso”. El termino Impacto puede ser expresado como el numero de heridas o fatalidades, daño a la comunidad, instalación o negocio”. De acuerdo a la IEC 61511 un Evento/Impacto es equivalente al termino Consecuencia utilizado en los estudios de Hazop. Esto implica que el evento/impacto es una consecuencia indeseada de un evento peligroso o evento accidente referido como una desviación del proceso. Evento/Impacto es relacionado de forma cercana a una consecuencia indeseada, y la pregunta que permanece es cual es el nivel que la consecuencia y el evento/impacto representan, ya que por ejemplo podemos tener eventos/impactos intermedios y eventos/impactos finales. Por esto escojamos definir el termino evento/impacto como “El primer signo de daño en personas, ambiente e instalaciones”.

## Escenario.

De acuerdo a CCPS (2001) un escenario es descrito como un par único causa-consecuencia dado por el Hazop. En la terminología de LOPA puede ser definido como un único par causa-evento/impacto. Esto implica que el escenario consiste en una relación mayor que únicamente el evento/impacto y también es mucho mas que solo un resultado de una consecuencia, en términos concretos podemos definir al escenario como “ El desarrollo que tiene un evento desde la desviación en el procesos hasta el evento/impacto incluyendo las causas que generaron la desviación del proceso.

## Capas de Protección vs Capas Independientes de Protección.

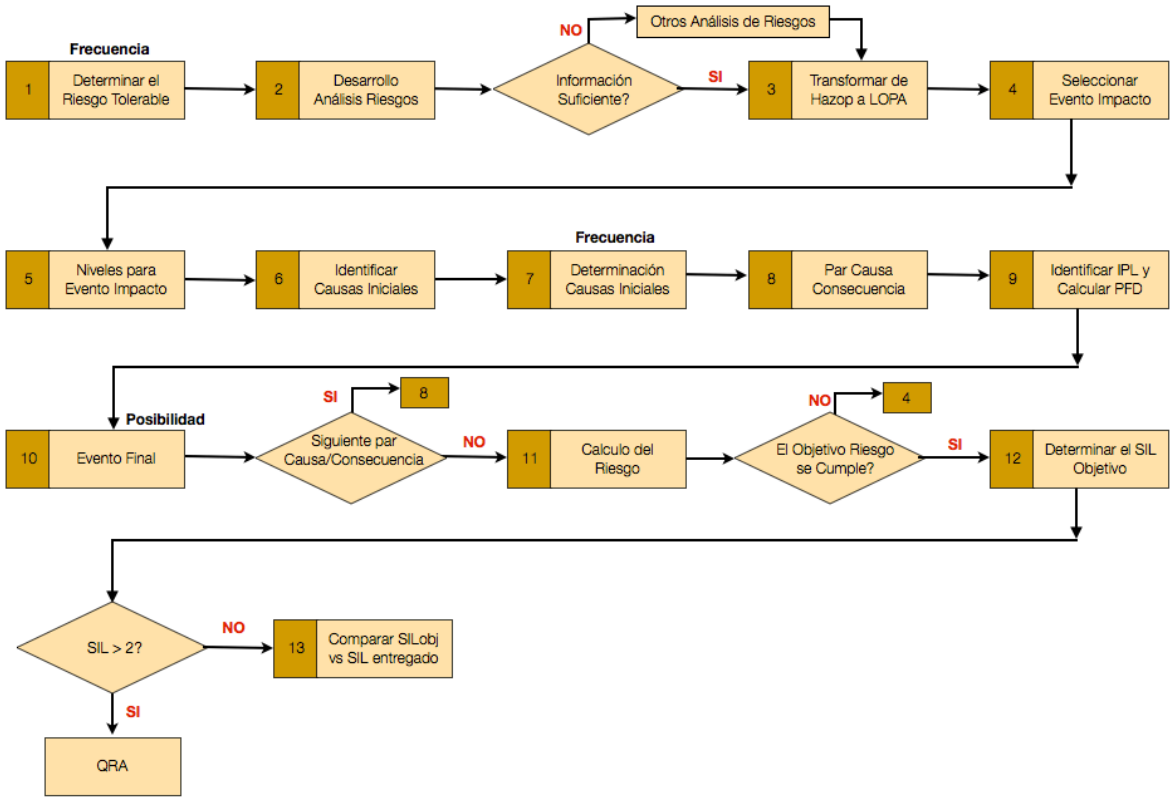
El termino “Capa de Protección” fue definido en la IEC 61511 y como hemos mencionado debe de cumplir con las cuatro características (Especifico, Independiente, Confiable, Auditable). Entonces encontramos que hay una diferencia entre la definición de que es una Capa de Protección (PL) y una Capa Independiente de Protección (IPL). De acuerdo a la IEC 61511 una IPL tiene las mismas características que una PL pero adicionalmente debe de proporcionar una reducción en el riesgo en un factor de 100 (Una PL proporciona 10) y también debe de proporcionar una disponibilidad de al menos 0.9. Esta definición puede parecer un poco confusa por lo que una definición mas exacta puede ser nombrar a las PL como IPL y a las IPL como IPL de Alta Integridad. La definición que establece la CCPS (2001) para PL es: “Dispositivo, Sistema o Acción que es capas de prevenir una desviación del proceso que pueda llevarlo a una consecuencia final”. Subsecuentemente una IPL puede ser definida como: “ Una Capa de Protección PL, capas de prevenir una desviación del proceso que pueda llevar a una consecuencia final independientemente de la acción de otra PL asociada al mismo evento/impacto y del par causa consecuencia del evento inicial”.

LOPA es un método de determinación del SIL que requiere de una metodología para su implementación, hay diferentes variaciones a esta metodología que se han desarrollado por compañías u organizaciones, pero en términos generalas LOPA es un método que parte del par Causa-Consecuencia y evalúa las Capas Independientes de Protección necesarias para reducir el riesgo inicial dado por la definición de Riesgo Individual/Social/Corporativo a un riesgo aceptable.

La figura #6 nos muestra un diagrama de flujo detallado de los pasos requeridos por LOPA, como podemos observar LOPA requiere de un esfuerzo mayor que otras técnicas pero también nos proporciona mucha mas información del procesos y sus riesgos y principalmente evita o disminuye radicalmente la utilización de criterios en la selección y determinación del Nivel de Integridad de Seguridad SIL Objetivo y del SIL que deberá ser proporcionado por el SIS.

## Metodología de LOPA.

El proceso para la determinación del SIL objetivo utilizando la tecnica de LOPA, requiere varias fases que han sido definidas a detalle y se muestras en la siguiente figura:




**1) Determinación del Riesgo Tolerable:**

La determinación del nivel de riesgo tolerable generalmente esta definida por la empresa o por leyes locales, en términos generales hay tres formas de determinar el Riesgo y son: Riesgo Individual, Riesgo Social y Riesgo Corporativo.

La determinación del Riesgo Tolerable es el primer paso en la metodología LOPA este valor nos indica a donde debemos llegar.
En muchos países este valor es establecido por leyes.
Tres criterios son establecidos:

- Riesgo Individual
- Riesgo Social
- Riesgo Corporativo

Se expresa en unidades de Frecuencia/#Año:

- Numero de fatalidades
- Numero de incidentes
- Numero de perdidas económicas
- Numero de días de producción perdidos

Si bien el valor de FRT es fijada de forma corporativa basandose en cualquiera de los criterios de riesgo (individual, social,corporativo) es obvio con no todas las áreas de un proceso sea este una refinería, petroquímica, farmacéutica, etc, tienen el mismo nivel de riesgo. Es por esto que se debe ajustar el valor de FRT para cada una de las áreas de proceso, a este ajuste se le puede llamar Frecuencia de Riesgo Tolerable Final (FRTF) y debe ser considerado para cada área del proceso analizado.

$$FRTF = \frac{FRT}{PVH}$$

El valor de PVH puede ser expresado como:

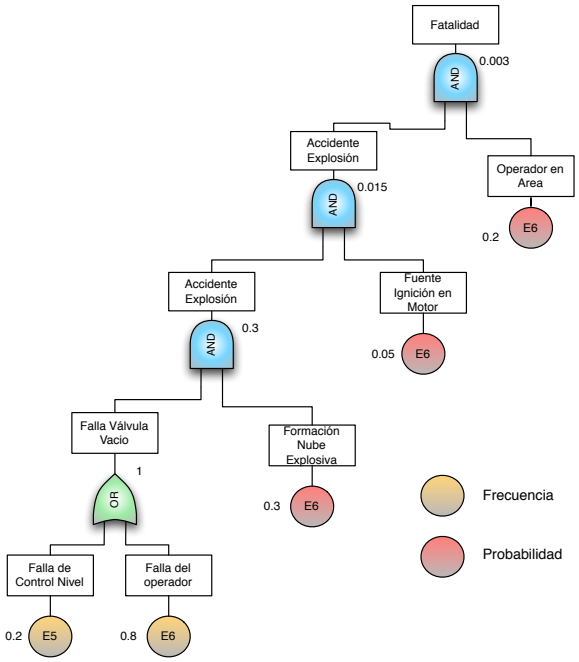
- # de perdidas de vidas humanas
- Probabilidad de perdida de vidas humanas

**2) Determinación de la Frecuencia del Evento Inicial:**

Existen varios métodos para determinar la frecuencia de las causas iniciales que detonan un evento, tres son los métodos mas utilizados en la industria:

- Tablas de frecuencias de eventos iniciales basadas en bases de datos.
- Modelacion por medio de Análisis de Arboles de Falla.
- Juicio de Expertos.

Una practica común en el desarrollo de nuestros proyectos es la de modelar la frecuencia de los eventos utilizando Análisis de Arboles de Falla (FTA) y comparar los valores con datos establecidos en bases de datos como OREDA, el utilizar FTA nos proporciona no solo un valor de frecuencia del evento inicial, también nos ayuda a determinar los puntos mas débiles en los sistemas y como estos fallan.




**3) Análisis de Riesgos.**

Hay varias técnicas identificadas y disponibles para la realización de Un Análisis de Riesgos que puedan ayudar a la Identificación de Peligros, las técnicas mas utilizadas para el análisis de riesgos y peligros de procesos son:

- Que Pasa Si? (What-If)
- Listas de Revisión. (Checklist)
- Que Pasa Si?/ Listas de Revisión. (What-If/Checklist)
- Estudios de Peligro y Operación Hazard and (Operability Study HAZOP)
- Análisis de Modos y Efectos de Fallas (Failure Mode and Effects Analysis FMEA)
- Arboles de Falla. (Fault Tree Analysis)
- Metodología Propias

Una vez identificados los eventos que son incluidos en el análisis de riesgos, es necesario estimar la frecuencia con que estos eventos pueden ocurrir, generalmente hay tres acercamientos para realizar esto: 1) Utilizar valores históricos que nos indican que tan frecuente este tipo de eventos han ocurrido en el pasado. 2) Utilizar técnicas analíticas o simulaciones (como árboles de falla) para predecir que tan frecuente puede ser. 3) Utilizar el juicio de los expertos. El método mas sencillo es el de utilizar valores históricos, estos pueden ser utilizados de dos maneras: a) Determinando la frecuencia del incidente (por ejemplo la frecuencia de un incendio en un tanque, o las fallas presentadas en una torre de destilación) b) Determinando la frecuencia del equipo (fallas en un tipo de válvula, bomba, compresor)

En el contexto de análisis de riesgos, el análisis de las consecuencias involucra la determinación de los efectos de cada evento, en el interés de conocer las consecuencias físicas generadas y la severidad. La determinación de los efectos físicos

generalmente involucra el calculo de la distancia máxima desde la fuente hasta las personas que son afectadas. La severidad de un evento es expresado en el nivel de daño de las personas afectadas

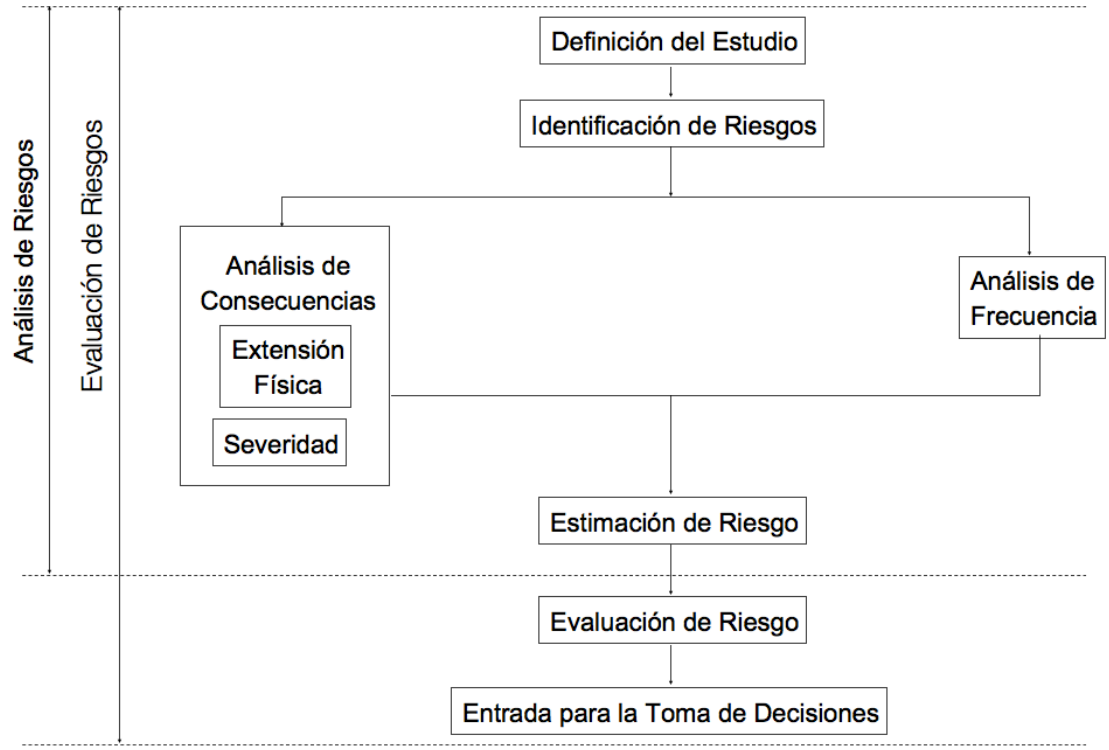
El análisis de las consecuencias de un evento considera varios factores como son 1) Impacto en Humanos, 2) Impacto Ambiental, 3) Impacto Económico, y 4) Las afectaciones a la reputación de las empresas. Aun cuando ya es común encontrar que al realizar un análisis de peligros las empresas o los analistas en riesgo consideran los cuatro factores, es un echo que el impacto sobre los seres humanos es el valor mas importante a considerar, también tiende a ser el valor mas conservador, es decir realizar un análisis donde la consecuencia sea expresada como impacto a los humanos, conllevara a que el estudio sea mas confiable y seguro.

El acercamiento que tendremos para el estudio de los análisis de consecuencia considera varias etapas; 1) Modelaje en términos de la fuente ( caracterización de evento en términos de la relación de eventos que genera una liberación de producto ó cambios en la temperatura, presión, velocidad, densidad, flujo, composición) 2) Modelos de Dispersión (para calcular el movimientos de las sustancias tóxicas o explosivas). 3) Modelaje de Fuego y Explosión (para conocer la forma en que actúan) 4) Modelaje de los efectos (para determinar el efecto que una liberación de producto o energía tiene sobre las personas, equipos y comunidad)

Cada una de las etapas requiere cálculos detallados de desempeño. En la mayoría de los casos se requiere de computadoras con software dedicado, algunas compañías han desarrollado sus propios software para estos cálculos. Para utilizar estas herramientas se requiere de información para realizar los cálculos como es: a) Datos toxicológicos de las sustancias, b) Propiedades químicas de las sustancias, c) Efectos del calor debido al fuego, d) Efectos de las explosiones, f) Condiciones ambiéntales del proceso, como ubicación, altura, vientos dominantes, velocidad del viento, presión atmosférica, g) Otros datos como enriquecimiento de oxigeno, impacto de los misiles de las explosiones.

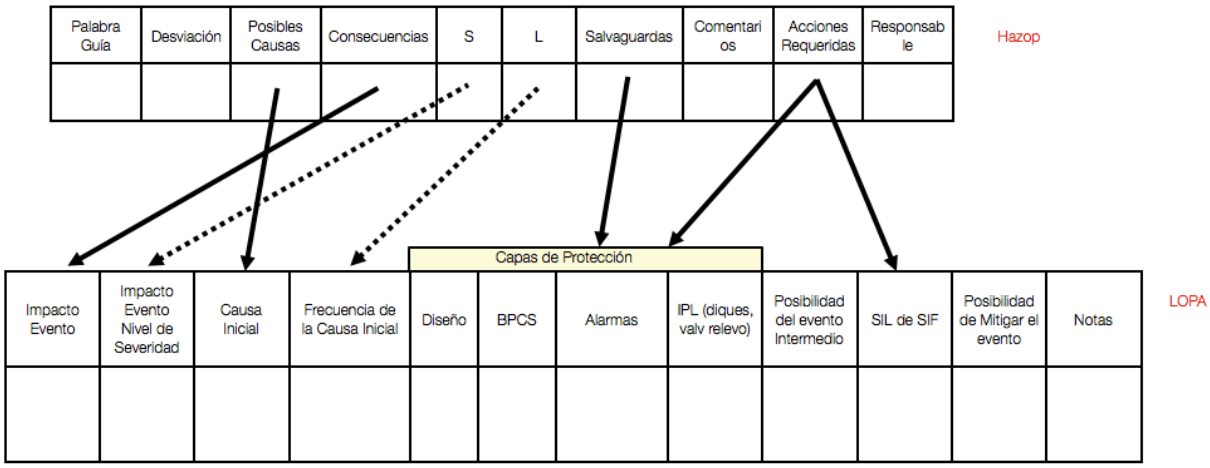
El efecto final del evento puede depender de varios factores entre ellos se incluyen: a) La peligrosidad de las sustancias involucradas, b) Las condiciones en las cuales la sustancia es contenida, c) El tamaño del evento (en términos de que tan rápido la sustancia puede ser liberada y la cantidad de esta), d) La naturaleza del medio en donde es depositada (Agua, concreto, tierra). La información para alimentar los modelos puede ser obtenida de diferentes fuentes pero en general los gobiernos publican información que puede ser de utilidad como son las oficinas meteorológicas, secretarias del medio ambiente, datos locales, etc.

Como un factor importante en el análisis de consecuencias es la determinación del nivel de daño que puede generar el evento. La HSE ha determinado nombrar al nivel de daño como “Dosis Peligrosa”. Una dosis peligrosa es considerada como aquella que puede generar los siguientes efectos sobre la población: 1) Daños severos a casi todos los afectados por el evento, 2) Cuando una sustancial parte de la población requiere atención medica, 3) Algunas personas que son heridas seriamente y requieren tratamiento prolóngalo y 4) Cuando un grupo puede resultar muerto. Las principales razones dadas para el uso de una dosis peligrosa como un criterio de daño en caso de fatalidad son a) La sociedad esta preocupada respecto a lesiones graves y potenciales muertes, b) Hay dificultades técnicas en el calculo de los riesgos dadas las muertes en una condición peligrosa ya que las poblaciones pueden tener un rango de vulnerabilidad diferente.



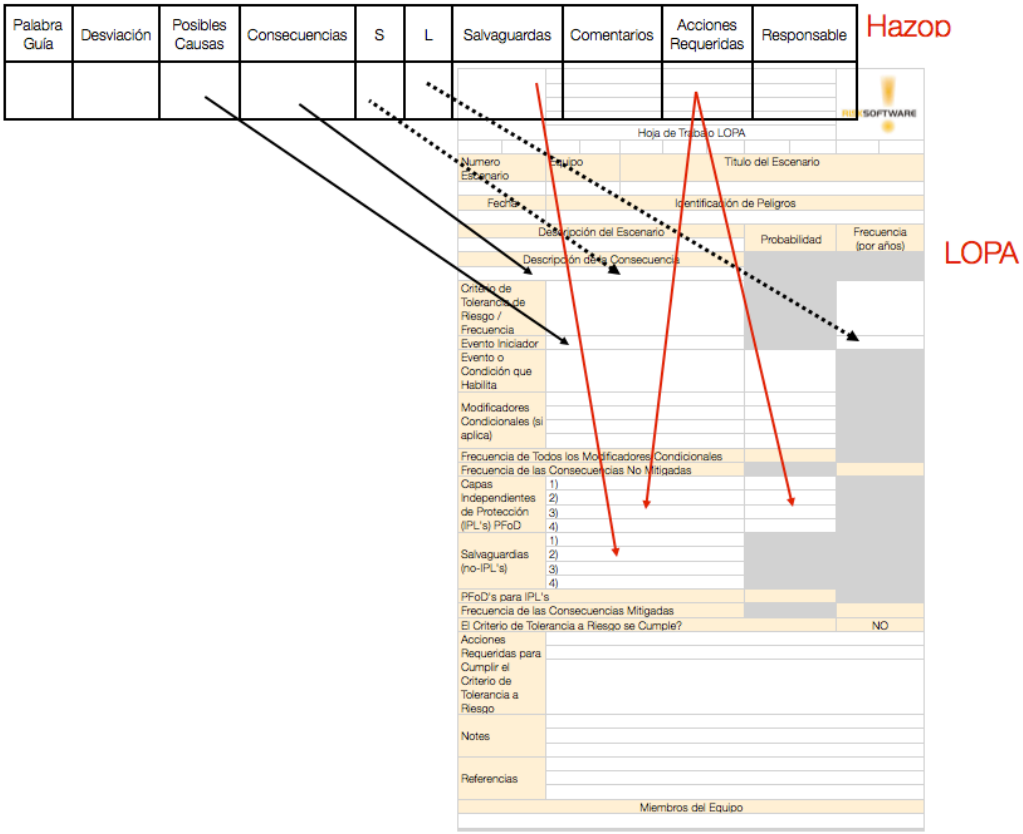

**3) Transferir de Hazop a LOPA.**

Normalmente los software comerciales nos proporcionan herramientas para transferir los estudios Hazop a LOPA, presentamos dos hojas de trabajo típicas.




Las celdas en Hazop que son automáticamente transferidas a la hoja de LOPA son:

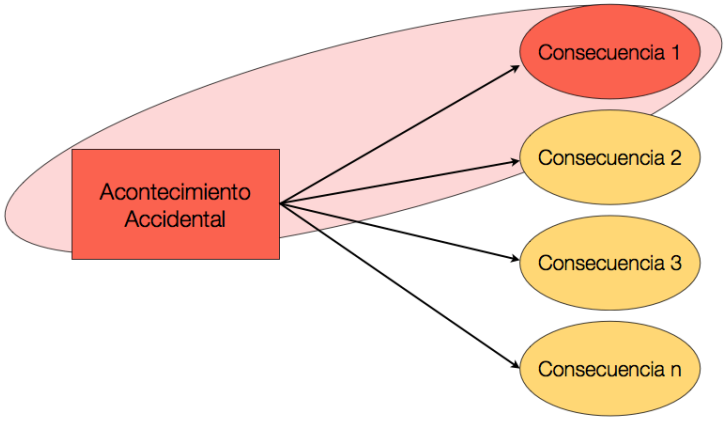
Consecuencias en Hazop = Impacto ó Evento
Posible Causa en Hazop = Causa Inicial en LOPA
(Likelihood) Posibilidad de Consecuencia en Hazop = Frecuencia de la Causa Inicial




Esencial en el proceso de LOPA es la determinación del “Par” Causa Consecuencia
Cada Evento Impacto se compone del par causa consecuencia, un error común en el desarrollo de esta metodología es la de asignar mas de una consecuencia para una causa o bien seleccionar varias causas para una consecuencia.

Cada par debe ser avaluado de forma independiente. Un acontecimiento/evento accidental se define como la primera desviación significativa de una situación normal que puede conducir a consecuencias no deseadas (por ejemplo, fugas de gas, objeto que cae, el inicio de fuego).

Un acontecimiento accidental puede llevar a muchas consecuencias diferentes. Las posibles consecuencias puede ser ilustrada por un espectro de consecuencias:




**5) El método de LOPA tiene como principales características:**

1. Utiliza como punto de partida el establecimiento del Criterio de Tolerancia al Riesgo, puede utilizarse el Riesgo Individual, Social o corporativo.
2. La frecuencia del evento iniciador, este valor puede ser tomado de tablas o valores publicados en bases de datos, de valores corporativos o bien de análisis y simulaciones por medio de arboles de fallas o diagramas de bloques de confiabilidad.
3. Calcula la Frecuencia de las Consecuencias no Mitigadas y de las Consecuencia Mitigadas.
4. Considera eventos o condiciones que permiten que un evento iniciador se propagué, este termino es particularmente importante en procesos tipo batch o procesos que requieren interacción con el operador.
5. Utiliza Modificadores Condicionales, que son circunstancias o eventos que pueden suceder a la par del evento iniciador y que pueden amplificar, modificar o exponenciar el evento iniciador.
6. Considera todas las Capas Independientes de Protección existentes y potencialmente existentes para determinar cuando el criterio de riesgo se cumple utilizando los valores de Probabilidad de Falla Sobre Demanda (PFD), esto permite de forma fácil evaluar las modificaciones y adiciones requeridas para reducir el riesgo a un valor de riesgo necesario.
7. Proporciona información de los requerimientos o modificaciones que hay que realizar en el proceso para cumplir con el criterio de riesgo.

**LOPA es cuantitativo por que se basa en:**

1. Calcula la frecuencia del evento iniciador.
2. Calcula la frecuencia de las consecuencia mitigadas y no mitigadas.
3. Calcula la Probabilidad de Falla sobre Demanda de cada Capa Independientes de Protección.

**LOPA es Semi Cuantitativo por que se basa:**

1. En valores de Criterio de Tolerancia al Riesgo que pueden ser generados por leyes y normas para estimar el Riesgo Social, Individual o corporativo.
2. Puede utilizar valores publicados en tablas o bases de datos para estimar la frecuencia del evento iniciador.
3. Puede utilizar valores publicados para estimar los eventos condicionales y modificadores condicionales.

**LOPA es Cualitativo por que se basa:**

1. En criterios basados en experiencia para seleccionar las Capas de Protección necesarias y mas eficientes.
2. Criterios para asignar eventos condicionales y modificadores condicionales.
3. Criterios para seleccionar el concepto de Tolerancia al Riesgo.

## 8) CONCLUSIONES.

El objetivo del presente documento es el de demostrar los diferentes métodos que existen para la determinación del Nivel de Integridad de Seguridad (SIL), pero también fijamos una posición en el tipo de método adecuado para instalaciones o procesos críticos o de importancia, encontramos que en el mundo las grandes corporaciones petroleras, químicas y petroquímicas utilizan LOPA como el método mas adecuado, la tabla #3 muestra claramente las características de los diferentes métodos, y se puede observar que LOPA representa una ventaja clara debido a que nos proporciona no solamente métodos analíticos para la determinación de frecuencias y probabilidades, también nos proporciona herramienta para el uso de criterios de ingeniería al seleccionar las diferentes capas de protección.

Como comentarios finales incluimos:

1. Las Matrices de Riesgos y Gráficos de riesgos se basan únicamente en criterios y se requiere que las corporaciones tengan claros sus criterios y se halla realmente desarrollado ingeniería en seguridad, aun así el uso de únicamente criterios no es recomendable ya que cada aplicación y proceso es diferente.
2. Las Matrices Calibradas ayudan únicamente cuando la corporación fije los criterios basados en estimaciones y evaluaciones corporativas.
3. Los Gráficos de riesgos con capas de protección facilitan la determinación del SIL ya que consideran las diferentes capas de protección pero no consideran la tolerancia al riesgo, no podemos aceptar que este criterio no sea utilizado ya que si no entendemos lo que tenemos que limitar como podemos fijar los criterios de protección?.
4. LOPA y el Método Cuantitativo de la IEC 61508 son los únicos que utilizan cálculos reales para determinar la frecuencia del evento iniciador y no criterios basados en tablas, también utilizan como valoración la tolerancia al riesgo, y en especial LOPA permite utilizar criterios de ingeniería para determinar que capa de protección debe de ser utilizada.

Los comentarios de este documento expresan el punto de vista de:

Victor Machiavelo Salinas
TUV FS Expert ID-141/09
Risk Software SA de CV

victorm@risksoftware.com.mx
www.risksoftware.com,mx

Agradeceremos cualquier comentario.