INSTITUTO ARGENTINO DEL PETROLEO Y DEL GAS

3er. Congreso Latinoamericano y 1er. Congreso Iberoamericano de Calidad en la Industria del Petróleo y del Gas

Gestión de Riesgo en un Horno de Tratamiento de Petróleo

Sinopsis
Se desarrolló el cálculo del nivel de integridad de seguridad en la instalación de un sistema de control / seguridad de un horno de tratamiento de crudo ubicado en una planta deshidratadora de la UNAS.
Las Normas IEC 61508 y 61511 se utilizaron como marco para la evaluación de nivel de riesgo del equipo bajo control y su entorno operativo, tanto en cuanto al proceso como en cuanto a medio ambiente y legislación.
Se identificaron los escenarios de riesgo posibles, las condiciones de falla y su secuencia en un árbol de fallas de eventos.
Las Funciones Instrumentadas de Seguridad fueron determinadas y se incorporaron Sistemas Instrumentados para cumplir con dicha función y lograr la seguridad funcional requerida.
Se realizó una reducción del riesgo tanto con instalaciones externas como con el propio sistema de seguridad implementado.
Cumpliendo los requisitos que la Norma exige para los elementos de campo y aplicando redundancia (en caso de alto SIL) se logró una considerable reducción de riesgo y con un valor aceptado en la industria.
El desarrollo se vincula con el Modelo de Cálculo de Confiabilidad en instalaciones petroleras de manera de obtener el Nivel de Confiabilidad tanto a nivel operativo como de seguridad.

Introducción

El mantenimiento con base riesgo implica una gestión relevante con políticas establecidas, programas de intervenciones, procedimientos operativos y de mantenimiento, control de cambios y consecuentes optimizaciones.
Esta gestión que incumbe equipos estáticos y sistemas de control de proceso y seguridad con tolerancia a las fallas, autodiagnóstico y redundancia y una cuantificación del riesgo.
Esta evaluación considera efectos a la salud, interrupción del negocio, daños a equipos industriales e impactos ambientales.
Asimismo la gestión de mantenimiento moderno se considera integrada al proyecto, planificando las inspecciones e intervenciones basándose en rigurosos estándares internacionales a fin de garantizar el riesgo tolerable.
El RIESGO se define como el producto de la Frecuencia del Evento por la Consecuencia del mismo y se relaciona con la Integridad física o funcional del equipo bajo estudio.
El riesgo se divide en tres clases (ver Fig.1)

- Clase I: El riesgo es inaceptable
- Clase II: Riesgo no deseado y tolerado solamente si la reducción del riesgo es impracticable.
- Clase III: El riesgo es despreciable.

Los objetivos del presente trabajo fueron:

- Realizar la evaluación de Riesgo y Diseño de Protecciones industriales basándose en los estándares internacionales IEC

- Verificar el nivel de seguridad y proyectar las mejoras necesarias para alcanzar un valor de Riesgo Aceptable y Tolerable.

- Determinar el SIL (Safety Integrity Level) en función de los componentes de riesgo de la unidad operativa y su probabilidad de acontecimiento del evento indeseable.

Tradicionalmente, los sistemas de seguridad estuvieron separados del BPCS (**B**asic **P**rocess **C**ontrol **S**ystem / Sistema de Control del Proceso Básico). El estándar IEC 61511 dentro del marco de la IEC 61508 permite la integración entre sistemas de control y de seguridad en una misma arquitectura (ICSS / **I**ntegrated **C**ontrol and **S**afety **S**ystem) (ver Fig.2). Sin embargo, debe haber una separación funcional suficiente para asegurar que las funciones de seguridad y las que no comprenden la seguridad sean independientes. Las funciones que no están relacionadas con la seguridad no deben afectar peligrosamente a las que si lo están.
Con frecuencia se logra la integración operando las funciones de seguridad y las independientes de la seguridad en procesadores o nodos de control separados.
La instalación analizada es un horno de tratamiento de crudo de una planta deshidratadora. En el cálculo se estimó la probabilidad de falla de la operación del sistema de control del horno, con la finalidad de asegurar la operación sin accidentes, sin fallas peligrosas, y respetando la política de seguridad y medio ambiente establecida por la compañía. Se consideró la operación exitosa del sistema cuando el mismo puede cumplir las funciones para la cual fue diseñado.
El modelo se utilizó en el cálculo de la confiabilidad y riesgo del sistema funcional con su diseño original para luego implementar las acciones resultantes de acuerdo al valor de SIL requerido.
Las condiciones de seguridad y medio ambiente adoptadas por la compañía y las regulaciones gubernamentales exigen constantemente trabajar con grados de confiabilidad aceptados internacionalmente, por lo que este cálculo se ha adoptado como estándar en otros sistemas de similares características.

Desarrollo

El sistema de control original del horno comprendía un PLC (Controlador Lógico Programable) que tenía a su cargo realizar en forma automática el arranque y parada del horno, y a su vez, controlar el funcionamiento del mismo manteniendo un nivel de seguridad aceptable. El sistema sufrió una falla severa, lo cual dejó inoperante al PLC y esto originó un revamping, donde se actualizó la instrumentación del horno y se realizó un nuevo sistema de control luego de la obtención del SIL.
Los sistemas de seguridad toman acción cuando las variables de los equipos y del proceso alcanzan valores fuera del rango de seguridad de los mismos.
Esta situación puede deberse a múltiples motivos, falla de un equipo (rotura de caños, válvulas trabadas), condiciones anormales del proceso (caudal de gas anormal, bajas temperaturas) y falla del propio equipo de control, errores del operador al conducir en manual el proceso, etc.
Una situación particular a considerar es la puesta en marcha normal o de emergencia de un equipo, ya que las variables críticas pueden moverse a valores fuera del rango de seguridad.
Se debe tener en cuenta que las interrupciones inesperadas del proceso son en si mismas peligrosas mas allá de las pérdidas económicas que se producen.
Cumplir con la Confiabilidad que la norma exige, es condición necesaria pero no suficiente, por cuanto debe verificarse que el sistema de seguridad seleccionado garantice un valor de confiabilidad a la no interrupción del proceso suficientemente razonable.

Definiciones Fundamentales
Confiabilidad: Habilidad de un sistema para ejecutar las funciones requeridas, bajo determinadas condiciones, durante un período de tiempo establecido. Se mide como la probabilidad que un sistema esté operativo sin falla

durante el tiempo de la misión.
Falla: Situación en la que el equipo o sistema deja de realizar la ó las funciones para la cual fue diseñado o instalado.
Modo de Falla: Es el efecto por el cual se manifiesta una falla. El modo de falla se lo puede dividir en dos clases principales:

a) No se logra el cambio de estado demandado o requerido.
b) Cambio no deseado en las condiciones o en el estado.

Falla peligrosa: Falla a la función asignada, falla no detectable. Sólo detectable por inspección. La falla peligrosa impide actuar al sistema de seguridad en caso ser demandada su acción, o sea, el sistema está indisponible.
Falla segura: Falla que provoca la acción segura del sistema.
Fracción Falla Segura: Fracción de la tasa de falla total de un equipo, que resulta en una falla segura ó una falla peligrosa detectable
Tolerancia a la Falla: Es el máximo número de fallas en un sub-sistema que puede ocurrir sin llevar el sistema a una falla peligrosa.
Cobertura de Diagnóstico: Es la relación entre la Probabilidad de fallas peligrosas detectables y la probabilidad de fallas totalmente peligrosas.
Probabilidad de Falla Sobre Demanda: Es la que ocurre encontrándose el sistema de protección indisponible.
Tasa de Falla: Se define como Tasa de Falla a la función que nos dice la cantidad de fallas que un ítem tendrá durante un cierto tiempo de vida del mismo.
Árbol de falla: Método sistemático para adquirir información de un sistema. Esta información se puede utilizar para la toma de decisiones, el cual es un proceso complejo.
Contexto operacional: Es el entorno en el cual está trabajando un equipo o sistema. Este entorno es de gran importancia ya que influye en las fallas que puede tener el sistema. En otras palabras, un mismo sistema puede fallar de diferentes maneras según el contexto en el que se encuentre operando.
Equipos Tipo A: Los modos de falla de todos los componentes son bien definidos
Equipos Tipo B: Los modos de falla de al menos un componente no es bien definido.

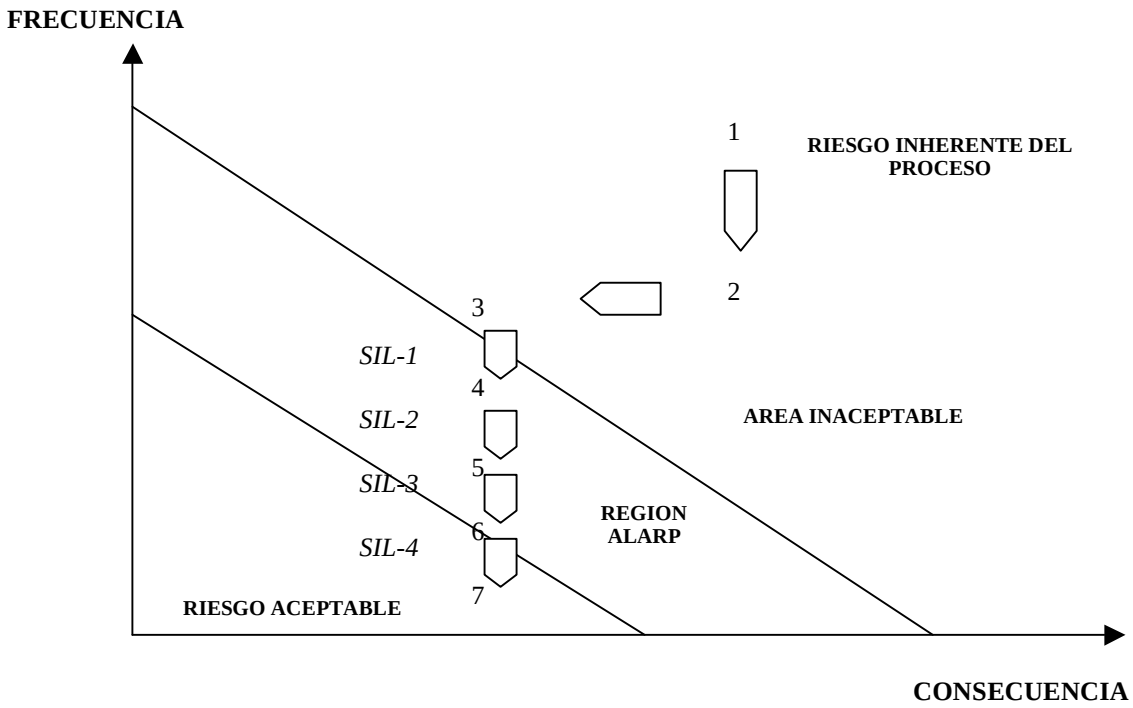
El ciclo de vida de seguridad funcional de un sistema como lo define la IEC 61511 (ver Fig.3)

La fase de análisis (resaltada en color azul claro) está enfocada en la determinación y documentación de cuanta seguridad se requiere o necesita.

La fase de ejecución o realización (resaltada en color verde claro) está enfocada en el diseño mismo y en la implementación del sistema, así como en la documentación del nivel de seguridad alcanzada con dicho diseño.

La fase de operación (resaltada en color rojo claro) está enfocada en las actividades y documentación necesaria para operar y mantener el sistema al nivel integral de seguridad original.

Asignación en la Reducción del Riesgo a Diferentes Sistemas



Evolución 1-2: Uso de tecnologías (PSV, Frecuencias de Inspección, Mejoras de Procedimientos, etc.)
Evolución 2-3: Uso de sistemas externos (Bunkers, Muros de contención, Cortinas de Vapor, Cortinas de Agua, etc.)
Evolución 3-4: Uso de sistemas instrumentados de seguridad. SIL 1
Evolución 4-5-6-7: IEC 61508 Uso de sistemas eléctrico-electrónicos, programables.

Análisis

- Descripción de la instalación
- Análisis Funcional de la unidad funcional
- Definición de los escenarios de riesgo
- Identificación de los componentes de riesgo
- Cuantificación de los componentes de riesgo
- Base de datos generales de la instalación
- Definición de LOPA
- Identificación y validación de LOPA
- Determinación del SIL requerido
- Verificación del SIL existente
- Propuestas de mejora

- Análisis en estado de normal operación
- Análisis de estados transitorios posibles

- Verificación de Integridad Mecánica
- Recipientes a Presión y Temperatura
- Cañerías
- Accesorios, Válvulas, bridas, juntas, etc.

Metodología de Cálculo
Análisis del Nivel de Integridad requerido para el sistema de control y seguridad instrumentada correspondiente a un Horno de Tratamiento de Crudo.
Aplicación del estándar IEC 61508 – Seguridad Funcional de sistemas relacionados con la seguridad
Aplicación del estándar IEC 61511-3
(Ver Fig. 4)

Método Cualitativo "Risk Graph" (Ver fig. 5 y 6)
- Consecuencia del evento indeseable
- Frecuencia y tiempo de exposición en zona peligrosa
- Posibilidad de evitar el evento peligroso
- Probabilidad de ocurrencia del evento no deseado

Método Cualitativo "Severity Matrix" (Ver fig. 7)
- Número de Independientes Sistemas Relacionados con la seguridad
- Número de Facilidades externas para reducción de riesgo (LOPA)
- Severidad del evento indeseable
- Probabilidad del evento indeseable

Método Cuantitativo
- Frecuencia Tolerable para el acontecimiento del evento indeseable
- Frecuencia NO protegida (PFD sobre el sistema de seguridad instrumentado)

Se adoptará como valor de Integridad del Sistema de Protección el que resulte más conservador (seleccionando el peor escenario en temas relacionados con la seguridad)

Antecedentes
- Especificaciones elaboradas por la compañía, códigos aplicados y a aplicar
- PIDs durante la fase de Ingeniería Básica del diseño del equipo
- Diagrama Causa – Efecto
- Especificaciones del equipo en cuanto a piping e integridad
- Historial de incidentes ó accidentes ocurridos en la instalación
- Sistemas de Control Básicos, Lazos de control, Instrumentación

Bases de Datos
- Tasa de Falla según OREDA DATA BANK – 4th Edición – 2002
- Base de Datos de Falla propia
- Otros Bancos de Datos Internacionales
- Documentación del proveedor del equipo
- Documentación del proveedor de instrumentación y control
- Experiencias

Descripción de la instalación

Horno para calentamiento de crudo hidratado, del tipo tubular, radiante y convectivo
Condiciones de Servicio
Calor a transferir: 2300000Kcal/h
Servicio: Calentamiento de crudo
Fluido: Petróleo Hidratado
Caudal: Total: 2800 m3/día, Petróleo: 2632 m3/día, Agua: 168 m3/día
Porcentaje de Agua: 6%
Temperatura de entrada: 40°C
Temperatura de salida: 80 °C
Grado API: 24
Presión de entrada: 8 kg/cm2
Presión de salida: 12 Kg/cm2
Caída admisible de presión: 2 kg/cm2
Combustible: Gas Natural
Exceso de aire máximo: 15%
Rendimiento: 84%
PCI: 8900 Kcal/m3

Tubos: A 106 GrB
Diámetro exterior: 114,3 mm
Schedule Nominal: 40
Máxima temperatura de la pared: 365°C

Análisis de la unidad funcional

Análisis en estado de normal operación
La existencia de un doble loop de control de la temperatura de salida de producto y temperatura de salida de gases de chimenea brinda la posibilidad de un funcionamiento constante del horno en condiciones normales de operación (presiones de entrada de producto, temperatura de entrada de producto, presión de alimentación de gas combustible).
Las secuencias de pre y post barrido otorgan un nivel de seguridad adecuado al momento del arranque y parada normales del equipo.
El sistema de control es el responsable de mantener una temperatura constante de funcionamiento y asegurar la calidad de la combustión. Posee una tolerancia a fallos adecuada para mantener el proceso trabajando a baja temperatura, hasta que la anomalía sea normalizada. La tolerancia se ha implementado a través de redundancia sobre las variables de proceso principales.
El proceso posee un sistema Scada con monitoreo constante de las variables más interesantes.

Análisis de estados transitorios posibles
Las PSVs mecánicas existentes en la línea de gas y de producto serán mantenidas a fin de absorber los transitorios de presión. Dependiendo de la temperatura, es posible un congelamiento de la misma por la expansión y formación de hidratos.

Verificación de Integridad Mecánica: El Vessel esta sujeto a un plan de RBI.
Vessel: Tasa de Falla: 0,0365292 fallas/año

Tubos: Tasa de Falla: 0,00876 fallas/año
Piping: Tasa de Falla: 0,0077 fallas/año
Válvulas: Tasa de Falla: 0,029 fallas/año

Se consideró al horno un sistema integrado con los siguientes subsistemas:

- Puente de Gas Combustible
- Alimentación de Aire
- Sistema de Control
- Sistema de Seguridad
- Recipiente, tubos, piping, válvulas, etc.

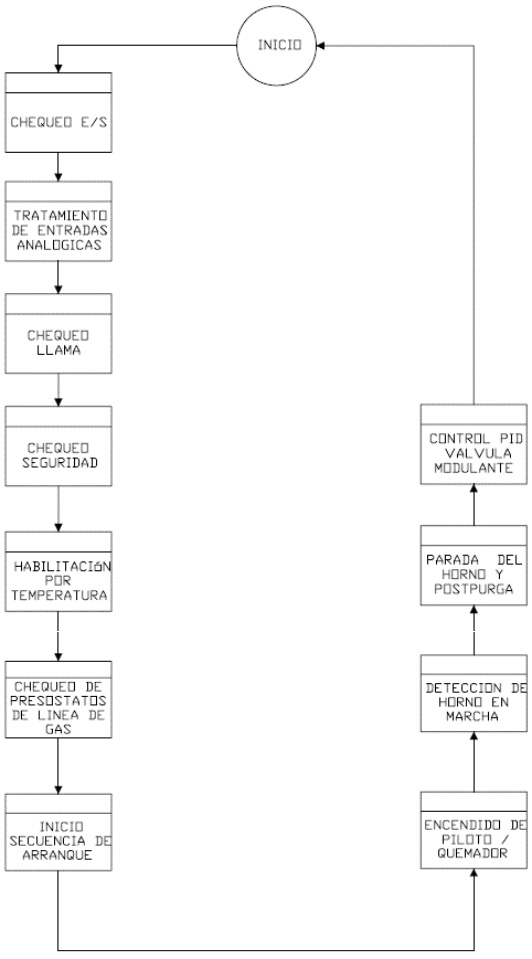
Definición de Funciones del horno
La función principal del sistema es calentar el fluido garantizando un ΔT de +40°C.

Definición de Fallas
No calentar el fluido un ΔT de +40°C.

Definición de Modos de Falla
El sistema deja de cumplir la función para la cual fue diseñado cuando existe cualquiera de los siguientes eventos:

Alta Temperatura de entrada
Alta temperatura de salida
Alta temperatura de salida de gases de chimenea
Alta temperatura en serpentines
Baja Presión de gas regulado
Alta presión de gas de entrada
Alta presión de entrada de producto
Alta presión de salida de producto
Baja presión de entrada de producto
Falta de llama
Baja presión aire en soplador
Rotura del recipiente
Rotura de serpentines
Bajo caudal de salida de producto
Falla válvula de gas a quemador al abrir
Falla válvula de gas a piloto al abrir
Falla secuencia de prebarrido
Falla secuencia de precalentamiento
Falla secuencia de postbarrido
Falla modulación de llama
Falla de alimentación de energía eléctrica
Falla de alimentación de gas
Falla Motor eléctrico soplador
Parada de emergencia

Determinación de Lógica de Control

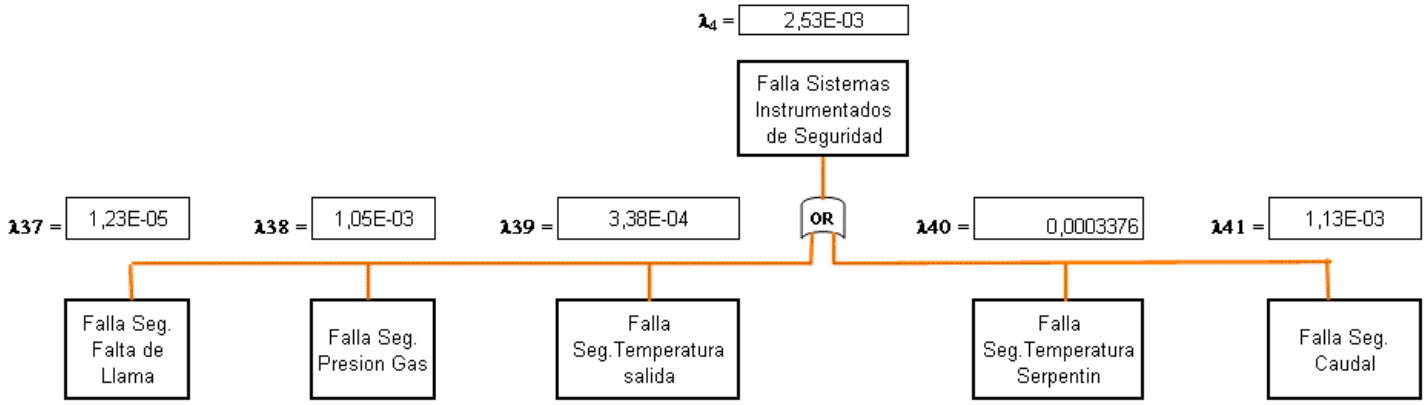


Definición de Funciones Instrumentadas de Seguridad

Alivio de gas ante un aumento de presión de entrada. Parada del horno. Activación secuencia de post barrido
Control de temperatura de salida de producto. Parada del horno.
Control de temperatura de serpentines. Parada del horno. Activación secuencia de post barrido
Control de bajo caudal de salida. Parada del horno.
Control de llama. Parada del horno. Activación de secuencia post barrido

Determinación de Sistemas Instrumentados de Seguridad
Válvula de seguridad instrumentada en la entrada de gas al puente de regulación.
Termostato con lógica 2OO2
Termostato con lógica 2OO2
Flujostato en piping de salida y Presostato Diferencial Lógica 2OO2
Detector de llama con lógica 2OO2

Árbol de Fallas Resumido



Teniendo en cuenta que está la posibilidad de intervención del un operador (falla humana), el nuevo standard IEC-61511 permite adicionar a los cálculos realizados un "**FRR" FACTOR DE REDUCCIÓN DE RIESGO DE 0,1**- Llevando el resultado final a 2,53 E-4, es decir, **"SIL -2".**
Se aceptará una distribución de tasa de falla constante, la cual es suficientemente representativa de la realidad fundamentada en lo siguiente:

- Diferentes distribuciones combinadas para una variedad de componentes sigue una ley exponencial. Esto es demostrable matemáticamente.
- La reparación de fallas en un determinado equipo tiende a producir una tasa de falla constante
- Cuando se trata de comparar confiabilidades entre equipos (confiabilidad relativa) la distribución a tasa de falla constante es excelente.

Para calcular la confiabilidad del sistema se utilizará la siguiente ecuación:

$$R(t) = e^{-\lambda t}$$

Reliability Exponential Function

Lo que nos entrega una confiabilidad del 99,97% en seguridad.

Definición de los escenarios de riesgo

Escenario 1

Generación de una Onda de Presión de entrada de gas motivada por falla en equipos de control aguas arriba, fallas humanas, operativas y/o mantenimiento

El valor de presión supera la presión de diseño de equipos y sistemas incluidos

Equipos involucrados

Línea de Piping

Válvulas

Fitting

Requiere falla funcional de:

Sistema de control primario – Demanda: Tasa de Falla Peligrosa: 3,73 E-02 fallas/año (BASE….)

Sistema de protección secundario: Tasa de Falla: 1,05 E-3 fallas /año (BASE….)

Determinación del SIL requerido

Método Cualitativo "Risk Graph"

- Consecuencia del evento indeseable

C2: Heridas serias permanentes a una o más personas, muerte de una persona.

- Frecuencia y tiempo de exposición en zona peligrosa

F1: Rara frecuencia de exposición en la zona de peligro

- Posibilidad de evitar el evento peligroso

P1: Posibilidad de evitar el evento peligroso bajo ciertas condiciones

- Probabilidad de ocurrencia del evento no deseado

W2: Baja probabilidad de ocurrencia del evento indeseable.

Resultado: SIL 1

Método Cualitativo "Severity Matrix"

- Número de Independientes Sistemas Relacionados con la seguridad

UNO (instrumentado)

- Número de Facilidades externas para reducción de riesgo (LOPA)

UNO (Válvula de Seguridad)

- Severidad del evento indeseable

Serio

- Probabilidad del evento indeseable

Media

Resultado: SIL 1

Método Cuantitativo

- Frecuencia Tolerable para el acontecimiento del evento indeseable

- Frecuencia NO protegida (PFD sobre el sistema de seguridad instrumentado)

La tasa de falla obtenida desde el árbol de fallas es de 1,05E-3 fallas/año
Según valores internacionales estamos en el orden > 1E-3 lo que corresponde a un **SIL 2.** El estándar IEC 61511 permite adicionar un FRR (Factor de Reducción de Riesgo) de 0,1 teniendo en cuenta la intervención del hombre, obteniendo una tasa de falla de 1,05E-4

$$PFD = \frac{F_t}{F_{NP}}$$

$$PFD = Tasa\_Falla\_Peligrosa \times Tiempo\_entre\_tests$$
$$F_t = PFD \times F_{NP}$$
$$F_t = \lambda_D \times Tiempo\_entre\_inspecciones \times Demanda/año$$
$$F_t = SIL \times 0{,}5 años/test \times 1$$
$$F_t = 1{,}05E-4 \times 0{,}5 años/test \times 1 = 5{,}25E-4 (accidentes/año)$$

Validación IEC 61511

Determinación de consecuencia "C"
Número de personas expuestas al área de peligro: Tres personas (3)
Vulnerabilidad: "Grandes pérdidas de material inflamable" V=0,1
Consecuencias: 3 x 0,1 = 0,3 → Corresponde a un rango entre 0,1 y 1,0
Clasificación: C_C
Ocupación del área de riesgo "F"
Rara a más frecuente exposición en la zona. Ocupación menor que el 0,1 del tiempo
Clasificación: F_A
Probabilidad de evitar el evento indeseable "P"
El sistema cuenta con alarmas de control ópticas para la visualización de parámetros importantes para la seguridad del proceso. La intervención manual bloquea los equipos críticos. Sistema red contra incendio disponible 100%. Procedimientos escritos de seguridad con conocimiento y práctica de los operarios.
Clasificación: P_A
Tasa de Demanda "W"
El número de veces por año que el evento se produciría en ausencia de la FIS.
Tasa de demanda entre 0,1 y 1 Demanda por año.
Clasificación: W2
Siguiendo el camino del Risk Graph

C_C -----F_A-------P_A----------W2 → SIL 2

Escenario 2
Generación de una Onda de Presión de entrada de gas, seguida de pérdida, explosión ó fuego en el RSP. El calor producido generará una debilitación del material del recipiente y de los tubos y posible rotura de los mismos.
Equipos involucrados

Vessel
Piping interior

Requiere falla funcional de:
Válvula de seguridad (PSV) mecánica pura – Demanda: Tasa de Falla Peligrosa: 0,0244 fallas/año (BASE….)
Válvula de regulación instrumentada: Tasa de Falla: 3,11E-5 fallas /año (BASE….)
Sistemas de control primario: Demanda – Tasa de Falla Peligrosa: 3,73 E-2 fallas /año (BASE….)

Método Cualitativo "Risk Graph"

- Consecuencia del evento indeseable

C2: Heridas serias permanentes a una o más personas, muerte de una persona.

- Frecuencia y tiempo de exposición en zona peligrosa

F1: Rara frecuencia de exposición en la zona de peligro

- Posibilidad de evitar el evento peligroso

P1: Posibilidad de evitar el evento peligroso bajo ciertas condiciones

- Probabilidad de ocurrencia del evento no deseado

W2: Baja probabilidad de ocurrencia del evento indeseable.

Resultado: SIL 1

Método Cualitativo "Severity Matrix"

- Número de Independientes Sistemas Relacionados con la seguridad

UNO (instrumentado)

- Número de Facilidades externas para reducción de riesgo (LOPA)

UNO (Válvula de Seguridad)

- Severidad del evento indeseable

Extensiva

- Probabilidad del evento indeseable

Media

Resultado: SIL 2

Método Cuantitativo

- Frecuencia Tolerable para el acontecimiento del evento indeseable
- Frecuencia NO protegida (PFD sobre el sistema de seguridad instrumentado)

La tasa de falla obtenida desde el árbol de fallas es de 1,06E-3 fallas/año
Según valores internacionales estamos en el orden > 1E-3 lo que corresponde a un **SIL 2.** El estándar IEC 61511 permite adicionar un FRR (Factor de Reducción de Riesgo) de 0,1 teniendo en cuenta la intervención del hombre, obteniendo una tasa de falla de 1,06E-4

$$PFD = \frac{F_t}{F_{NP}}$$

$$PFD = Tasa\_Falla\_Peligrosa \times Tiempo\_entre\_tests$$

$$F_t = PFD \times F_{NP}$$

$$F_t = \lambda_D \times Tiempo\_entre\_inspecciones \times Demanda / año$$
$$F_t = SIL \times 0{,}5 años / test \times 1$$
$$F_t = 1{,}06E-4 \times 0{,}5 años / test \times 1 = 5{,}31E-4 (accidentes / año)$$

Validación IEC 61511

Determinación de consecuencia "C"
Número de personas expuestas al área de peligro: Tres personas (3)
Vulnerabilidad: "Grandes pérdidas de material inflamable y alta probabilidad de fuego" V=0,5
Consecuencias: 3 x 0,5= 1,5→ Corresponde a un rango mayor a 1,0
Clasificación: C_D
Ocupación del área de riesgo "F"
Rara a más frecuente exposición en la zona. Ocupación menor que el 0,1 del tiempo
Clasificación: F_A
Probabilidad de evitar el evento indeseable "P"
El sistema cuenta con alarmas de control ópticas para la visualización de parámetros importantes para la seguridad del proceso. La intervención manual bloquea los equipos críticos. Sistema red contra incendio disponible 100%. Procedimientos escritos de seguridad con conocimiento y práctica de los operarios.
Clasificación: P_A
Tasa de Demanda "W"
El número de veces por año que el evento se produciría en ausencia de la FIS.
Tasa de demanda entre 0,1 y 1 Demanda por año.
Clasificación: W2
Siguiendo el camino del Risk Graph

C_D -----F_A-------P_A----------W2 → SIL 2

Escenario 3
Generación de incorrecta mezcla explosiva en el interior del vessel motivada por falla en el sistema de control, falla humana, operativa y/o mantenimiento, seguida de explosión.
Equipos involucrados
Vessel
Piping interior
Piping exterior

Requiere falla funcional de:
Sistema de control primario: Demanda – Tasa de Falla Peligrosa: 3,73 E-2 fallas /año (BASE….)
Válvulas de Shut Off: Demanda – Tasa de Falla Peligrosa: 0,438 fallas /año (BASE….)

Método Cualitativo "Risk Graph"

- Consecuencia del evento indeseable

C2: Heridas serias permanentes a una o más personas, muerte de una persona.

- Frecuencia y tiempo de exposición en zona peligrosa

F1: Rara frecuencia de exposición en la zona de peligro

- Posibilidad de evitar el evento peligroso

P1: Posibilidad de evitar el evento peligroso bajo ciertas condiciones

- Probabilidad de ocurrencia del evento no deseado

W1: Muy Baja probabilidad de ocurrencia del evento indeseable.

Resultado: No requiere sistema de seguridad. Se decide un SIL 1

Método Cualitativo "Severity Matrix"

- Número de Independientes Sistemas Relacionados con la seguridad

UNO (instrumentado)

- Número de Facilidades externas para reducción de riesgo (LOPA)

NINGUNA

- Severidad del evento indeseable

Seria

- Probabilidad del evento indeseable

Baja

Resultado: SIL 1

Método Cuantitativo

- Frecuencia Tolerable para el acontecimiento del evento indeseable
- Frecuencia NO protegida (PFD sobre el sistema de seguridad instrumentado)

La tasa de falla obtenida desde el árbol de fallas es de 2,53E-3 fallas/año
Según valores internacionales estamos en el orden > 1E-3 lo que corresponde a un **SIL 2.** El estándar IEC 61511 permite adicionar un FRR (Factor de Reducción de Riesgo) de 0,1 teniendo en cuenta la intervención del hombre, obteniendo una tasa de falla de 2,53E-4

$$PFD = \frac{F_t}{F_{NP}}$$

$$PFD = Tasa\_Falla\_Peligrosa \times Tiempo\_entre\_tests$$
$$F_t = PFD \times F_{NP}$$
$$F_t = \lambda_D \times Tiempo\_entre\_inspecciones \times Demanda/año$$
$$F_t = SIL \times 0{,}5 años/test \times 1$$
$$F_t = 2{,}53E-4 \times 0{,}5 años/test \times 1 = 1{,}26E-4 (accidentes/año)$$

Validación IEC 61511

Determinación de consecuencia "C"
Número de personas expuestas al área de peligro: Tres personas (3)
Vulnerabilidad: "Grandes pérdidas de material inflamable" V=0,1
Consecuencias: 3 x 0,1= 0,3→ Corresponde a un rango entre 0,1 y 1,0
Clasificación: C_C
Ocupación del área de riesgo "F"
Rara a más frecuente exposición en la zona. Ocupación menor que el 0,1 del tiempo
Clasificación: F_A
Probabilidad de evitar el evento indeseable "P"

El sistema cuenta con alarmas de control ópticas para la visualización de parámetros importantes para la seguridad del proceso. La intervención manual bloquea los equipos críticos. Sistema red contra incendio disponible 100%. Procedimientos escritos de seguridad con conocimiento y práctica de los operarios.
Clasificación: P_A
Tasa de Demanda "W"
El número de veces por año que el evento se produciría en ausencia de la FIS.
Tasa de demanda menor que 0,1 Demandas por año.
Clasificación: W1
Siguiendo el camino del Risk Graph

C_C -----F_A-------P_A----------W1 → No requiere sistema de seguridad. Se decide un SIL 1

Escenario 4
Generación de exceso de presión de producto motivada por falla en el proceso, falla humana u operativa, provocando pérdida en piping exterior o en piping interior seguida de fuego.
Equipos involucrados
Piping
Válvulas

Requiere falla funcional de:
Sistema de control primario: Demanda – Tasa de Falla Peligrosa: 3,73 E-2 fallas /año (BASE….)
Válvula de seguridad mecánica pura: Demanda – Tasa de Falla Peligrosa: 0,0244 fallas /año (BASE….)

Método Cualitativo "Risk Graph"

- Consecuencia del evento indeseable

C2: Heridas serias permanentes a una o más personas, muerte de una persona.

- Frecuencia y tiempo de exposición en zona peligrosa

F1: Rara frecuencia de exposición en la zona de peligro

- Posibilidad de evitar el evento peligroso

P1: Posibilidad de evitar el evento peligroso bajo ciertas condiciones

- Probabilidad de ocurrencia del evento no deseado

W1: Muy Baja probabilidad de ocurrencia del evento indeseable.

Resultado: No requiere sistema de seguridad. Se decide un SIL 1

Método Cualitativo "Severity Matrix"

- Número de Independientes Sistemas Relacionados con la seguridad

NINGUNO

- Número de Facilidades externas para reducción de riesgo (LOPA)

UNO (Válvulas de Seguridad)

- Severidad del evento indeseable

Seria

- Probabilidad del evento indeseable

Baja

Resultado: SIL 1

Método Cuantitativo

- Frecuencia Tolerable para el acontecimiento del evento indeseable
- Frecuencia NO protegida (PFD sobre el sistema de seguridad instrumentado)

La tasa de falla obtenida desde el árbol de fallas es de 1,13E-3 fallas/año
Según valores internacionales estamos en el orden > 1E-3 lo que corresponde a un **SIL 2.** El estándar IEC 61511 permite adicionar un FRR (Factor de Reducción de Riesgo) de 0,1 teniendo en cuenta la intervención del hombre, obteniendo una tasa de falla de 1,13E-4

$$PFD = \frac{F_t}{F_{NP}}$$

$$PFD = Tasa\_Falla\_Peligrosa \times Tiempo\_entre\_tests$$
$$F_t = PFD \times F_{NP}$$
$$F_t = \lambda_D \times Tiempo\_entre\_inspecciones \times Demanda/año$$
$$F_t = SIL \times 0{,}5 años/test \times 1$$
$$F_t = 1{,}13E-4 \times 0{,}5 años/test \times 1 = 5{,}64E-5 (accidentes/año)$$

Validación IEC 61511

Determinación de consecuencia “C”
Número de personas expuestas al área de peligro: Tres personas (3)
Vulnerabilidad: “Grandes pérdidas de material inflamable con probabilidad de fuego” V=0,5
Consecuencias: 3 x 0,5= 1,5→ Corresponde a un rango mayor a 1,0
Clasificación: C_D
Ocupación del área de riesgo “F”
Rara a más frecuente exposición en la zona. Ocupación menor que el 0,1 del tiempo
Clasificación: F_B
Probabilidad de evitar el evento indeseable “P”
El sistema cuenta con alarmas de control ópticas para la visualización de parámetros importantes para la seguridad del proceso. La intervención manual bloquea los equipos críticos. Sistema red contra incendio disponible 100%. Procedimientos escritos de seguridad con conocimiento y práctica de los operarios.
Clasificación: P_A

Tasa de Demanda “W”
El número de veces por año que el evento se produciría en ausencia de la FIS.
Tasa de demanda menor que 0,1 Demandas por año.
Clasificación: W1
Siguiendo el camino del Risk Graph

C_D -----F_B-------P_A----------W1 → No requiere sistema de seguridad. Se decide un SIL 2

Propuestas de mejora

Realizar un estudio para la incorporación de facilities relacionadas con la seguridad y que correspondan a nuevas layers de protección. Automatización de RCI, Bloqueos remotos, Enfriamientos del horno en caso de fuego, muros de división con la sala de control, etc.

Si bien el grado de Confiabilidad en la operación del Horno está en el orden del 21% lo cual es un valor relativamente bajo, no obstante es aceptable considerando una alta confiabilidad en la seguridad del sistema, se propone realizar un balance económico para elevar el nivel de confiabilidad en la operación del Horno.

Conclusiones

Los cálculos realizados muestra que los sistemas instrumentados de protección satisfacen las exigencias del estándar IEC 61511.
Se debe considerar además que las coberturas de diagnóstico que se realizan en las inspecciones de mantenimiento son adecuadas para la detección y evaluación de fallas incipientes en los instrumentos y equipos, por lo que debe adicionarse un coeficiente de ajuste de la tasa de falla de los SIS.

Los beneficios producidos en esta gestión fueron:

- El valor de Nivel de Seguridad Integrada (SIL) aplicado es el indicado por los estándares internacionales.
- La tasa de falla del sistema completo es del orden de 7,5 meses a la falla, por lo que el tiempo entre inspecciones utilizado actualmente en mantenimiento (6 meses) es adecuado.
- El valor de confiabilidad de la seguridad del horno es del orden del 99,97 %
- Justificación del proyecto de revamping en base a la cuantificación del riesgo.
- Intervención de Ingeniería de Mantenimiento en el diseño del sistema de control y seguridad generando economía de costo y tiempo en las inspecciones y optimización de recursos.
- Aplicación de actividades de precomisionado y comisionado en la puesta en marcha.
- Operación confiable con una performance de seguridad en niveles internacionales, reduciendo la posibilidad de rotura de equipos y/o accidentes personales.
- Optimización del proceso de planta.
- Aumento de la disponibilidad.
- Disminuir los costos de mantenimiento durante todo el ciclo de vida del activo.

Bibliografía

1. “Programa de Ingeniería y Gestión del Mantenimiento”- Univ. Austral – Modulo III “Confiabilidad, Mantenibilidad y Riesgo” Ing. Héctor Ecay
2. “Actualización de Evaluación de Riesgo Industrial”– Ing. Ecay – 2005 – Univ.Austral
3. “Mantenimiento Centrado en la Confiabilidad”- J.Moubray. 2004. Edición en español
4. “Análisis de Confiabilidad de una Batería Estandarizada” – Pablo Alonso, Luis Palmieri, Angel Moreno- Paper Presentado en las 4tas.Jornadas de Calidad en Mantenimiento. IAPG Neuquén 2006
5. “Offshore Reliability Data” 4ta Edición – 2002 – Oreda Participantes.
6. “Manual de Árbol de fallas” D.F.Haasl, N.Roberts – USA Comisión de Regulaciones Nucleares -1981
7. IEC 61508 y 61511 Estándares Internacionales
8. “Seminario de Seguridad en Oficinas de la BIPC” – T.Morovati -2003. Publicación de Internet

Agradecimientos

- Profesor Ing. Héctor Ecay, Universidad Austral Buenos Aires, por su invalorable ayuda en nuestro análisis y por haber sido nuestro mentor en la Ingeniería de la Confiabilidad.
- Universidad Austral, Buenos Aires, Argentina en las figuras de los Ingenieros Pedro Univaso y Roberto Bottini, en nuestra formación como ingenieros de mantenimiento.
- Ingeniería de Mantenimiento Repsol YPF, por el apoyo recibido en el proyecto.
- Gerencia de Plantas Repsol YPF por el apoyo y compromiso en el estudio e implementación.
- Operativos de Plantas, por su invalorable aporte de experiencia.

Referencias

FPD = Failure Probability on Demand
λ = Failure rate
SIL = Safety Integrity Level
F_t = Frecuencia tolerable del evento indeseable
PFD: Probabilidad de Falla sobre Demanda
Ft: Frecuencia aceptable del accidente
Fnp: Frecuencia del accidente sin protección
λ_D: Tasa de Falla por Demanda
T_{test} : Tiempo entre inspecciones
D: Demanda
PSV: Pressure Safety Valve

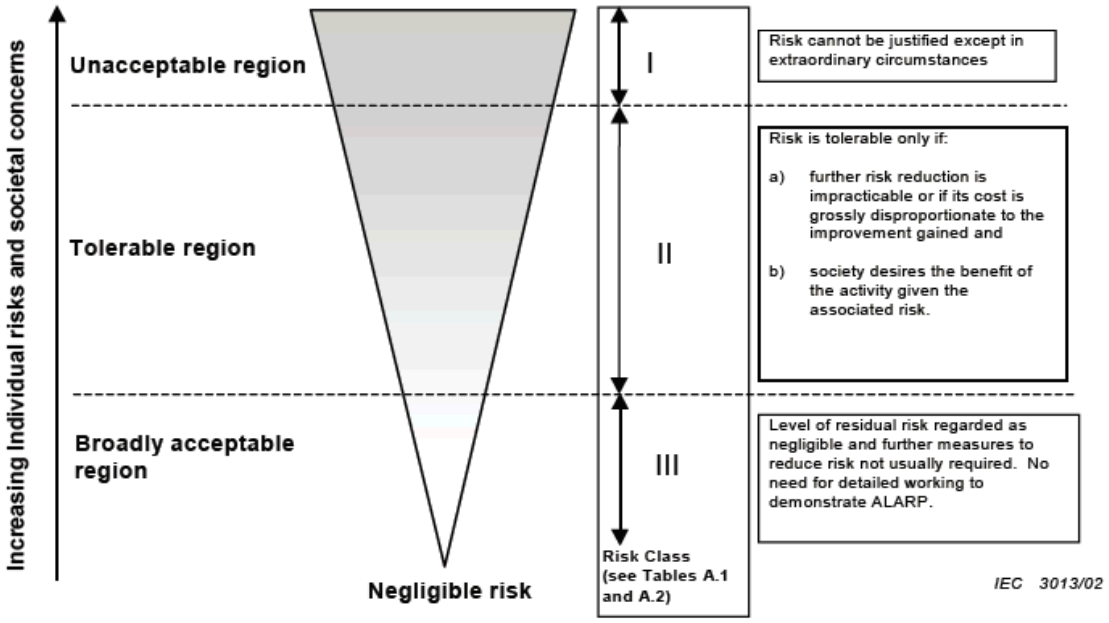


Fig.1 Clasificación de Riesgo

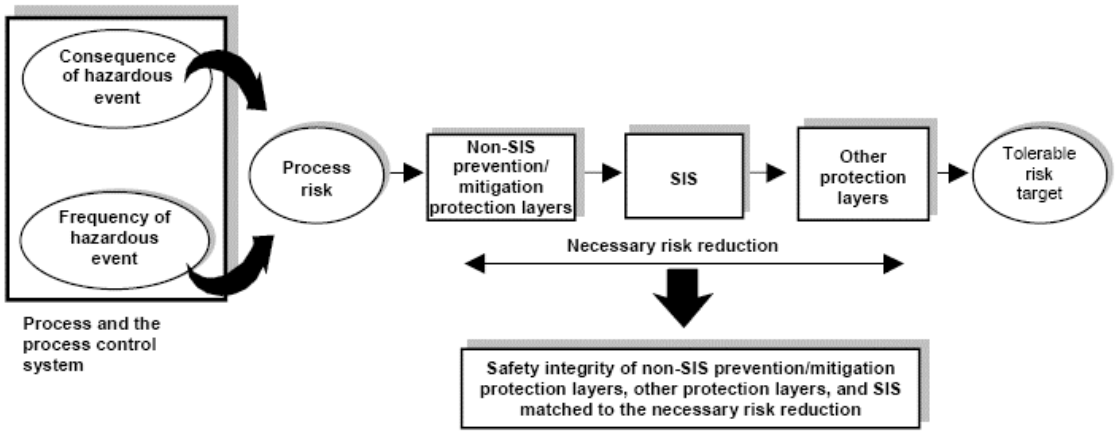


Fig.2 – Conceptos de Riesgo y Seguridad Integrada

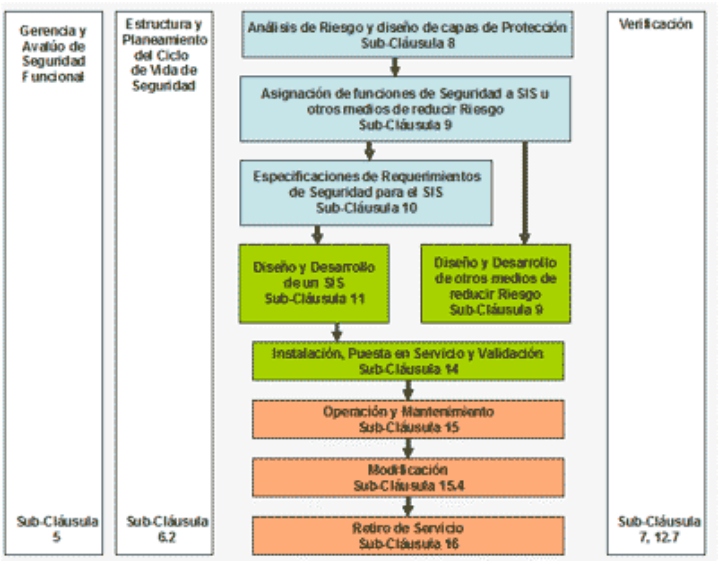


Fig.3 – Fases Ciclo de Vida de un Sistema de Seguridad

Parameter		Description
Consequence	C	Number of fatalities and/or serious injuries likely to result from the occurrence of the hazardous event. Determined by calculating the numbers in the exposed area when the area is occupied taking into account the vulnerability to the hazardous event.
Occupancy	F	Probability that the exposed area is occupied at the time of the hazardous event. Determined by calculating the fraction of time the area is occupied at the time of the hazardous event. This should take into account the possibility of an increased likelihood of persons being in the exposed area in order to investigate abnormal situations which may exist during the build-up to the hazardous event (consider also if this changes the C parameter).
Probability of avoiding the hazard	P	The probability that exposed persons are able to avoid the hazardous situation which exists if the safety instrumented function fails on demand. This depends on there being independent methods of alerting the exposed persons to the hazard prior to the hazard occurring and there being methods of escape.
Demand rate	W	The number of times per year that the hazardous event would occur in the absence of the safety instrumented function under consideration. This can be determined by considering all failures which can lead to the hazardous event and estimating the overall rate of occurrence. Other protection layers should be included in the consideration.

Fig.4 Descripción de parámetros de riesgo

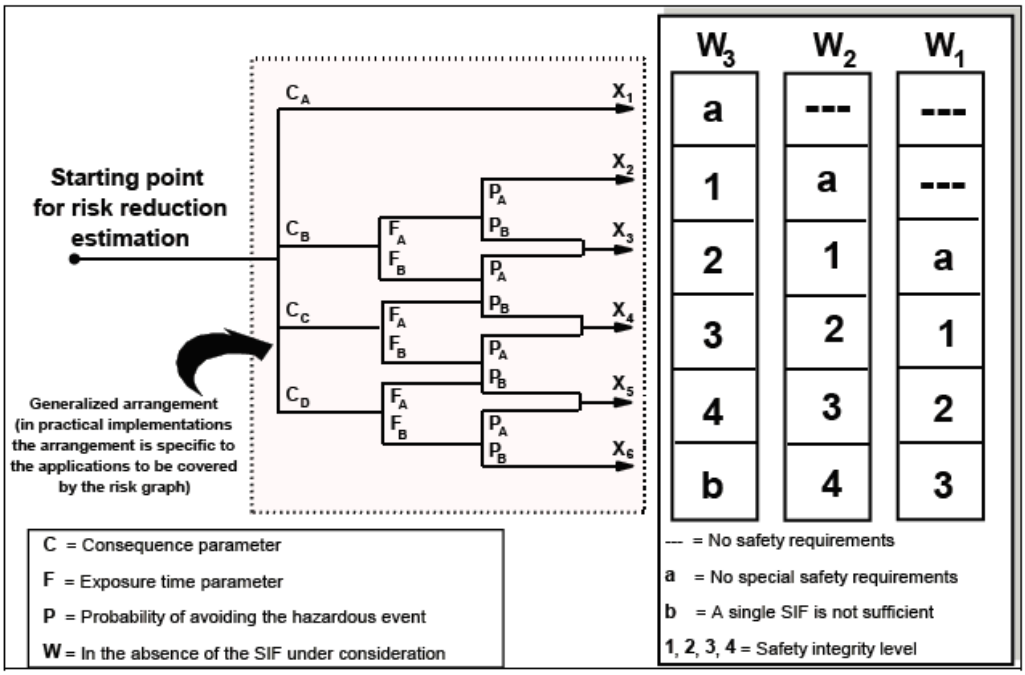


Fig.5 Risk Graph

Risk parameter		Classification	Comments
Consequence (*C*)	C_1	Minor injury	1 The classification system has been developed to deal with injury and death to people. Other classification schemes would need to be developed for environmental or material damage.
	C_2	Serious permanent injury to one or more persons; death to one person	2 For the interpretation of C_1, C_2, C_3 and C_4, the consequences of the accident and normal healing shall be taken into account.
	C_3	Death to several people	
	C_4	Very many people killed	
Frequency of, and exposure time in, the hazardous zone (*F*)	F_1	Rare to more often exposure in the hazardous zone	3 See comment 1 above.
	F_2	Frequent to permanent exposure in the hazardous zone	
Possibility of avoiding the hazardous event (*P*)	P_1	Possible under certain conditions	4 This parameter takes into account – operation of a process (supervised (i.e. operated by skilled or unskilled persons) or unsupervised); – rate of development of the hazardous event (for example suddenly, quickly or slowly); – ease of recognition of danger (for example seen immediately, detected by technical measures or detected without technical measures); – avoidance of hazardous event (for example escape routes possible, not possible or possible under certain conditions); – actual safety experience (such experience may exist with an identical EUC or a similar EUC or may not exist).
	P_2	Almost impossible	
Probability of the unwanted occurrence (*W*)	W_1	A very slight probability that the unwanted occurrences will come to pass and only a few unwanted occurrences are likely	5 The purpose of the *W* factor is to estimate the frequency of the unwanted occurrence taking place without the addition of any safety-related systems (E/E/PE or other technology) but including any external risk reduction facilities.
	W_2	A slight probability that the unwanted occurrences will come to pass and few unwanted occurrences are likely	6 If little or no experience exists of the EUC, or the EUC control system, or of a similar EUC and EUC control system, the estimation of the *W* factor may be made by calculation. In such an event a worst case prediction shall be made.
	W_3	A relatively high probability that the unwanted occurrences will come to pass and frequent unwanted occurrences are likely	

Fig.6 – Tabla Risk Graph

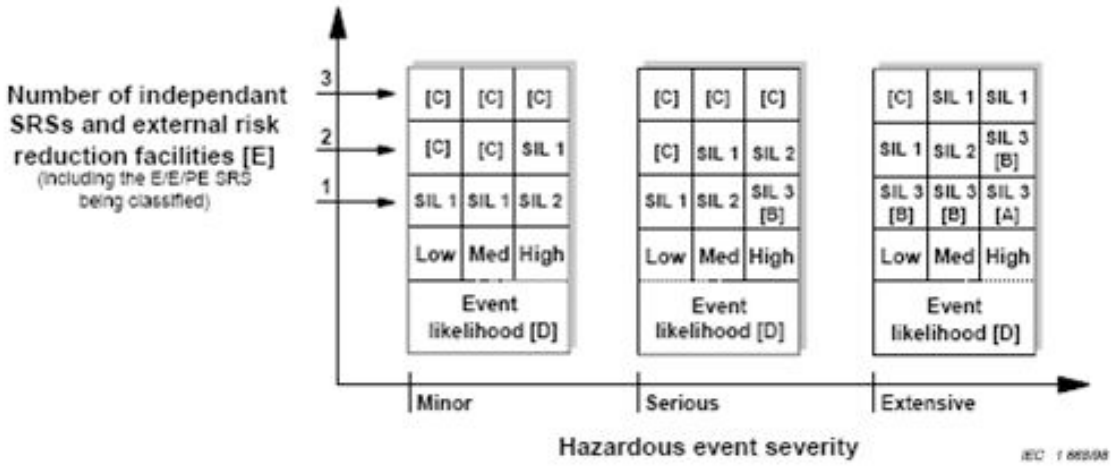


Fig.7 Severity Matrix