

	<b>Título:</b> ASIGNACIÓN SIL A LAS FUNCIONES INSTRUMENTADAS DE SEGURIDAD	
<b>Código:</b> PG-1-DGSMS-81-B	<b>Aprobador:</b> GGL	<b>Fecha de aprobación:</b> 06/10/2022
	<b>Gestor:</b> GGL/DGSMS	<b>Firma:</b> Omar Alarcón Saigua

## 1. OBJETIVO

Describir y dar pautas acerca de la metodología a seguir para la asignación de funciones de seguridad a las capas de protección y asignación de los Niveles de Integridad de Seguridad(SIL) a las Funciones Instrumentadas de Seguridad (SIF) de acuerdo con la norma IEC 61511-1:2003 capítulo 9.

## 2. ALCANCE

Aplica tanto a instalaciones existentes (planta, unidad de proceso, almacenamiento, carga y descarga, servicios técnicos, etc., propiedad de YPFB Refinación, S.A.) como para nuevos proyectos (nuevas plantas, nuevas unidades y/o modificación de existentes) que constituyan un riesgo de carácter significativo en la refinería

## 3. DOCUMENTOS COMPLEMENTARIOS

### 3.1. NORMAS

ISO 9001: Sistema de Gestión de la Calidad.  
 ISO 14001: Sistema de Gestión de Medio Ambiente.  
 ISO 45001: Sistemas de gestión de la seguridad y salud en el trabajo  
 ISO 17776: Petroleum and natural gas industries—Offshore production installations—Guidelines on tools and techniques for hazard identification and risk assessment.  
 IEC 61508: Seguridad funcional de los sistemas eléctricos / electrónicos / electrónicos programables relacionados con la seguridad.  
 IEC 61511: Seguridad funcional. Sistemas instrumentados de seguridad para el sector de las industrias de procesos.  
 VDI/VDE 2180 Safeguarding of industrial process plants by means of process controlengineering

### 3.2. PROCEDIMIENTOS DE TRABAJO

**PG-3-ING-4** GESTION DE CAMBIOS DE INSTALACIONES Y TECNOLOGIA EN LA REFINERIA GUALBERTO VILLARROEL  
**PG-2-ING-2** GESTIÓN DE CAMBIOS DE INSTALACIONES Y TECNOLOGÍA  
**PG-1-DGSMS-86** PROCEDIMIENTO GENERAL PARA LA REALIZACIÓN DE ESTUDIOS DE RIESGO  
**PG-1-DGSMS-80** PROCEDIMIENTO PARA LA REALIZACIÓN DE ESTUDIOS LOPA

### 3.3. LEGISLACIÓN

Ley de Medio Ambiente 1333/96 y sus correspondiente Reglamentos.

Ley de Hidrocarburos 3058/05 y el Reglamento Ambiental para el Sector Hidrocarburos (RASH).

Reglamento 25502/99 para Construcción y Operaciones de Refinerías, Plantas Petroquímicas y Unidades de Proceso.

Ley General 16998/76 de Higiene, Seguridad Ocupacional y Bienestar.

## 4. DEFINICIONES Y SIGLAS

### 4.1. DEFINICIONES

**Evento:** Cualquier suceso relevante para que se produzca un escenario. En un análisis LOPA se usan eventos iniciadores y eventos condicionantes a diferencia de un estudio de asignación del SIL donde un evento puede referirse a todo el escenario de accidente (desde su inicio hasta sus consecuencias finales).

**Evento iniciador:** El evento que actúa como punto de partida del escenario y que da lugar a las consecuencias indeseadas. No confundir con las causas o eventos básicos.

Se pueden distinguir tres tipos de eventos iniciadores

- a. Eventos externos
- b. Fallos en equipos
- c. Fallos humanos o acciones inapropiadas

**Evento condicionante:** Un evento es condicionante de un evento iniciador cuando es necesario para que dicho evento dé lugar a los diferentes eventos finales o consecuencias.

Los eventos condicionantes no son fallos ni capas de protección. Se expresan como probabilidades y sólo se usan si son necesarios. Se considerarán siempre antes del LoC

**Consecuencia:** Los resultados de la desviación en caso de que ocurra. Las consecuencias pueden abarcar tanto riesgos asociados al proceso, como problemas de operatividad, tal como parada de la planta o pérdida de calidad del producto. Pueden asociarse varias consecuencias para una misma causa y, a su vez, una sola consecuencia puede ser originada por varias causas. Ver **daño**

**Daño:** Perjuicio, lesión o detrimento que se produce sobre elementos vulnerables sometidos a los efectos derivados de situaciones de peligro. Los daños pueden ser: sobre la salud y seguridad de las personas (trabajadores o público en general), sobre el medio ambiente o sobre la propiedad (el patrimonio o cualquier activo intangible asociado a la imagen de YPFBR). Todo daño tiene asociado un riesgo que debe ser evaluado.

**LoC:** Pérdida de contención o fuga (*Loss of Containment*)

Evento superior (*Top event*) en un árbol de fallos y punto de partida de un árbol de eventos. El nodo central en un modelo *BowTie*. El punto límite entre la prevención y la mitigación

**Modificador condicional:** Una condición que es necesaria para que, a partir de una pérdida de contención, la consecuencia ocurra

Los modificadores condicionales no son fallos ni capas de protección. Se expresan como probabilidades. Sólo se usan si son necesarios. Se considerarán siempre después del LoC

**Frecuencia:** Número de ocurrencias por unidad de tiempo

Es la unidad común para expresar escenarios, eventos y fallos de capas de protección

**Probabilidad:** Existen razones para creer que sucederá

Cuantificación de la posibilidad de ocurrencia de un evento o de una secuencia de acontecimientos durante un intervalo de tiempo, o posibilidad de éxito o fracaso de una actuación bajo demanda

La probabilidad se expresa de modo adimensional y comprendida entre 0 y 1

**Riesgo:** Es una medida o índice que combina la severidad y la probabilidad asociados a un peligro identificado

**Causa básica** (*root cause*): El sistema o causa más básica que posibilita una cadena de eventos y su efecto o resultado indeseado

**Prevención:** Reducción de riesgo mediante medidas destinadas a reducir la probabilidad de la causa básica o los eventos condicionantes. Por ejemplo: Buenas prácticas de diseño de procesos, el BPCS, SIS, sistemas de alivio de presión, alarmas, etc.

**Mitigación:** Reducción de riesgo mediante medidas destinadas a reducir las consecuencias una vez ha ocurrido el incidente (Ej. pérdida de contención). Por ejemplo: Sistema Fire & Gas, alarmas, PPE, cubetos y diques, planes de emergencia, extintores de fuego, brigada de bomberos, etc.

**Efectos físicos:** Resultado directo de una pérdida de contención o fuga

Los efectos físicos se expresan mediante variables tales como concentración en el aire, intensidad de la radiación térmica, pico de sobrepresión de una onda expansiva. Normalmente son función de la distancia

**Peligro:** Capacidad de un sistema o situación de causar daños. Por ejemplo: Fuga de producto tóxico, inflamable, etc

**Causa:** Condición o estado que da lugar directamente a una LoC

**Capa de protección o salvaguarda:** Una salvaguarda es un mecanismo, sistema o acción que puede interrumpir la cadena de eventos desencadenados desde el evento iniciador, evitando la materialización del peligro. Las salvaguardas se clasifican en técnicas y organizativas

**Salvaguarda organizativa:** Previenen la aparición de peligros derivados del error humano

**Salvaguarda técnica:** Previenen la aparición de peligros (Sistema Básico de Control de Proceso, Sistema Instrumentado de Seguridad, PSV, etc.) o mitigan sus efectos (Sistema Fire & Gas, cubetos y diques, red contra incendios, etc.).

**Capa Independiente de Protección:** Es una salvaguarda específicamente diseñada para reducir el riesgo. Para que una salvaguarda pueda ser considerada como una capa de protección independiente se deben cumplir los siguientes criterios: debe ser efectiva, debe ser independiente y debe ser auditable

**Probabilidad de fallo en demanda (PFD):** La probabilidad de que un sistema falle cuando se le requiere para ejecutar una función específica. Ver también probabilidad.

**Probabilidad de fallo (PoF):** La probabilidad que tiene un sistema de fallar mientras ejecuta una función específica durante un intervalo de tiempo. Ver también probabilidad

**Escenario de peligro:** Situación identificada en un proceso que puede ocasionar daño en caso de que se desarrolle completamente y sin control

Cada escenario es una única cadena '*evento iniciador - causa - LoC - consecuencia*'. Debe contener, como mínimo, dos elementos: evento iniciador y consecuencia.

**Medidas críticas de seguridad:** Medidas que son esenciales para reducir el riesgo desde un nivel inaceptable a un nivel aceptable

Las actividades críticas de seguridad o el equipo pueden ser una IPL por si misma o puede mejorar la fiabilidad de una IPL (Por ejemplo: reducir la PoF). Las actividades críticas de seguridad no se deben confundir con 'actividades peligrosas'.

**SIL:** Nivel de integridad de la seguridad. Una especificación o medida de la bondad con la que una SIF (o función instrumentada de seguridad) realiza correctamente una acción. El nivel SIL es el recíproco a la probabilidad de fallo en la ejecución de su función.

**Recomendación:** Es una medida correctiva resultante de un estudio ARP definida para reducir el riesgo de un posible escenario accidental

**Comentarios:** Cualquier aclaración a hacer a las recomendaciones o a aspectos surgidos durante las sesiones de asignación SIL

**Grupo de SIL:** Personas designadas por la Gerencia de Área / Sectorial o de Proyecto para realizar estudios SIL

## 4.2. SIGLAS

**ALARP:** As Low As Reasonably Practicable

**ARP:** Análisis de Riesgos de Proceso

**ASME** American Society of Mechanical Engineers

**ASP:** Administración de Seguridad de los Procesos

**HAZOP:** Hazard and Operability Analysis (Análisis de Peligros y Operabilidad)

**IEC:** International Electrotechnical Comisión

**IPL:** Independent Protection Layer (Capa de protección independiente)

**LoC:** Loss of Containment (Pérdida de contención o Fuga)

**LOPA:** Layers of Protection Analysis (Análisis de las capas de protección)

**PFD:** Process Flow Diagrams (Diagrama de flujo de proceso)

**PFD:** Probability of Failure on Demand (Probabilidad de fallo en demanda)

**PLC:** Programmable Logic Controller (Controlador programable)

**PSV:** Process Safety Valve (Válvula de seguridad)

**RAC:** Risk Acceptance Criteria (Criterios de aceptabilidad de riesgo)

**RG:** Risk Gap (diferencia entre el nivel de riesgo requerido y el real sin capas de protección)

**ROSOV:** Remote Operated Shut-Off Valve (Válvula de corte operada remotamente)

**RRF:** Risk Reduction Factor (Factor de reducción del riesgo)

**SIF:** Safety Instrumented Function (Función instrumentada de seguridad)

**SIL:** Safety Integrity Level (Nivel de integridad de la seguridad)

**SIS:** Safety Instrumented System (Sistema instrumentado de seguridad)

**SRS:** Safety Requirement Specification (Especificación de los requerimientos de seguridad)

**TSO:** Tight Shut Off

**UFD:** Utility Flow Diagrams (Diagramas de flujo de servicios)

**2B&B:** Double block and bleed (doble bloqueo y venteo).

## 5. RESPONSABILIDADES

### 5.1 GERENTES DE ÁREA / SECTORIAL O GERENTE DE PROYECTO

- En base a lo establecido en el PG-1-DGSMS-86 Procedimiento General para la realización de Estudios de Riesgos, decidir cuándo se tiene que llevar a cabo el estudio de asignación SIL.
- Designar el grupo de personas que deben intervenir en el estudio de asignación SIL
- Garantizar que las actividades bajo su control sean manejadas de acuerdo con este procedimiento.
- Definir el responsable de plantear al resto de participantes la propuesta de SIF del proyecto, proceso o instalación a estudiar

### 5.2 FACILITADOR DE SIL

- Garantizar que el equipo SIL siga el presente procedimiento.

- Liderar las sesiones de ejecución y desarrollo del estudio de asignación SIL.
- Fomentar el debate de ideas con el fin de garantizar una elevada calidad en los resultados.
- Asegurar que se realiza el registro de todos los hallazgos del estudio de asignación SIL.

### **5.3 SECRETARIO SIL**

- Registrar todos los hallazgos del estudio de asignación SIL.
- Participar en los talleres SIL según el requerimiento.

### **5.4 GRUPO DE SIL**

- Participar activamente en los talleres SIL según el requerimiento.

### **5.5 PERSONAL SST**

- Asesorar acerca del uso de la metodología SIL.

### **5.6 COMITÉ ASP**

- Garantizar el desarrollo y mantenimiento del registro del estudio de asignación SIL.
- Realizar el seguimiento e implementación de las recomendaciones identificadas en el estudio de asignación SIL.
- Verificar mediante inspecciones el seguimiento de las recomendaciones establecidas en el estudio de asignación SIL.

## **6. MEDIDAS DE SMS**

No aplica

## **7. DESARROLLO**

### **7.1 INTRODUCCIÓN**

#### **7.1.1. Sistemas de mitigación instrumentados de seguridad**

Se considera que los siguientes sistemas de mitigación quedan fuera del alcance del presente procedimiento:

- Fire & Gas (Sistemas de protección contra incendios, sistemas de detección de gases, etc.)
- Sistemas de paro de emergencia mediante pulsadores manuales.
- Válvulas de aislamiento de accionamiento remoto manual (ROSOV).
- Sistemas de despresurización y vaciado de emergencia mediante pulsadores manuales.

En efecto, la IEC 61511 se basa en conceptos que van dirigidos a las funciones instrumentadas de seguridad que son capas de protección preventivas, aunque deja la puerta abierta a su aplicación a las capas de mitigación. El problema con los sistemas de mitigación instrumentados de seguridad es que no siempre pueden identificar la condición de peligro (p.ej. el viento sopla en dirección opuesta a la ubicación de los detectores de gas) y no siempre pueden evitar o mitigar correctamente el peligro (p.ej. el diluvio puede no extinguir un fuego grande; una despresurización de emergencia puede no ser suficientemente rápida para evitar una acumulación de gases). Puede que un sistema instrumentado de mitigación cumpla por diseño un SIL 2 pero que no resulte en una función SIL 2, es decir que no reduzca el riesgo en un factor de 100.

#### **7.1.2. La asignación SIL en el ciclo de vida de la seguridad**

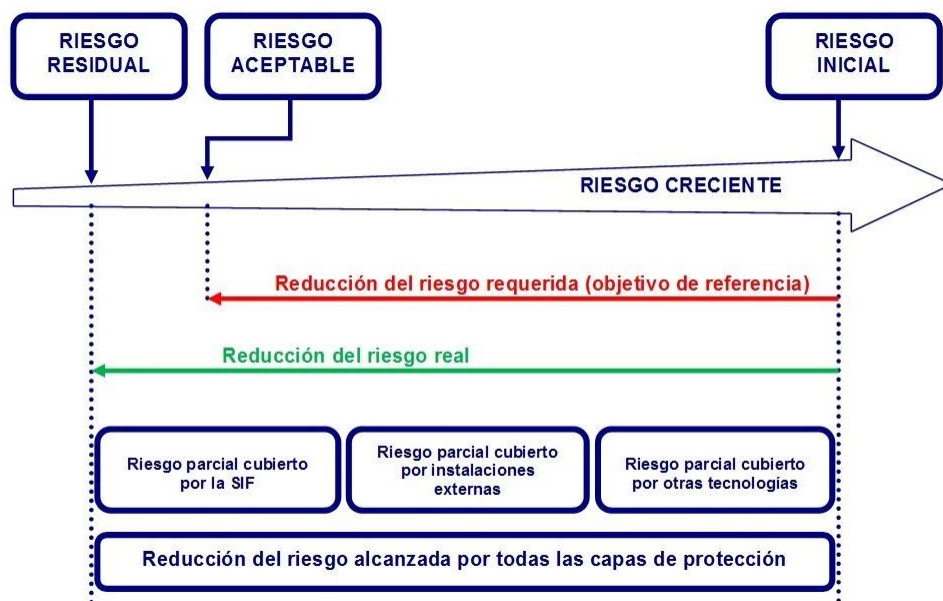
La asignación de funciones instrumentadas como sistema de prevención para la seguridad, protección del medioambiente, de las instalaciones y de la producción, así como la determinación

del correspondiente nivel de SIL, es uno de los primeros pasos en el ciclo de vida de la seguridad según la norma IEC 61511. Esta actividad se lleva a cabo a continuación del análisis de los peligros y riesgos del proceso (ARP), como por ejemplo HAZOP, una vez determinados los escenarios accidentales y las salvaguardas o capas de protección.

Concluida esta fase, se procede a definir los requerimientos y especificaciones de diseño del SIS y de otras medidas de reducción de riesgos.

### 7.1.3. Reducción del riesgo con capas de protección

El riesgo inicial asociado a la operación de una planta de proceso o de un equipo (riesgo inherente) se puede reducir mediante varias medidas de reducción de riesgo entre las cuales están las funciones instrumentadas de seguridad. La figura 1 muestra que la suma de la contribución de todas ellas debe llevar el riesgo remanente (p.ej. riesgo del proceso una vez se han incluido todas las capas de protección: riesgo actual) a un nivel inferior al riesgo de referencia (definido por criterios corporativos).



**Figura 1:** Reducción del riesgo - Conceptos generales (adaptado de IEC 61508-5)

Las medidas de reducción de riesgo o capas de protección, incluyendo las SIF pueden estar incluidas en el diseño original o pueden ser requeridas tras un análisis de los peligros y riesgos del proceso (generalmente un HAZOP). El presente procedimiento presenta una metodología para determinar la reducción de riesgo respecto al objetivo de referencia, la reducción de riesgo alcanzada por cada capa de protección, y el SIL requerido para las SIF de modo que el riesgo inicial del proceso sea reducido a un nivel inferior al nivel de referencia.

Los riesgos contemplados en el Anexo E de la Parte 3 de la norma IEC 61511 se refieren a los riesgos del proceso hacia las personas. El presente procedimiento contempla los riesgos del proceso hacia las personas, el medio ambiente, las instalaciones y la producción, teniendo en consideración el **Anexo D** de la Parte 3 de la misma norma.

### 7.1.4. Introducción a la metodología de asignación SIL

La metodología desarrollada en este procedimiento es un proceso de varios pasos, que dependen del nivel SIL asignado a cada función SIF, tal y como se muestra en el flujograma del **Anexo A**.

Previamente al estudio que se describe en este procedimiento, es necesario identificar los escenarios peligrosos y las funciones instrumentadas de seguridad que requieren estudio.

La primera etapa (véase **Sección 7.5.1**) descrita en este procedimiento, es un método cualitativo. En primer lugar, para cada escenario se estima la reducción de riesgo requerida con gráficos de riesgo (se aplican tres gráficos, para la seguridad de las personas, el medio ambiente y protección de las instalaciones y la producción). A continuación, se analiza la independencia de cada una de las capas de protección y la reducción de riesgo efectiva que llevan a cabo. Se precisará una SIF, a la que será necesario asignar un SIL, cuando el conjunto de capas de protección independientes no instrumentadas no sean capaces de reducir el riesgo del proceso hasta el nivel de referencia.

La segunda etapa (véase **Sección 7.5.2** y PG-1-DGSMS-80 PROCEDIMIENTO PARA LA REALIZACIÓN DE ESTUDIOS LOPA) consiste en un análisis detallado y cuantitativo del riesgo y solo será necesario llevarla a cabo en:

- aquellos escenarios que requieran la instalación de una SIF con  $SIL \geq 2$  de acuerdo a los gráficos de riesgo;
- cualquier escenario, si se cree conveniente para lograr un cálculo más riguroso del nivel de integridad requerido.

Este análisis incluye la preparación de árboles de fallos y/o eventos detallados y eventualmente un estudio de consecuencias. El valor de SIL de la SIF quedará confirmado o por el contrario se modificará, al comparar el riesgo del “escenario protegido” con los criterios de referencia de aceptación de riesgo.

Adicionalmente, para aquellos escenarios para los cuales se requiera un SIL 3 motivado por los importantes daños a las instalaciones y a la producción (siendo menor el SIL requerido por los daños hacia el personal o el medio ambiente), se deberá realizar un estudio coste-beneficio (o demostración ALARP) para evaluar la mejor opción económica entre asumir un riesgo mayor o implementar un SIS más fiable y costoso.

## **7.2 PLANIFICACIÓN Y ORGANIZACIÓN DE LA ASIGNACIÓN DE SIL**

La planificación de la asignación de SIL (definición del alcance, calendario, nivel de competencia del equipo de trabajo, asignación de responsable, documentación, etc.) es parte de la planificación del ciclo de vida del SIS

### **7.2.1. Alcance**

El Alcance del estudio de asignación de SIL será el conjunto de Funciones Instrumentadas de Seguridad SIF identificadas durante el estudio de identificación de peligros (normalmente HAZOP), ya sean salvaguardas previstas en el proyecto o propuestas de acciones o recomendaciones.

### **7.2.2. Programación**

La programación del estudio de asignación de SIL se realizará en conjunto con la del estudio HAZOP correspondiente. Normalmente, el estudio de asignación de SIL se lleva a cabo a continuación del estudio HAZOP pues para su realización se precisa la información y datos generados en el estudio HAZOP.

Conviene dejar un periodo de tiempo entre la finalización del estudio HAZOP y el inicio del estudio de asignación SIL, al objeto de permitir la revisión del estudio HAZOP y, a partir de éste, elaborar las fichas de asignación SIL (**Anexo D**), para facilitar el análisis.



### 7.2.3. Equipo

El equipo que lleva a cabo la asignación SIL debería ser el mismo que ha participado en el estudio HAZOP. El equipo deberá estar formado por personal competente y responsable de las siguientes áreas: diseño y tecnología del proceso, seguridad del proceso, instrumentación y control de procesos, operaciones. La calidad del estudio será proporcional a la competencia del personal implicado en el mismo. Se recomienda que el grupo no supere las 6 - 8 personas.

La norma IEC 61511-3, Anexo D, apartado D.4 propone la siguiente composición típica para el equipo de asignación de SIL:

- Un especialista de proceso;
- Una persona de control de procesos;
- Un responsable de gestión de operaciones;
- Una persona de seguridad;
- Una persona con experiencia práctica en la operación del proceso que se considera.

Es importante que la persona de operación se elija entre aquellos que tengan la mayor experiencia posible ya que la calidad del estudio SIL está relacionada con su experiencia.

Se consultarán personas de otras áreas cuando se evalúen las SIF de un área específica (por ejemplo, para las SIF relacionadas con compresores se requerirá la participación de especialistas en equipos dinámicos). Así, personas de áreas concretas tales como especialistas en equipos dinámicos y estáticos, especialistas en materiales, etc. deberán estar disponibles para poder ser consultados cuando se requiera su ayuda.

El facilitador de las sesiones será un experto en la metodología de asignación de SIL. El papel del facilitador será guiar al equipo durante los distintos pasos del proceso de asignación de SIL, marcar las normas establecidas para la asignación y garantizar que cada paso queda registrado de forma satisfactoria para el equipo antes de proceder con el siguiente escenario. Dos de los objetivos más importantes del facilitador son avanzar en el estudio de acuerdo con la planificación y evitar desviaciones del procedimiento a seguir. El facilitador deberá ser personal entrenado de YPF Refinación, S.A. y/o pertenecer a una compañía calificada para este tipo de estudios.

Cuando sea necesario llevar a cabo la segunda etapa (véase **Sección 7.5.2**) no se realiza en equipo, sino que es el facilitador de la primera etapa (asignación mediante gráficos de riesgo) u otro experto en la metodología y en el proceso objeto de análisis, quien llevará a cabo

la segunda etapa individualmente o con ayuda de otras personas según sea necesario, y enviará los resultados y explicaciones pertinentes al resto del equipo.

### 7.2.4. Documentación e información requerida

Los siguientes documentos conformarán como mínimo la información de partida para las discusiones y deberán estar disponibles con suficiente antelación para que el equipo y el facilitador puedan revisarla y prepararse para el ejercicio SIL (por ejemplo, 3 semanas):

- Procedimiento de asignación de SIL a las funciones instrumentadas de seguridad
- Diagramas de flujo de procesos (PFD) y diagramas de flujo de servicios (UFD)
- Diagramas de tuberías e instrumentación (P&IDs)
- Descripción del proceso y sus distintos modos de operación (puesta en marcha, operación normal y parada)
- Fichas de datos de seguridad de las sustancias
- Descripción del sistema de control.
- Informe del análisis de peligros y riesgos del proceso ARP (HAZOP, WHAT IF, HAZID)
- Información del VENDOR sobre los escenarios a analizar



- Análisis de riesgo preliminar, Estudio de Alcance de Consecuencias y/o Análisis Cuantitativo de Riesgo (ACR) si están disponibles.
- Estudio de impacto ambiental si está disponible
- Plano de implantación de la planta
- Reglas y supuestos que se vayan a emplear en el estudio SIL tales como:
  - Políticas de venteo y descargas a la antorcha,
  - Plantilla y ubicación del personal de operación y mantenimiento,
  - Etc.
- Descripción del sistema de enclavamientos
- Matriz causa / efecto

Los análisis de riesgos y estudios medioambientales serán de gran ayuda para seleccionar los parámetros de consecuencias para la seguridad del personal y el medioambiente (**C** y **E** en el gráfico de riesgos). Se recomienda encarecidamente que el equipo consulte esta información durante el estudio SIL, lo cual requiere la presencia de especialistas en seguridad, medioambiente y salud.

La documentación deberá estar actualizada, especialmente el ARP, los P&IDs y la matriz de causas y efectos, para evitar perder tiempo y tener que rehacer luego trabajo.

Para la realización de un análisis de riesgo cuantitativo (segunda etapa), se necesitará la misma documentación de partida, así como las fichas de asignación de SIL e información sobre tasas de fallos de equipos y de intervención humana. Si el especialista responsable de este análisis requiriese más información, ésta debería por supuesto facilitársele. También es posible que el especialista requiera la utilización de software específico para el cálculo de las consecuencias y de las frecuencias.

### 7.2.5 Preparación

Para minimizar los retrasos y pérdida de tiempo de los miembros del equipo, la revisión íntegra de la documentación de partida deberá realizarse antes de las sesiones del estudio SIL. Esto incluye:

- Identificar y listar todas las SIF, y sus correspondientes escenarios, a partir del estudio HAZOP y/o de la matriz causa-efecto o de la descripción de enclavamientos
- Identificar y listar los escenarios adicionales para los cuales se recomienda una SIF (u otra capa de protección) aunque no aparezca en la matriz causa efecto y la descripción de enclavamientos. Dichas recomendaciones normalmente deben haberse identificado durante el estudio HAZOP.
- Identificar y listar los escenarios de consecuencias sinérgicas, cuando varias SIF comparten el mismo elemento iniciador o elemento final. (ver explicaciones más adelante)

Los resultados del ARP deberán de estudiarse cuidadosamente para asegurar que se incluyenen la lista aquellas SIF potencialmente requeridas y que no están todavía implementadas, o que tampoco se han identificado en la matriz de causas y efectos y en los P&IDs.

Se rellenará previamente al estudio la primera parte de la ficha de asignación de SIL del **Anexo D** hasta la descripción de las “consecuencias sin mitigación”. Adicionalmente, se incluirá la lista de capas de protección o salvaguardas, sin asignar la reducción de riesgo que proporcionan (p.ej. sin asignar los créditos de las IPL).

Cualquier información introducida preliminarmente en el registro de una SIF deberá ser revisada por el equipo durante las sesiones.

Las sesiones se realizarán proyectando en una pantalla mural las fichas de asignación SIL

con el desarrollo del estudio, para que el equipo pueda acordar la redacción del informe.

Para la realización del Análisis de Riesgo Cuantitativo (segunda etapa de la asignación de SIL) la preparación no es tan crucial debido a que no se realiza en equipo.

## 7.3 REDUCIR EL RIESGO CON CAPAS DE PROTECCIÓN

### 7.3.1. Capas de protección – Conceptos generales

De acuerdo con lo indicado en la introducción, las salvaguardas o capas de protección o medidas de reducción de riesgos son necesarias para que el riesgo de las instalaciones sea aceptable según los criterios de referencia de YPFB Refinación, S.A. y cumplan con los requisitos legales locales, nacionales o internacionales y con las buenas prácticas de diseño.

Las capas de protección previstas durante el diseño, se revisarán durante el estudio ARP. En algunos casos se pueden recomendar capas de protección adicionales. Durante el estudio de asignación de SIL se analiza para cada escenario la independencia de las capas de protección tanto entre sí, como con el evento iniciador. Se verifica su eficacia para reducir el riesgo significativamente, bien reduciendo la frecuencia de ocurrencia o bien la severidad de las consecuencias. Los distintos tipos de capas de protección se describen en detalle en el **Anexo B**.

### 7.3.2. Requerimientos esenciales de las IPL (Independent Protection Layer)

En este apartado se indican los requisitos esenciales de las capas de protección para que puedan ser consideradas “capas de protección independiente” (IPL) y para que se les pueda otorgar una contribución en la reducción del riesgo:

- Una IPL debe ser **independiente** de las otras capas de protección y de los eventos que causan el accidente.

**Independencia:** Por ejemplo, el fallo de un transmisor de nivel incluido en un lazo de control de nivel puede ser la causa de un sobrellenado y rebose. Este transmisor, a pesar de tener configurada una alarma de alto nivel, fallará al dar la alarma al operador. Por lo tanto, para este escenario, no se podrá considerar que la capa de protección “supervisión del BPCS e intervención humana” es una IPL.

- Una IPL debe ser capaz de **detectar, decidir, proteger** y ser **específica** para un escenario.

**Medida de prevención para un escenario específico:** Muchas acciones relacionadas con la seguridad no actúan de forma específica ante un escenario de riesgo. Por ejemplo, la formación del personal o el mantenimiento afectan a la eficacia de algunas IPL. No obstante, dichas actividades en sí mismas nunca prevendrán un escenario porque no detectan irregularidades, no deciden qué camino seguir y no evitarán el escenario (prevención o mitigación). Por tanto, está claro que la formación del personal, el mantenimiento y otras actividades afectan a la probabilidad de que las IPL funcionen cuando sean requeridas, pero no pueden ser consideradas IPL.

- Una IPL tiene que ser **suficientemente grande** (capacidad física), **suficientemente rápida** (para actuar), **suficientemente inteligente** (bien diseñada) y **suficientemente robusta**.

**Suficientemente grande, rápida, inteligente y robusta:** Una válvula de alivio de presión (PSV), por ejemplo, es una capa de protección. Sin embargo, para ser eficaz, ésta debe ser capaz de descargar una cantidad determinada de producto en un tiempo determinado. Así, si en el caso de una reacción *runaway* la presión aumenta demasiado rápido para que la PSV pueda descargar suficiente producto, en esta situación, una PSV no se puede considerar una IPL.

- Una IPL debe ser **suficientemente fiable**.

**Fiabilidad:** Una IPL debe ser razonablemente fiable. Por ejemplo, una IPL debe reducir la frecuencia de ocurrencia del escenario de accidente en al menos un factor 10.

- Una IPL debe ser **auditable**.

**Auditable:** La correcta operación, mantenimiento y supervisión de una IPL deberá ser auditable en cualquier momento, para verificar que la función para la que ha sido diseñada se mantiene.

La evaluación de estos criterios debe ser documentada de una manera lógica y sistemática permitiendo así controles y auditorías de validación. Esto también aplica a los registros de mantenimiento e informes de pruebas en caso de ser requeridos.

### **Todas las IPL son salvaguardas, pero no todas las salvaguardas son IPL.**

#### **7.3.3. Orden de preferencia para la selección de IPL**

Existen reglas de preferencia para la selección de capas de protección. Aunque el presente procedimiento presenta un método para asignar un nivel SIL a cada SIF, NO significa que la mejor capa de protección sea un SIF y siempre que sea posible, se debe reconsiderar su instalación por una salvaguarda de otro tipo que proporcione una mayor reducción de riesgo.

De manera general, es mejor una capa de protección que actúe lo antes posible en el desarrollo del escenario, que sea preventiva mejor que de mitigación, que sea simple y de fácil mantenimiento y que sea pasiva mejor que activa. Siguiendo esa idea, el orden de preferencia es el siguiente:

- Diseñar el proceso para eliminar el problema utilizando principios de seguridad inherente al mismo, es decir tratar de sustituir requisitos de seguridad funcional por otros de seguridad no funcional.
- Protección con un sistema no instrumentado. Para estos sistemas, la preferencia en la elección será primeramente sistemas de protección mecánicos pasivos (por ejemplo, doble pared, dique o un disco de ruptura antes que un dispositivo mecánico activo que tenga el mismo efecto.
- Una función instrumentada de seguridad o SIF. Esta debería ser una solución de diseños sólo se debería considerar cuando otras soluciones no son practicables. Las SIF pueden producir tanto fallos peligrosos como seguros (espurios)

#### **7.4 IDENTIFICACIÓN DE LAS SIF**

Antes de proceder al estudio de asignación SIL es necesario identificar todos los escenarios objeto del estudio (Ver Sección 7.2.5).

A continuación, se define que es una SIF y se dan pautas para ayudar a su identificación.

##### **7.4.1. Descripción de una SIF y un SIS**

Una Función Instrumentada de Seguridad (SIF) es una función de seguridad implementada mediante Sistemas Instrumentados de Seguridad (SIS) cuyo propósito es llevar a estado seguro o, mantener en estado seguro, un proceso frente a un evento peligroso. El SIS que realiza una SIF está formado por:

- **Detectores**, que pueden ser uno o más de uno. Se incluyen todos los componentes desde la conexión con el proceso hasta la tarjeta de entrada del procesador.
- **Procesador lógico:** Generalmente un PLC de seguridad.
- **Elementos finales:** Se incluyen todos los elementos desde la tarjeta de salida "output" del procesador, hasta el dispositivo que es actuado y los servicios asociados como el suministro

de aire y electricidad para la actuación del SIS. Pueden ser uno o más de uno.

El (Los) elemento(s) detector(es) de un SIS son todos aquellos cuya función es detectar un peligro, y van desde un único detector, hasta múltiples detectores del mismo parámetro, o en algunos casos múltiples detectores de diferentes parámetros que todos juntos dan una indicación del peligro.

- Uno o más detectores individuales de un SIS específico podrán ser parte de otro SIS.

- El(Los) elemento(s) final(es) del SIS tienen como misión llevar el proceso a estado seguro evitando el peligro.
- Uno o varios elementos finales de un SIS específico también podrán formar parte de otro SIS.
- Tanto los detectores como los elementos finales podrán configurarse en una arquitectura o configuración robusta teniendo en cuenta los fallos peligrosos y/o seguros.

Los sistemas de control protegen unidades de proceso y equipos manteniendo las variables de proceso dentro del rango normal de operación. Ejemplos son los lazos de control de mínimo caudal, o los lazos de control de presión (máxima o mínima). A pesar de ello, estos sistemas no se consideran SIS y por lo tanto no se les asignan un SIL. Sin embargo, estos sistemas constituyen una capa de protección (capa de control de procesos) y pueden considerarse como medidas de reducción de riesgo (ver Sección 7.3 y el Anexo B, Sección B).

Las alarmas son parte de la capa de control y como tales ayudan a reducir las demandas sobre las SIS. Sin embargo, las alarmas no se consideran SIF.

La asignación de SIL deberá cubrir a todas las SIF, y por tanto, cada SIF deberá haberse identificado previamente. Para las SIF formadas por un detector simple y un elemento final simple esto puede resultar sencillo. Sin embargo, cuando varias SIF comparten detectores o elementos finales se deberá establecer una distinción clara de los componentes.

Las SIF independientes con detectores comunes o con elementos finales comunes deberán estudiarse individualmente durante las sesiones de asignación del SIL considerando que las otras funciones son capas de protección que reducen el riesgo en función de su correspondiente SIL y por tanto, que funcionan adecuadamente. Si un detector actúa sobre dos o más elementos finales, aplicando esta regla resulta que únicamente deberá considerarse el fallo de un elemento final. En estos casos, es necesario realizar una evaluación más que considere el fallo del detector. Se trata de la evaluación de las consecuencias sinérgicas que se describe en detalle a continuación.

De la correcta definición de una SIF depende llegar a conclusiones adecuadas durante el estudio SIL.

#### **7.4.2. Evaluación de las sinergias**

Cuando varias SIF tienen un elemento detector en común, cada una de ellas se evalúa considerando solo el fallo del elemento final y que las otras SIF funcionan correctamente reduciendo el riesgo en un orden de magnitud equivalente al SIL que se les asigna. A continuación, hay que considerar la posibilidad de fallo del elemento detector y valorar las consecuencias de esta sinergia, que pueden redundar en un aumento o disminución del nivel SIL del detector.

Este enfoque no es aplicable cuando varios detectores de distintas SIF actúan sobre el mismo elemento final debido a que en esta configuración solamente el fallo del elemento final se considera para cada SIF individualmente

#### **7.4.3. Modos de funcionamiento del SIS**

La norma IEC 61511 define dos modos de funcionamiento de las SIF: el modo 'bajo demanda' y el modo continuo. El modo de funcionamiento 'bajo demanda' significa que el tiempo entre cada

demanda del proceso para que actúe el SIS (p.ej. entre cada vez que se presenta el peligro y que se requiere el funcionamiento de la SIF) es muy superior al intervalo entre pruebas periódicas y el intervalo entre diagnósticos automáticos. El presente procedimiento solo aplica para las SIF que funcionen en modo 'bajo demanda' que corresponde a la gran mayoría de los casos.

## 7.5 METODOLOGÍA PARA LA ASIGNACIÓN SIL

La metodología de asignación SIL puede tener dos etapas dependiendo del nivel asignado en la primera, así como una etapa opcional:

- Primera etapa: método cualitativo de los gráficos de riesgo.
- Segunda etapa: método cuantitativo: con cálculo de las frecuencias de las consecuencias.
- Etapa opcional: Estudio coste-beneficio o demostración ALARP.

Las dos etapas principales del proceso de asignación de SIL se muestran en el flujograma del **Anexo A**.

### 7.5.1. Primera etapa: Estudio cualitativo con gráficos de riesgo

El método presentado a continuación procede del método descrito en IEC 61511-3 Anexo E adaptado para su aplicación en YPF Refinación, S.A.

En consecuencia, por razones de congruencia con dicha norma, no se emplea la matriz de riesgos de YPF Refinación, S.A. (Ver PG-1-DGSMS- 86 Procedimiento general para la realización de Estudios de Riesgos), aunque se han adaptado, en la medida de lo posible, los distintos niveles de severidad de las consecuencias y probabilidad de los escenarios.

Para prevenir incongruencias, durante la realización del estudio HAZOP, aquellos escenarios en los que las salvaguardas incluyan alguna SIF o se recomiende alguna SIF, no se efectuará la evaluación del riesgo, dejando dicha actividad para el estudio de asignación SIL.

#### 7.5.1.1. Evaluación del 'Risk Gap'

La metodología consiste en evaluar cualitativamente el impacto potencial de cada escenario accidental mediante los tres gráficos de riesgo presentados en el **Anexo E**. Se consideran tres tipos de impactos o consecuencias:

- Impacto sobre la salud y la seguridad de las personas
- Impacto sobre el medioambiente
- Impacto sobre las instalaciones y la producción.

El impacto sobre la imagen o la reputación de YPF Refinación, S.A. no se tendrá en cuenta explícitamente debido a la dificultad de una valoración objetiva sobre tal impacto.

Los parámetros de los gráficos de riesgos se listan a continuación:

- **C** Consecuencias personales
- **E** Consecuencias medio ambientales
- **A** Consecuencias para las instalaciones y/o la producción
- **F** Probabilidad de presencia de personas
- **P** Probabilidad de evitar las consecuencias una vez desencadenado el evento
- **W** Frecuencia del escenario.

Dado que este método es cualitativo es importante mantener la coherencia, objetividad, transparencia y repetibilidad durante la selección de estos parámetros. Las directrices para la selección de los mismos se presentan a continuación.

#### 7.5.1.1.1 Frecuencia o probabilidad de ocurrencia del evento indeseado (W)

El propósito del parámetro **W** es estimar la frecuencia del escenario no deseado (el par causa-escenario de peligro o consecuencia en estudio) sin tener en cuenta los sistemas de seguridad. Sólo se tienen en cuenta las seguridades inherentes al proceso y sus sistemas básicos de control. No se tiene en cuenta por lo tanto ninguna capa de protección (p.ej. supervisión del operador, acciones manuales, SIFs, PSVs, etc.).

Los gráficos de riesgos presentados en el **Anexo E** sólo persiguen que el equipo valore la frecuencia del evento durante la vida de la planta. No debe confundirse con la probabilidad del evento iniciador. Se consideran:

- Eventos frecuentes (pequeñas fugas de productos inflamables).
- Eventos que puedan ocurrir una vez durante la vida de la planta.
- Eventos no esperables durante la vida de la planta, como p.ej. una explosión de una nube inflamable (VCE) en una unidad.

W1 Estimación cualitativa: el evento no es esperable en la vida de la planta.

[Equivalente a:  $0 \leq W1 < 10^{-2} \text{ años}^{-1}$ ].

W2 Estimación cualitativa por defecto: el evento es esperable en la vida de la **planta** (media geométrica de 30 años @ esperanza de vida de la planta).

[Equivalente a:  $10^{-2} \text{ años}^{-1} \leq W2 < 10^{-1} \text{ años}^{-1}$ ].

W3 Estimación cualitativa: el evento es esperable varias veces en la vida de la planta (pero no más de una vez al año).

[Equivalente a:  $10^{-1} \text{ años}^{-1} \leq W3 \leq 1 \text{ años}^{-1}$ ].

La **Sección 7.5.1.1.7** proporciona más indicaciones para ayudar a seleccionar el parámetro **W**.

#### 7.5.1.1.2. Parámetro de consecuencias para las personas (C)

Para estimar el parámetro **C**, se deben considerar las consecuencias “potencialmente creíbles” sin las capas de protección. Se debe considerar el número de personas presentes cuando está ocupada la zona expuesta al peligro. Para ello se necesita conocer los datos de ubicación de personal en la planta (operación, mantenimiento, etc.).

C0 Lesión menor de una persona

- Lesión leve, sin baja médica

C1 Lesión moderada de una persona, sin poder resultar en una muerte

- Lesión grave necesitando hasta 30 días de baja médica
- Restricción en el trabajo o enfermedad ocupacional afectando la capacidad de trabajo
- Efectos graves pero reversibles sobre la salud (p.ej. irritaciones, quemaduras de extensión moderada)

Ejemplos de escenarios:

- Quemaduras de personal por falta de aislamiento en tuberías con fluidos entre 50 y 100° C.
- Pequeñas fugas en bridas de tuberías con sustancias no tóxicas.
- Cortes con astillas y/o trozos de acero o herrumbre o con mallas de aislamiento.
- Descarga de electricidad estática debido a una mala conexión a tierra de un equipo.
- Derrame de producto caliente durante la carga de un camión y el líquido entra en el calzado del operador.

C2 Lesión seria o muy seria de una o varias personas, o una muerte

Ejemplos y consideraciones:

- Discapacidad parcial o seria permanente o enfermedad ocupacional o lesión muy grave resultando en la baja médica prolongada de más de 30 días de una o varias personas
- Una muerte Ejemplos de escenarios:
- Explosión de una nube de polvo en una planta.
- Quemaduras extensas de un operador durante el encendido de un quemador (o unacaldera).
- Llamaradas o explosiones debido a pequeñas fugas en bridas de producto inflamable procedente de un equipo de proceso no presurizado.
- Pequeñas fugas tóxicas. P.ej. una fuga repentina de un gas rico en  $H_2S$  a través de unabrida o de una válvula.
- Rotura de tubería que transportan material peligroso (p.ej. rotura de una línea de vaciado de un reactor o en un sistema caliente de condensado).

#### C3 Muerte de varias personas (de 2 a 9)

- Hay que tener en cuenta que cuando los operadores trabajan por parejas o en equipo, existe la tendencia de ayudar a los compañeros en caso de un accidente. La asfixia de un operador en un área con  $H_2S$  a menudo lleva a la muerte de varios operadores si no están bien entrenados en ponerse primero el equipo de protección.
- Fugas importantes de materiales inflamables, gases tóxicos, vapor, etc.
- Rotura de un equipo con elevada energía mecánica, p.ej. un compresor grande o una turbina. Una puesta en marcha fallida de una turbina podría atraer a demasiados espectadores; un nuevo intento podría dañar la carcasa (frecuencia crítica) y chorros de vapor a 100 bar podrían afectar a los presentes.

#### C4 Muerte de muchas personas (10 o más)

Ejemplos y consideraciones:

- Fugas masivas de sustancias inflamables o tóxicas. Entre otras razones, estas fugas pueden ser el resultado de:
  - Un orificio de 25 mm en una línea con líquido supercalentado (p.ej. benceno a 250° C y 30 bar, o GLP a temperatura ambiente.
  - Un orificio de 100 mm en un sistema de alta presión (> 10 bar) de vapor o gas.
  - Un iniciador como la rotura catastrófica de la una línea causada por una fractura frágil debido a la auto-refrigeración en una evaporación por flash o una expansión (GLP, etileno, LNG o error humano).
  - Explosiones o incendios masivos en almacenamientos (BLEVE, *boil-over*, *roll-over*, etc.).
  - Fallo de la antorcha.

#### 7.5.1.1.3. Parámetro de la probabilidad de presencia de personas (F)

Es importante considerar los escenarios de manera coherente a lo largo de todo el estudio respecto a la probabilidad de presencia de personal o ocupación de la zona expuesta al peligro (proporción de tiempo en el que la zona expuesta al peligro está ocupada durante un periodo normal de trabajo).

#### F1 Exposición en la zona peligrosa de rara a ocasional (*parámetro por defecto*).

Ejemplos y consideraciones:

- Ocupación inferior al 10%.
- La mayoría de plantas en continuo tendrán exposición baja o poco frecuente. Esta será la



elección por defecto cuando el incidente evaluado ocurre durante la operación normal de la planta o cuando algo ocurre de repente (fallo aleatorio).

F2 Exposición frecuente o permanente en la zona peligrosa.

Ejemplos y consideraciones:

- Ocupación superior al 10%
- La mayoría de plantas en continuo tendrán que resolver y reparar desperfectos, realizar pruebas y mantenimiento. Esto supondrá que más personas estarán expuestas al peligro.
- El procedimiento correcto antes de realizar un trabajo peligroso es evacuar primero a las personas en las cercanías (p.ej. puesta en marcha de un horno).
- Considerar escenarios específicos a las fases de parada o puesta en marcha de una unidad o un equipo, con ocupación humana casi permanente (p.ej. arranque de un horno)
- Plantas batch o semi-batch que a menudo precisan de supervisión humana casi continua.

#### 7.5.1.1.4. Parámetro de la probabilidad de evitar las consecuencias (P)

Este parámetro solamente aplica a las consecuencias **C2** y es el más subjetivo de todos en el procedimiento de asignación de **RG**. La selección del parámetro **P** dependerá de si es posible que el personal expuesto se dé cuenta o sea avisado del peligro, de si tendría suficiente tiempo para evacuar la zona, o de si podría mediante sus propios medios u otros distintos prevenir las consecuencias en caso de fuga. Este parámetro depende por tanto de la velocidad con que un evento peligroso se desarrolla p. ej. bruscamente, rápidamente o lentamente (durante más de 40 minutos), la facilidad para reconocer el peligro (p.ej. visto inmediatamente, detectado por detectores, alarmas locales, panel, etc.), la posibilidad de evitar el daño (p.ej. rutas de escape accesibles y bien indicadas, escaleras verticales o de caracol), y de la experiencia real en seguridad (p.ej. que los operadores estén al corriente de que pueda ocurrir el incidente).

P1 Evitar el peligro es posible en ciertas situaciones

*(Sólo se podrá seleccionar si está adecuadamente justificado).*

**P2 Evitar el peligro es prácticamente imposible (parámetro por defecto).**

Los equipos de protección individual no están diseñados para garantizar un nivel de seguridad adecuado, aunque conllevan a cierta reducción del daño y no se puede elegir P1 en vez de P2 bajo ese concepto, a no ser que el personal lleve puesto siempre su EPP cuando trabaja en la unidad expuesta al peligro.

#### 7.5.1.1.5. Parámetro de las consecuencias para el medio ambiente (E)

**E0 Incidente sin fuga de producto o con fuga de producto, pero sin consecuencias.**

Descripción orientativa de los daños:

- Sin consecuencias relevantes.
- No es necesario reportar a las Autoridades.

Ejemplos:

- Descarga a antorcha dentro de los límites aceptados.

Fuga en el interior de la refinería que solamente requiere un informe rutinario

E1 Fuga dentro de la refinería con consecuencias mínimas conocidas, aunque suficientemente importantes como para que la Dirección tome medidas

Descripción orientativa de los daños:

- Implica que la Dirección debe informar a las Autoridades Locales Competentes.
- Fuera de la zona de influencia apenas hay impacto relevante.

Ejemplo:

Se necesita uno o más camiones para la limpieza de la fuga/derrame

E2 Fuga con afectación fuera de la refinería, sin efectos negativos conocidos, que causa indignación en la comunidad local y daña la imagen de la empresa.

Descripción orientativa de los daños:

- Incidente que causa indignación a la Comunidad Local o Provincial.
- Daños a especies de interés comercial o recreativo.

Ejemplos:

- Antorcha funcionando durante largos períodos de tiempo con o sin ruido molesto de baja frecuencia o contaminación luminosa del cielo o funcionando repetidamente en un tiempo corto, incluso dentro de la licencia de operación.
- Derrame de hidrocarburo de entre 5 y 50 barriles en aguas superficiales o subterráneas sensibles.
- Derrame de hidrocarburo de entre 50 y 500 barriles en aguas superficiales o subterráneas no sensibles.
- Incumplimiento de los límites del permiso de vertido.

E3 Fuga fuera del establecimiento con efectos negativos conocidos pero reversibles.

**Se espera que los efectos perjudiciales terminen en menos de cinco años.**

Descripción orientativa de los daños:

- Incidente que causa indignación en la comunidad provincial o estatal y que daña la imagen de la corporación a nivel nacional. El incidente viola la legislación boliviana (local, provincial o nacional).
- Desaparición temporal de especies de interés comercial o recreativo.

Ejemplos:

- Derrame de sustancias tóxicas con daños sobre el ecosistema en un tramo de al menos 100 m de un río, si lo hubiera.
- Daño significativo a 1 hectárea de suelo. Por ejemplo, tratamiento de tierra contaminada impuesta por las autoridades por un importe de hasta 10 M de dólares.
- Derrame de hidrocarburo de entre 50 y 5.000 barriles en aguas superficiales o subterráneas sensibles.
- Derrame de hidrocarburo de entre 500 y 50.000 barriles en aguas superficiales o subterráneas no sensibles.

**NOTA:** En el entorno próximo de la RCBA y RSCZ no hay ningún cauce fluvial que pudiera resultar afectado en caso de una fuga fuera del establecimiento

E4 Fuga con afectación fuera del establecimiento con efectos negativos conocidos a **largo plazo**

Descripción orientativa de los daños:

- Si se induce un cambio en el entorno.

- Incidente que causa indignación en la comunidad a nivel nacional y dañará la imagen de la corporación y afectará a la legislación a escala nacional.

Ejemplos:

- Derrame de 5.000 barriles (o más) de hidrocarburo en aguas superficiales o subterráneas vulnerables
- Derrame de 50.000 barriles (o más) de hidrocarburo en aguas superficiales o subterráneas no vulnerables.
- Derrame de sustancias tóxicas con daños ecológicos (reversibles) en el medio acuático, si lo hubiera.
- Contaminación atmosférica aguda afectando a comunidades locales.
- Contaminación masiva de aguas subterráneas. Daño a 1.000 hectáreas de ecosistemas vulnerables, si los hubiera.

**NOTA:** En el entorno existente en ambas refinerías no existen ecosistemas vulnerables ni especies protegidas, por lo que en caso de fuga con afectación fuera del establecimiento no se producirán efectos negativos a largo plazo, es decir, el parámetro E4, no es de aplicación a la RSCZ ni a la RCBA.

#### E5 Fuga con afectación fuera del establecimiento con efectos medioambientales catastróficos

Descripción orientativa de los daños:

- Incidente que causa indignación a nivel internacional y, daña la imagen de la corporación y afecta a la legislación, a escala internacional. Conlleva acciones por parte del gobierno.

Ejemplos de este tipo ocurridos en otras industrias:

- Eventos tipo Seveso.
- Eventos tipo Exxon Valdez.
- Daño irreversible a un acuífero.
- El accidente de la plataforma petrolífera Deep Water Horizon de BP.

**NOTA:** En el entorno existente en ambas refinerías no existen ecosistemas vulnerables ni especies protegidas, por lo que en caso de fuga con afectación fuera del establecimiento no se prevé ningún escenario susceptible de crear una catástrofe medioambiental, es decir, el parámetro E5, no es de aplicación a la RSCZ ni a la RCBA

#### 7.5.1.1.6. Parámetro de las consecuencias para las instalaciones y la pérdida de producción (A)

El parámetro para la protección de las instalaciones y la producción debe incluir todas las pérdidas económicas:

- Costes de demolición (para eliminar equipo dañado).
- Costes de material e instalación del equipo instalado (aproximadamente tres (3) veces el precio del equipo).
- Costes de la interrupción de la producción. Los costes de la interrupción de la producción **NO** son debidos a la pérdida de producción sino al valor del producto que no se ha podido expedir.

P.ej., un incendio en una unidad de nafta causa que la producción de gasolina se pare durante cinco días en la refinería. Sin embargo, la expedición puede continuar desde los tanques de almacenamiento donde existe un stock para siete días. En este caso los costes de la interrupción de la producción son nulos.

Cuando no se dispone de información de los costes de interrupción de la producción, se asume que la pérdida de producción empieza cinco días después de la parada.

A0 Incidente que no causa la interrupción del proceso ni daños importantes en **equipos**: Pérdidas Totales £  $10^5$  \$

A1 Interrupción menor del proceso y/o daño en el equipo:  
 $10^5$  \$ < Pérdidas Totales £  $5 \times 10^5$  \$

A2 Interrupción moderada del proceso o daño en el equipo:  
 $5 \times 10^5$  \$ < Pérdidas Totales £  $5 \times 10^6$  \$

A3 Interrupción severa del proceso o daño en el equipo:  
 $5 \times 10^6$  \$ < Pérdidas Totales £  $5 \times 10^7$  \$

A4 Daños severos en equipos esenciales:  
 $5 \times 10^7$  \$ < Pérdidas Totales £  $5 \times 10^8$  \$.

A5 Daños catastróficos:  
>  $5 \times 10^8$  \$

#### 7.5.1.1.7. Reglas generales para la selección de los parámetros de los gráficos de riesgo

Para aquellos escenarios que requieran una SIF, a partir del estudio HAZOP, se deben identificar y describir en detalle las causas y las consecuencias. Los parámetros de los tres gráficos de riesgos (seguridad de las personas, riesgo medioambiental, riesgos para las instalaciones y la producción) se deben evaluar **sin tener en cuenta la presencia de salvaguardas o capas de protección, incluida la SIF**.

Los parámetros por defecto son **W2**, **F1** y **P2**. Son los valores más asignados en plantas de proceso convencionales y podrán seleccionarse cuando el equipo multidisciplinario no sabe qué parámetros elegir. Sin embargo, es necesario que se discuta entre los miembros del equipo cada parámetro antes de tomar una decisión.

La frecuencia de ocurrencia del evento indeseado (parámetro **W**) es la misma en los tres gráficos. El **Anexo C** recoge datos de frecuencia de ocurrencia de eventos iniciadores típicos. Se recomienda que la selección del parámetro **W** se realice en base a estos valores. Sin embargo, estos valores son genéricos y se deberán revisar teniendo en cuenta la situación particular de cada planta. La selección de otros valores que los indicados en el **Anexo C** deberá detallarse debidamente.

En caso de haber un evento iniciador y un evento condicionante, se deberán multiplicar las frecuencias de ambos para determinar el parámetro **W**.

En caso de haber varios eventos iniciadores o causas que lleven a las mismas consecuencias y que tengan exactamente las mismas capas de protección independientes, se seleccionará la **W** correspondiendo a la suma de las frecuencias de cada una de las causas (puerta OR en un árbol de fallos).

Por ejemplo una muy alta presión en una columna regeneradora de aminas puede ser producida por un fallo eléctrico (**W3**) o por rotura de tubos en el *reboiler* de vapor (**W1**). Las consecuencias son una sobrepresión en el equipo y fuga al exterior de producto inflamable y tóxico. La única capa de protección independiente es una PSV. Dicha PSV permite mitigar las consecuencias en ambos casos. La frecuencia total es por lo tanto **W3**.

En caso de haber varias causas que lleven a la misma consecuencia y no tengan exactamente las mismas capas de protección, se estimarán los parámetros de los tres gráficos de riesgos para cada una de manera siguiente: los valores de los parámetros **W**, **F**, **P** se seleccionarán específicamente para cada causa (ya que cada causa puede tener una frecuencia de ocurrencia distinta, el personal puede estar presente o no y disponer de suficiente tiempo o no para escapar) mientras que los

parámetros **C**, **E** y **A** tendrán el mismo valor para cada causa (normalmente se deben esperar consecuencias iguales en caso de fallar todas las capas de protección). En caso de seleccionar distintos valores de consecuencia para cada causa, se deberán justificar adecuadamente las razones.

Si **W** > 1/año entonces el diseño deberá revisarse para optimizarlo y reducir la frecuencia de ocurrencia **W**. La calibración de los gráficos de riesgo no es válida para **W** > 1 año.

El **RG** será el mayor de los tres obtenidos al aplicar los tres gráficos. En caso de haber varias causas, se seleccionará de esa manera un **RG** para cada causa.

El resultado obtenido con los gráficos de riesgo corresponde a la reducción de riesgo necesaria o **RG** (Risk Gap) para dicho escenario. Se prefiere emplear el término **RG** para evitar confusión con la asignación de SIL de una SIF, que se realiza en una fase posterior. El **RG** define la diferencia (en órdenes de magnitud) entre el riesgo del escenario sin

protección y el riesgo de referencia de YPF Refinación, S.A. Por ejemplo, si se obtiene que el **RG** es igual a 2 esto quiere decir que la reducción de riesgo que se requiere es de al menos 2 órdenes de magnitud (equivalente a un factor de reducción de entre 100 a 1000 en el riesgo).

#### 7.5.1.2. Identificación de las capas de protección y asignación de créditos IPL

Una vez determinado el **RG** se analiza si las capas de protección o salvaguardas cumplen con los requisitos esenciales descritos en la **Sección 7.2** (se evalúa su independencia con el evento iniciador y con la SIF objeto del estudio, y se verifica su eficacia para reducir el riesgo significativamente, etc.). En esta etapa, debe quedar claro que no se debe listar y considerar la SIF objeto del estudio como una capa de protección (se debe suponer que no existe).

A cada capa de protección independiente (IPL) que cumpla con los requisitos esenciales, se le asigna un crédito IPL que corresponde al orden de magnitud de reducción de riesgo que proporciona. Por ejemplo, un crédito IPL = 1 significa que la IPL reduce el riesgo en al menos un orden de magnitud, que es equivalente a un factor de reducción de riesgo (RRF) entre 10 y 100.

En caso de haber varias causas que lleven a la misma consecuencia, y que no tengan las mismas capas de protección, se asignarán los créditos IPL de manera específica para cada causa.

El **Anexo C** recoge algunos valores típicos de créditos IPL y probabilidad de fallo para capas de protección que proceden de bases de datos genéricos. Se recomienda que la asignación de créditos IPL se realice en base a estos valores. No obstante, se deberán revisar teniendo en cuenta la situación particular de cada planta. La selección de otros valores de créditos IPL que los indicados en el **Anexo C** deberá justificarse debidamente (p.ej. uso de datos de fallo de planta, etc.).

El **Anexo B** describe los distintos tipos de capas de protección e indica reglas generales para la consideración o no de cada tipo capa en la reducción del riesgo.

En algunos casos, es posible que dos o más SIF protejan el mismo escenario (aunque no utilicen el mismo elemento detector). En este caso es importante evaluar su independencia y considerar posibles fallos comunes. Adicionalmente, es importante prestar atención a la asignación de SIL de ambas SIF debido a que estarán relacionados entre sí. En la práctica, esto se puede solucionar asignándole a una SIF los créditos IPL equivalentes al SIL que tentativamente se le dará posteriormente para poder determinar el SIL de la otra SIF y así cubrir el **RG**. Cuando se analice la otra SIF, se hará lo mismo pero al revés considerando la primera como una IPL.

Ejemplo: En terminales de almacenamiento de LNG existe el riesgo de enviar LNG "frío" aguas abajo de un vaporizador y provocar fractura frágil debido a falta de agua de mar. Este riesgo puede estar protegido por 2 SIF: la 1ª cerrará las válvulas de entrada y salida de LNG (lado proceso) por bajo caudal de agua de mar y la segunda cerrará las mismas válvulas por detección de baja temperatura en la salida del vaporizador (lado gas).

### 7.5.1.3. Asignación de SIL según los gráficos de riesgo

En definitiva, si la suma de todos los créditos IPL es menor que el **RG** y no hay mejores salvaguardas no-instrumentadas que reduzcan el riesgo, será necesaria una SIF y se deberá determinar el SIL mediante la siguiente fórmula:

$$\text{SIL} = \text{RG} - \sum \text{créditos IPL}$$

En caso de haber varias causas que lleven a las mismas consecuencias, se determinará con la fórmula anterior el SIL correspondiente a cada causa. En caso de haber varias causas que lleven a un mismo nivel SIL, se considerará si procede incrementar el nivel SIL requerido por los gráficos de riesgo (para tener en cuenta el efecto acumulativo de todas las causas) o se realizará un estudio cuantitativo más detallado (ver más adelante).

El significado del SIL se detalla en la **Sección 7.7.1**.

En caso de haber asignado un SIL -, SIL 0 o SIL 1 a una SIF con los gráficos de riesgo, y confirmado la independencia de las capas de protección a las cuales un crédito IPL ha sido asignado, se da por terminado el ejercicio de asignación de SIL y determinado el SIL requerido.

En caso de haber asignado un SIL 2 o SIL 3 a una SIF mediante los gráficos de riesgo, se deberá realizar un estudio más detallado y cuantitativo de los riesgos para confirmar el nivel SIL requerido. En efecto, diseñar y mantener una SIF con SIL 2 o SIL 3 a lo largo de la vida de la planta es caro y todo un desafío y es necesario justificar debidamente la necesidad de un SIL 2 o SIL 3 antes de implementarlo. La realización de un estudio cuantitativo se describe en la **Sección 7.5.2**.

Si el SIL está determinado por las consecuencias sobre las instalaciones y la producción, es decir si el **RG** protección activos > MAX (**RG** protección personal, **RG** protección medioambiental), puede que una solución de ingeniería sea más cara que el problema en sí (y por lo tanto igualmente inaceptable). En este caso se puede realizar un estudio

coste-beneficio (o demostración ALARP) para determinar si la solución es "práctica" desde un punto de vista económico.

Se recomienda de modo opcional realizar tal estudio cuando se ha asignado un SIL 3 únicamente por pérdidas económicas a una SIF. Se considerará tolerable o ALARP la instalación de una SIF de SIL 2 (en vez de SIL 3) siempre que esa alternativa se justifique económicamente.

En YPF Refinación, S.A. no se autoriza asignar un SIL 4 a una SIF. Ver **Sección 7.7.3**

La equivalencia entre los créditos IPL (asignados a las capas de protección independientes de la SIF), el SIL (asignado a la SIF) y los correspondientes factores de reducción del riesgo (RRF), y probabilidad de fallo se muestra en la siguiente tabla para información:

Tabla 1: Relación entre créditos IPL, probabilidad de fallo y RRF			
SIL	Crédito IPL	Probabilidad de fallo en demanda (PFD)	Factor de reducción de riesgo (RRF)
1	1	$10^{-1} > \text{PFD} \geq 10^{-2}$	$10 < \text{RRF} \leq 100$
2	2	$10^{-2} > \text{PFD} \geq 10^{-3}$	$100 < \text{RRF} \leq 1,000$
3	3	$10^{-3} > \text{PFD} \geq 10^{-4}$	$1,000 < \text{RRF} \leq 10,000$
4	4	$10^{-4} > \text{PFD} \geq 10^{-5}$	$10,000 < \text{RRF} \leq 100,000$

### 7.5.2. Segunda etapa: Estudio cuantitativo

Los escenarios protegidos por una SIF que haya recibido una asignación de SIL 2 o SIL 3 durante la primera etapa del proceso de asignación de SIL con gráficos de riesgo (u otros escenarios si se considera necesario en esa misma etapa) requieren un estudio más detallado y cuantitativo del

riesgo para definir de forma más rigurosa la integridad de seguridad requerida (ver IEC 61511-3 §3.8 y PG-1-DGSMS-80 Procedimiento para la realización de Estudios LOPA, el cual describe con mucho mayor detalle la metodología a aplicar para la elaboración del estudio cuantitativo).

## 7.6 REQUISITOS FUNCIONALES ADICIONALES

En este apartado se describen algunos de los requisitos funcionales que formarán parte de la especificación de los requisitos de seguridad, que son necesarios para la fase de diseño del SIS (Fase 4 del ciclo de vida de seguridad, ver Figura 1) y que se pueden definir bien durante la asignación del SIL o bien más adelante

### 7.6.1. Tiempo de seguridad del proceso

El tiempo de seguridad del proceso es el tiempo disponible para realizar la acción requerida. Es decir, es el tiempo que hay entre la señal de desviación en el proceso (p.ej., la variable del proceso se desvía hacia la zona de operación inaceptable) y el momento en que el mismo entra en situación peligrosa si no se ha hecho nada para evitarlo.

**Ejemplo:** Se dispone de un enclavamiento de parada por alta temperatura (280°C). Las consecuencias indeseadas de la alta temperatura no se materializarán hasta que la temperatura llegue a 330°C. A partir de la inercia térmica del proceso, se sabe que tardará aproximadamente 5 minutos en evolucionar desde 280°C hasta 330°C, y por lo tanto, el tiempo de seguridad del proceso es 5 minutos.

Durante la asignación de SIL, es necesario evaluar el tiempo de seguridad del proceso para cada función individual. La experiencia de Procesos y de Operación definirá estos tiempos.

El tiempo de seguridad del proceso se tiene que considerar para establecer el punto de disparo (*trip point*) de un SIS, y su actuación dinámica (tiempo de respuesta).

Del tiempo de seguridad del proceso también dependerá la probabilidad de error humano en la respuesta de un operador reaccionando ante una alarma y realizando la operación requerida, tal y como se explica en la **Sección C del Anexo B**. En dicho Anexo se indica cuando dar crédito a la capa de protección “supervisión e intervención humana” durante la asignación de SIL con los gráficos de riesgo, en función del tiempo de seguridad del proceso.

### 7.6.2. Requisito de estanqueidad (TSO)

Durante la asignación de SIL, se deberán determinar los requisitos de estanqueidad (válvula TSO, configuración con doble bloqueo y venteo 2B&B o clases VI o V) de los elementos finales de las SIF para llevar y mantener el proceso en posición segura cuando se produce la demanda (i.e. cuando se produce el peligro y la demanda de actuación de la SIF).

Las válvulas con requerimiento TSO tienen limitaciones prácticas que pueden imposibilitar su uso en diversas aplicaciones. Son válvulas muy especiales para las cuales existen pocos fabricantes. Muchas veces, se especifica (equivocadamente) TSO cuando en la realidad se instala una válvula con clase VI si la temperatura de operación lo permite o clase V si no (p. ej. corte de vapor de fuel a horno). Para gases tóxicos o inflamables, cuando se especifica

(equivocadamente) una válvula TSO, se prefiere muchas veces un montaje 2B&B. Es conveniente consultar siempre a un experto en operación o instrumentación qué requisito de estanqueidad es el adecuado en cada caso.

### 7.6.3. Modos de operación



Durante la asignación SIL es necesario considerar todos los modos operativos posibles para una SIF (desde puesta en marcha hasta parada). Adicionalmente, se deberá evaluar si es necesario desactivar o bypassar la SIF o incluso cambiar su punto de consigna en función del modo operativo.

En caso de que una SIF no sea necesaria en diferentes modos operativos o secuencias (por ejemplo, en la puesta en marcha de un horno), se establecerá si una anulación de automatismo (*by-pass* de software) o un punto de consigna distinto es necesario para permitir dichas operaciones o secuencias. En este caso, los requisitos funcionales de la anulación de automatismo se documentarán en la especificación de los requisitos de seguridad (SRS)

#### 7.6.4. Justificación de una arquitectura robusta para fallos seguros

Una vez asignados los requerimientos de seguridad (SIL) de una SIF en función de la frecuencia de demanda y las consecuencias del escenario en caso de fallo de la misma, se deberá evaluar el impacto de los fallos seguros (fallos espurios) que tendrán mayor o menor impacto en la pérdida de la producción, o que incluso pueden inducir estrés en varios equipos resultando en un aumento de los requerimientos de mantenimiento. El objetivo de evaluar estos impactos es determinar si la arquitectura robusta para fallos seguros está justificada desde el punto de vista del coste-beneficio.

La evaluación podrá hacerse cualitativamente (p.ej. la arquitectura robusta para fallos seguros quedará justificada si el coste de estos fallos es significativo basándose en estimaciones cualitativas) o cuantitativamente, si se basan en un análisis coste-beneficio (coste del fallo seguros versus coste del diseño robusto a fallo seguro). Se ha incluido un ejemplo de este último caso en la ficha de asignación de SIL incluida en el **Anexo D** considerando un periodo de amortización de 1 año.

### 7.7 IMPLEMENTACIÓN DE UNA SIF

#### 7.7.1. Significado del SIL

El SIL de una SIF es el requisito de integridad de la seguridad de esa función. En función del SIL asignado, el sistema instrumentado de seguridad que realiza la función deberá cumplir con unos requerimientos de mínima tolerancia a fallos (*minimum fault tolerance*) y de fiabilidad para la seguridad. La fiabilidad se expresa como la probabilidad promedio de fallo endemanda ( $PFD_{avg}$ ).

La relación entre el SIL de una SIF, la  $PFD_{avg}$  requerida y la clase TÜV-AK requerida (según Norma VDI/VDE 2180) se indica en la tabla presentada a continuación. La clase TÜV-AK aplica en algunas ocasiones al PLC de seguridad empleado para la implementación de la SIF

Tabla 2: Relación entre SIL, $PFD_{avg}$ y clase TÜV-AK		
SIL	$PFD_{avg}$ requerida en modo 'bajo demanda'	TÜV-AK class
-	Sin requisito de seguridad	-
a	Sin requisito de seguridad especial	1
1	$10^{-1} > PFD \geq 10^{-2}$	2 – 3
2	$10^{-2} > PFD \geq 10^{-3}$	4
3	$10^{-3} > PFD \geq 10^{-4}$	5 – 6
4	$10^{-4} > PFD \geq 10^{-5}$	7
h	No es suficiente una única SIF	8

**SIL** - quiere decir que no hay ningún requisito de seguridad. En la práctica significa que se puede considerar (o no) eliminar la SIF o bien implementar una alarma mediante el BPCS o bien implementar una función de *switch* mediante el BPCS. Sin embargo, no se podrá eliminar una SIF

sin haberlo comunicado y discutido con el equipo ARP y los especialistas correspondientes. Adicionalmente, si se elimina una SIF, será necesario revisar y evaluar el SIL de las otras SIF que contemplen las anteriores como una capa de protección independiente.

**SIL a** quiere decir que no hay un requisito de seguridad especial. En la práctica significa que no se puede eliminar la SIF, pero que se puede considerar (o no) implementarla mediante el BPCS y los elementos sensores y finales del lazo de control como un *switch* o como una alarma.

**SIL 1, SIL 2 y SIL 3** son los niveles para los cuales se deberán cumplir los requisitos definidos en la norma IEC 61511 durante todo el ciclo de vida de seguridad. Para las SIF asignadas un SIL 1, SIL 2 o SIL 3, se debería tratar, en la medida de lo posible, de utilizar elementos sensores y finales independientes de los del control. En caso contrario sería necesario realizar un análisis adicional de los fallos de causa común. Ese punto es especialmente crítico cuando durante la asignación de SIL, se ha dado crédito al BPCS como capa de protección independiente o cuando un fallo del BPCS es una causa de la demanda.

Para **SIL4**, ver **Sección 7.7.3**.

Un **SIL h** quiere decir que el riesgo es intolerable y que un único dispositivo de protección instrumentado no es suficiente, y por tanto, es necesario rediseñar el proceso. En la práctica, el tratamiento de un SIL h es similar a un SIL 4.

### 7.7.2. El uso de múltiples SIF para cubrir SIL altos

Cuando el nivel SIL asignado es alto (p.ej. SIL 3), se debe tratar de implementar capas de protección de distintas tecnologías (principio de diversidad) o cambiar el diseño en vez de implementar varias SIF independientes de nivel SIL menor.

En el caso extremo de que haya que montar más de una SIF para prevenir un mismo riesgo, será necesario realizar una evaluación de los fallos de causa común. Ver IEC 61511-1 §9.2.4 nota 4 y §9.5 así como IEC 61511-2 §9.2.4 y §9.5.

### 7.7.3. SIL 4

Implementar y sobre todo mantener un SIS con un SIL 4 es todo un desafío. Se puede conseguir un diseño de un SIS que satisfaga un SIL 4 utilizando plataformas redundantes, aunque la gestión de este SIS durante su ciclo de vida sería un proceso arduo. Este nivel de desempeño requiere un sistema de gestión muy riguroso y amplio para minimizar errores sistemáticos en todas las fases del ciclo de vida, así como un personal altamente cualificado. Además, supone un coste operativo muy elevado.

En YPFB Refinación, S.A. se ha decidido no autorizar una SIF con un SIL 4. Siempre será necesario recurrir a modificaciones en el diseño o a la utilización de salvaguardas de otro tipo (p.ej. de tipo mecánico) junto con la SIF, para reducir su nivel SIL requerido.

## 7.8 INFORME FINAL

Los resultados de la asignación SIL deberán recogerse formalmente en un informe. Este informe contendrá como mínimo la siguiente información:

- Alcance y objetivos del estudio SIL
- Descripción de la metodología o referencias a la misma
- Detalles de las sesiones (fechas, lugar, etc.)
- Datos sobre los participantes (nombre, empresa, cargo y disciplina)
- Referencias a la documentación de soporte, incluyendo la revisión (ver **Sección 7.2.4**)
- Hipótesis consideradas durante el estudio, incluyendo: Datos de pérdidas de beneficios debido a la parada de cada unidad y datos de plantilla y ubicación de personal de operación

y mantenimiento.

- Lista de SIF con sus SIL asignados
- Lista de SIF que requieran análisis cuantitativos adicionales
- Lista de SIF que requieran estudio coste beneficio adicional
- Lista de recomendaciones
- Para cada SIF, una ficha de asignación de SIL (conforme Registro RG-171-PG-1-DGSMS-81) y replicando cada hoja Excel por cada SIF

Además, se deberá generar una ficha de seguimiento para cada recomendación conforme al registro RG-136-PG-1-DGSMS-86 Hoja de seguimiento de recomendaciones (Ver PG-1-DGSMS-86 procedimiento general para la realización de estudios de riesgo). Se deberá realizar un seguimiento de las recomendaciones hasta su resolución. Pero estas recomendaciones ya tendrán su ficha de seguimiento que se elaboró al momento de cerrar el ARP.

En el Registro RG-106 PG-1-DGSMS-81 se incluye el formato de ficha recomendado para la asignación de SIL (al estar vinculado con el RG 171-PG-1-DGSMS-81 debe revisarse cada hoja Excel). El **Anexo D** muestra un ejemplo de cumplimentación de dicha ficha. Todos los supuestos realizados para cada escenario durante la asignación deberán quedar perfectamente documentados en las fichas de asignación de SIL.

En caso de ser necesarios estudios adicionales para la determinación del SIL requerido (p.ej. estudio cuantitativo, LOPA, demostración ALARP, coste-beneficio), la ficha de asignación de SIL deberá ser actualizada una vez terminados dichos estudios y fijado el SIL requerido.

Para todas las SIF que tengan un requerimiento SIL ( $SIL \geq 1$ ), la ficha de asignación de SIL llegará a formar parte de la especificación de requisitos de seguridad SRS.

## ANEXOS

NRO	ANEXO	TITULO DEL ANEXO
1	ANEXO A	<a href="#">ANEXO A FLUJO ASIGNACION SIL.DOCX</a>
2	ANEXO B	<a href="#">ANEXO B DESCRIPCIÓN DE IPL.DOCX</a>
3	ANEXO C	<a href="#">ANEXO C TASA DE FALLO TÍPICAS Y CRÉDITOS IPL.DOCX</a>
4	ANEXO D	<a href="#">ANEXO D FICHA DE ASIGNACION DE SIL PARA SIF MEDIANTE GRAFICO DE RIESGOS.DOCX</a>
5	ANEXO E	<a href="#">ANEXO E GRAFICO DE RIESGOS.DOCX</a>

## REGISTROS

NRO	REGISTRO	TITULO DEL REGISTRO
1	RG-106 A PG-1-DGSMS-81 Y RG-171 A PG-1-DGSMS-81	<a href="#">RESUMEN DE LOS NIVELES DE INTEGRIDAD DE SEGURIDAD (SIL) OBTENIDOS PARA CADA UNA DE LAS SIF ANALIZADAS // FICHA DE ASIGNACION DE SIL</a>

## REGISTROS COMPLEMENTARIOS

NRO	REGISTRO	TITULO DEL REGISTRO	PROCEDIMIENTO
1	RG-136 B PG	<a href="#">HOJA DE SEGUIMIENTO DE RECOMENDACIONES</a>	PG-1-DGSMS-86: PROCEDIMIENTO GENERAL PARA LA REALIZACIÓN DE ESTUDIOS DE RIESGO

## SUMARIO DE REVISIONES

REVISION	FECHA	DESCRIPCION
A	06/12/2021	Emisión original
B	06/10/2022	Se actualizó el Procedimiento con las siglas de DGSMS, los procedimientos integrados de <a href="#">PG-1-DGSMS-86</a> PROCEDIMIENTO GENERAL PARA LA REALIZACIÓN DE ESTUDIOS DE RIESGO y la enumeración de los Registros.

## LISTA DE DISTRIBUCION

DAL/PTO, DAL/SAL, DGSMS/MARSE, DGSMS/SSTLO, DGSMS/SSTSC, DTH/COBE, DTH/GETH, DTI/DES, DTI/INFRA, GAF/CONT, GAF/PRTE, GCO/COBI, GCO/COSE, GCO/GPYA, GDV/LUPE, GDV/OPDI, GDV/SERV, GDV/VENT, GGL, GGL/CEM, GGL/DAI, GGL/DAL, GGL/DGSMS, GGL/DTH, GGL/DTI, GGL/GAF, GGL/GCO, GGL/GDV, GGL/GPL, GGL/USP, GGL/UTR, GPL/DDN, GPL/PLES, GPL/PPRT, DGSMS/SSTCB, DTH/UTH, GAF/ADMC, GGL/GRCBA,

GRCBA/CAR, GRCBA/INSP, GRCBA/LAB, GRCBA/LUB, GRCBA/LUB/LUT, GRCBA/SET, ING, MAN, MAN/MEC, MAN/MEI, GGL/GRSCZ, GRSCZ/CAR, GRSCZ/ING, GRSCZ/MAN, GRSCZ/MAN/MEC, GRSCZ/MAN/MEI, GRSCZ/SET, INSP, LAB

#### **FECHA DE ANALISIS CRITICO**

La próxima fecha de análisis crítico es **28/09/2024**