RISKNOWLOGY®

Conceptos Básicos de la Seguridad Funcional de Procesos

Switzerland

Argentina Colombia

France riskfree@risknowlogy.com Germany

India Netherlands

United Arab Emirates United Kingdom

Mucho gusto…

- Somos Risknowlogy, una empresa que opera a nivel internacional ofreciendo servicios de certificación, asesoramiento, auditoría y entrenamiento en los campos de Gestión de Riesgos, Confiabilidad y Seguridad
- Soy Oscar Bollmann, Ingeniero Electrónico y especialista en Seguridad Funcional (Certificado por TÜV-SUD).
- Mi correo electrónico es:
  - oscarbollmann@risknowlogy.com

Durante el entrenamiento…

- Por favor ten en cuenta lo siguiente
  - En caso de emergencia, las salidas son…
  - Siéntete libre de hacer preguntas en todo momento
  - Siéntete libre de contestar su celular
    - Pero por favor ponlo en modo “vibrar” y sal de la sala para conversar

Contenido …

- Conceptos básicos: seguridad, peligro, riesgo, reducción del riesgo.
- Identificación de peligros, evaluación del riesgo.
- Técnicas cualitativas y cuantitativas para análisis de riesgos.
- Reducción del riesgo - capas de protección.
- Funciones de seguridad.
- Funciones de los Sistemas de Control y de Seguridad. Concepto SIL.
- Normas que la regulan.
- Fallas en las funciones de seguridad.
- Seguridad Funcional en procesos. Ciclo de Vida de la Seguridad Funcional.

Conceptos Básicos

¿Por qué falló la seguridad?

¿Por qué falló la seguridad?

¿Por qué falló la seguridad?

¿Por qué falló la seguridad?

Identificación de Peligros y Evaluación del Riesgo

Pero antes de tomar una decisión...

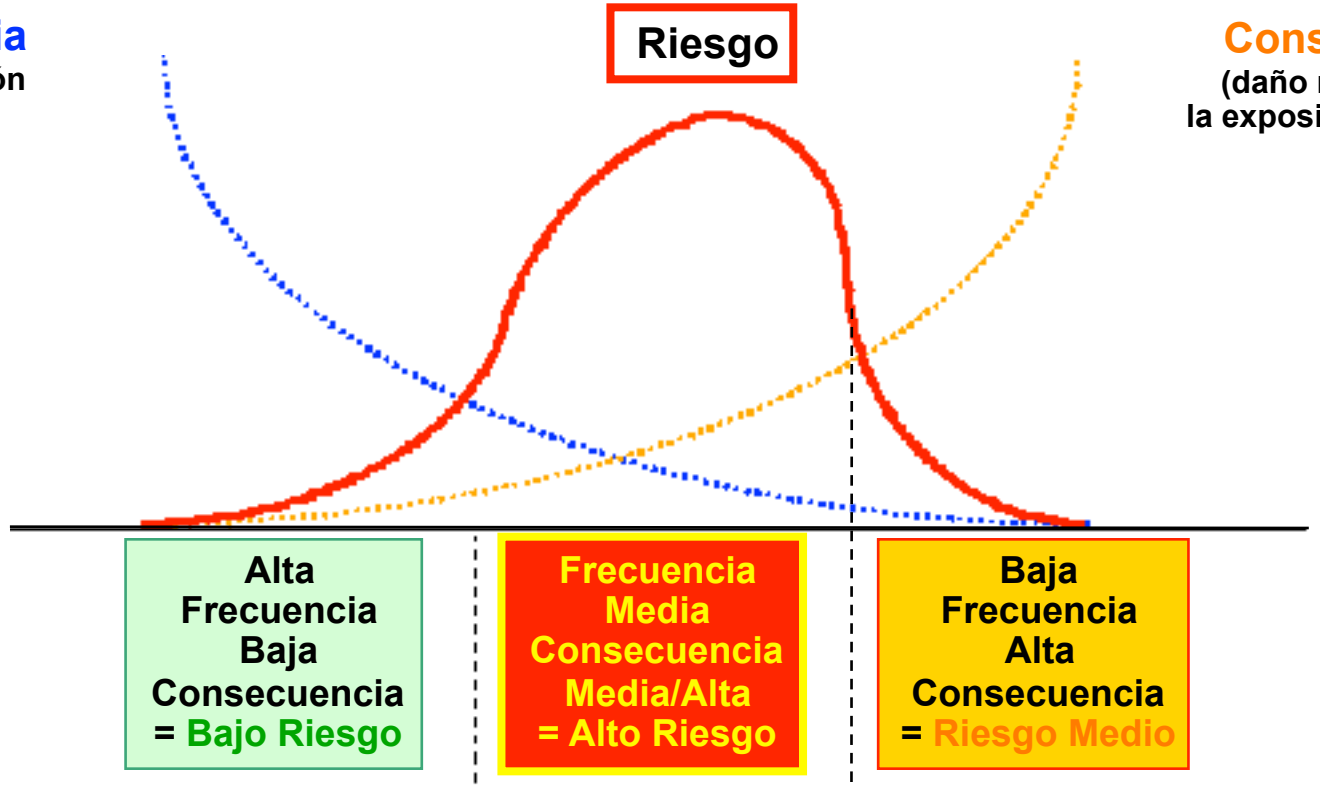
- Tenemos que conocer cuáles son los peligros
  - Peligro: fuente potencial de daño (IEC 61508-4/2000)
    - Peligro es lo podría hacernos perder
    - Daño es eso que podríamos llegar a perder
- Y también cuáles son los riesgos
  - Riesgo: combinación entre la probabilidad de ocurrencia de un daño y la severidad del mismo. (ISO/IEC Guía 51/1997)
    - Esto es, en qué medida es posible que perdamos

El peligro no siempre es evidente…

Mismos peligros, riesgos diferentes

El riesgo puede ser calculado

Frecuencia
(de exposición al Peligro)

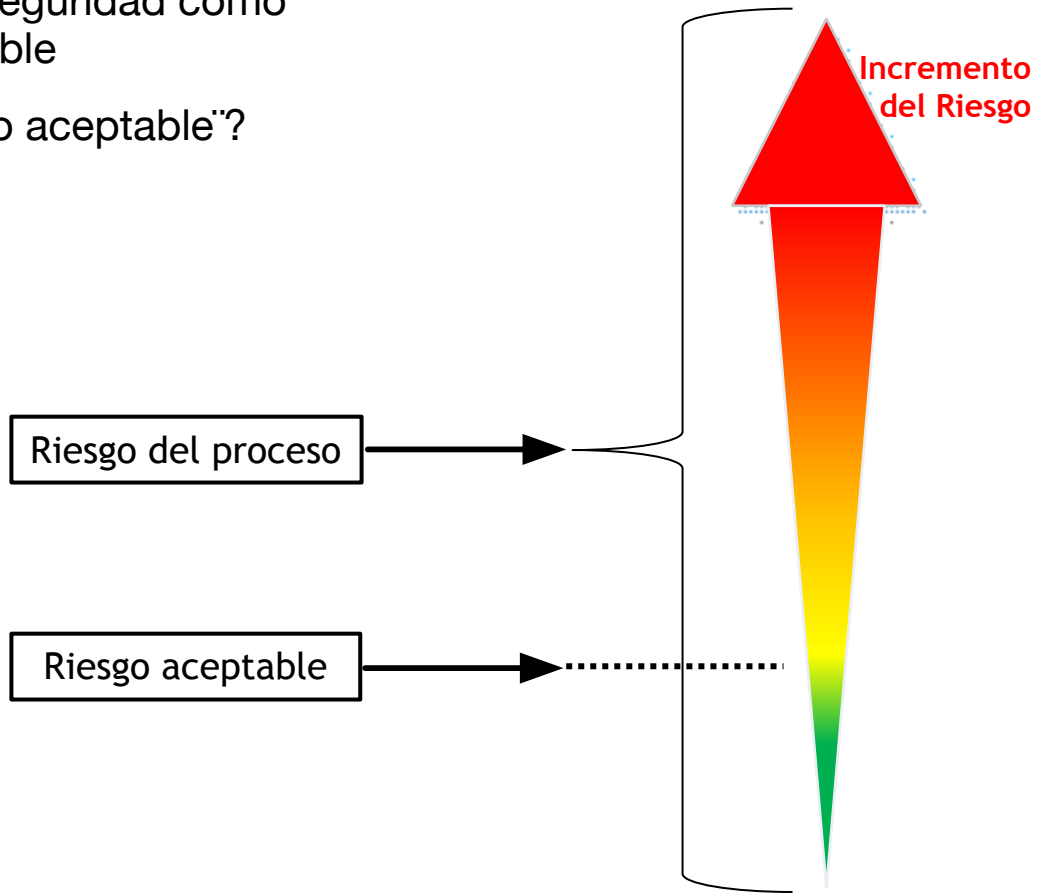


Consecuencia
(daño resultante de la exposición al Peligro)

Riesgo = Frecuencia x Consecuencia

¿Que es seguridad?

- La Guia 51 ISO/IEC define la seguridad como la ausencia de riesgo inaceptable
  - Existe entonces un ¨riesgo aceptable¨?

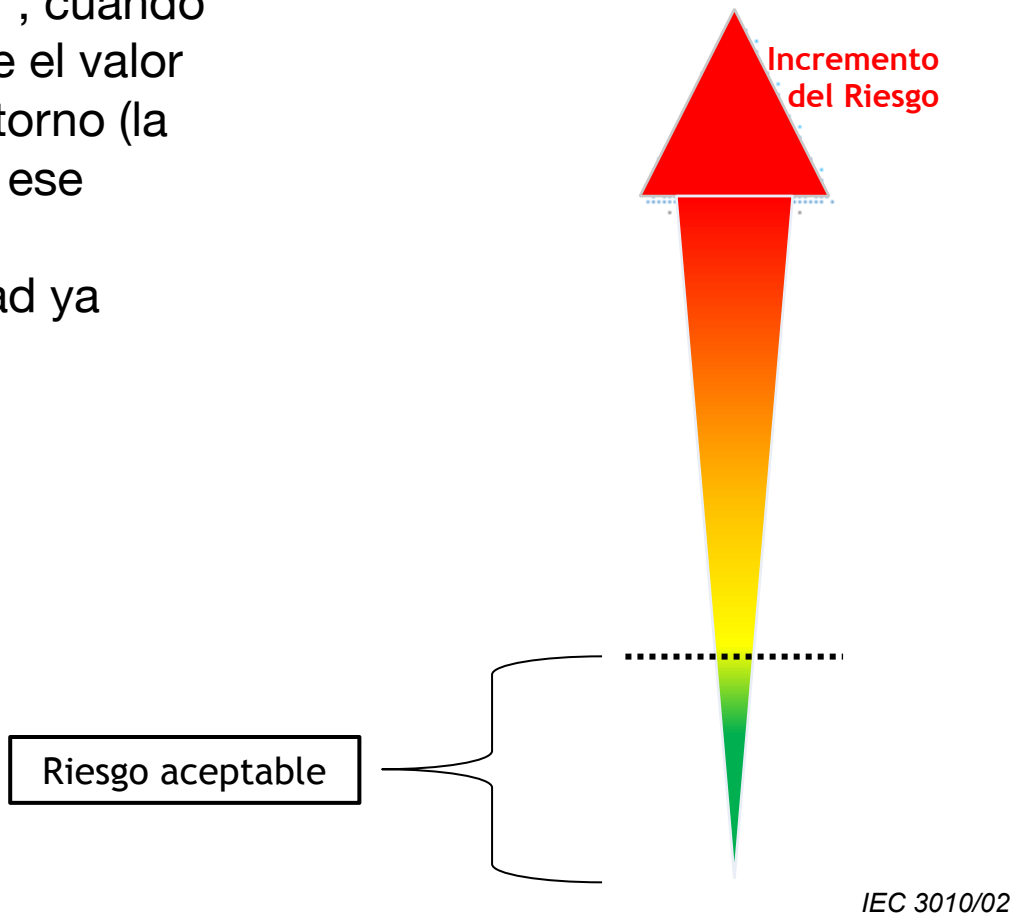


IEC 3010/02

Riesgo aceptable

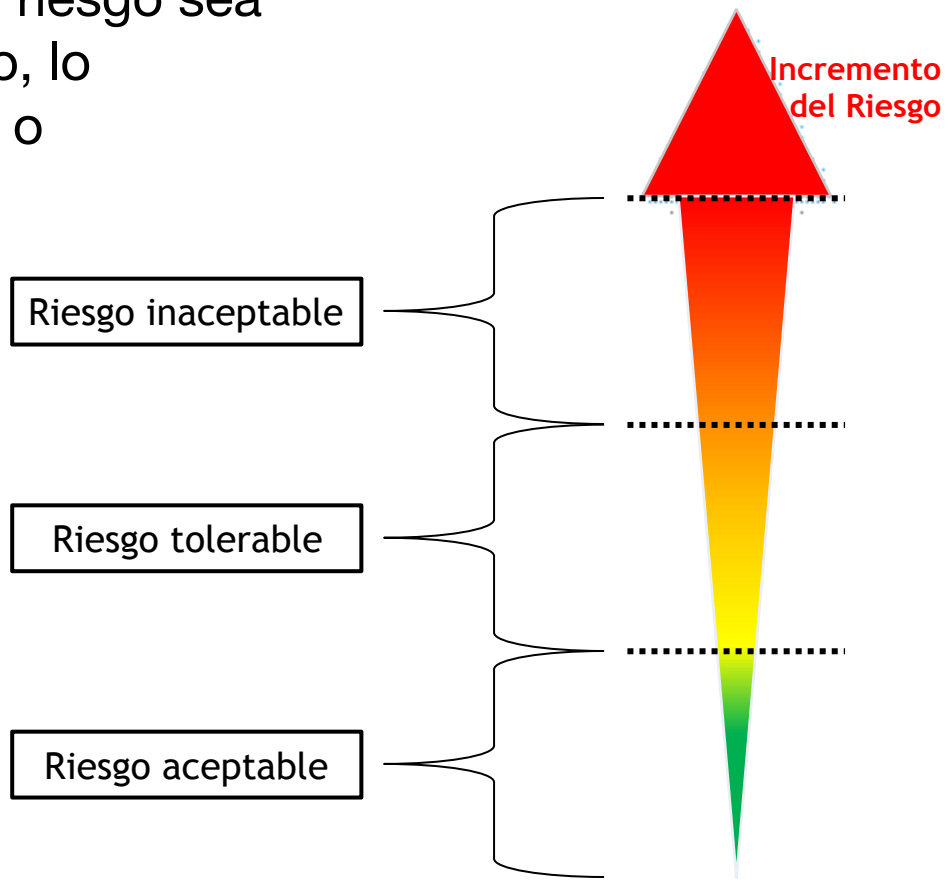
Llamaremos al riesgo “aceptable”, cuando su valor calculado sea menor que el valor naturalmente aceptado por el entorno (la empresa, la sociedad, etc.), para ese escenario

- En ese caso, la seguridad ya existe



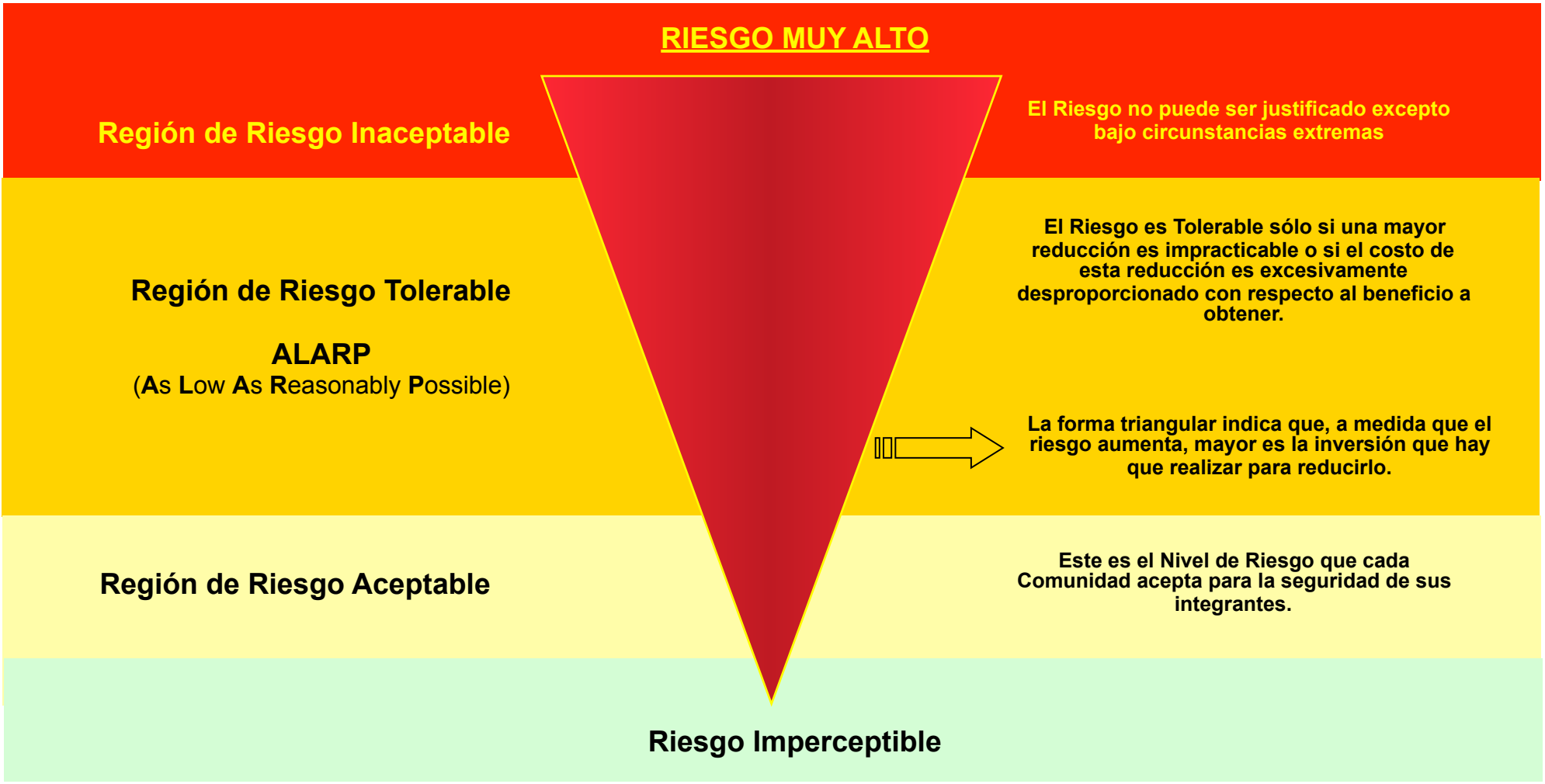
Riesgo tolerable e inaceptable

Cuando el valor calculado del riesgo sea mayor que ese valor aceptado, lo llamaremos riesgo “tolerable” o “inaceptable”, según el caso.

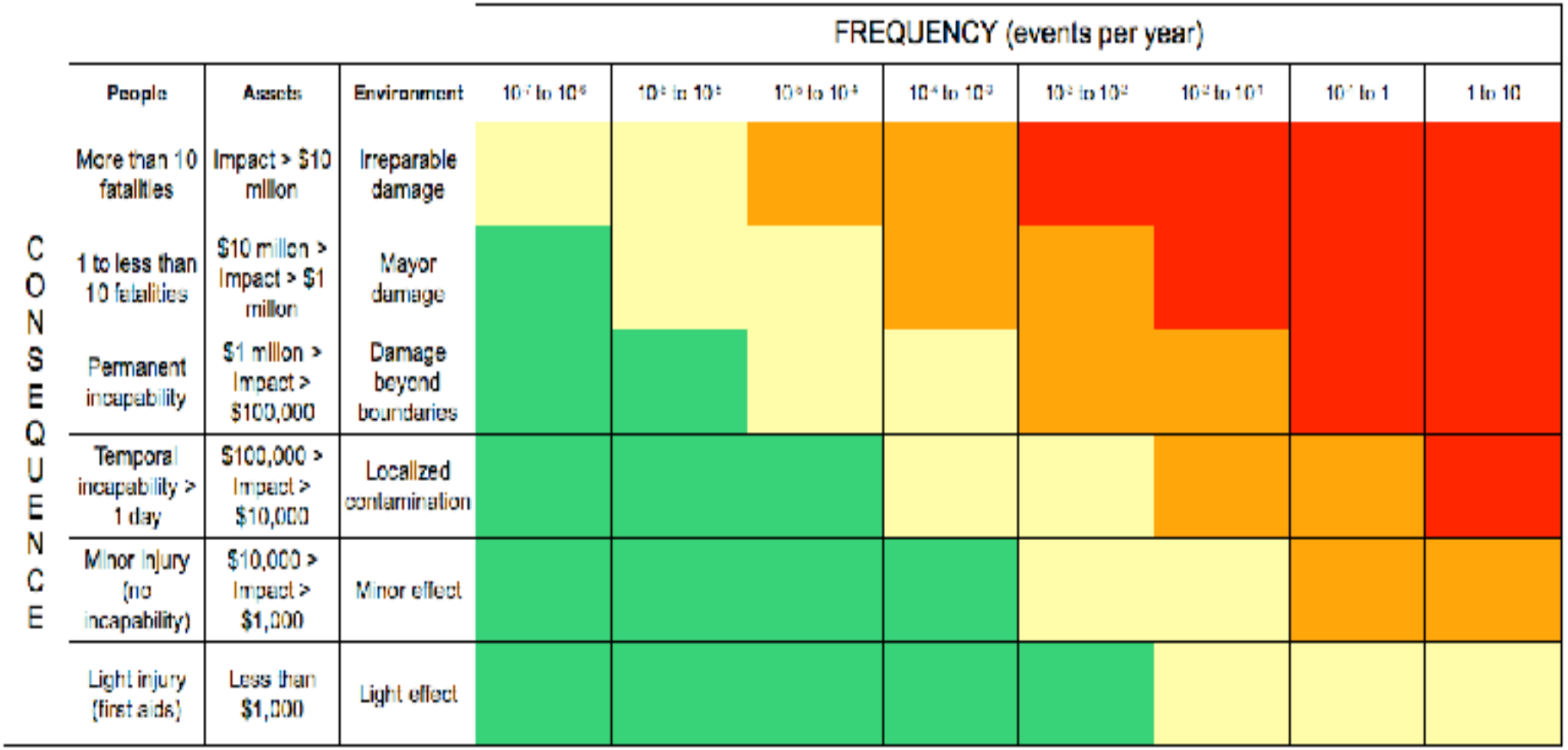


IEC 3010/02

El concepto ALARP



Matriz de Riesgo



Técnicas de Análisis del Riesgo

Risk Assessment

Análisis de Peligros
y Riesgos

- Identificación de Peligros
(FMEA, FTA, HAZID, HAZOP)
- Cálculo de Riesgos
(Uso de Matrices de Riesgo)

Risk Assessment

Gestión del Riesgo:

1) Identificar los peligros / eventos peligrosos
2) Analizar los Peligros / eventos peligrosos = Determinar en nivel de Riesgo
3) Reducir el Riesgo donde sea necesario.

Tres categorías de técnicas:

1) Cualitativa: todo expresado en palabras,
2) Cuantitativa: todo expresado en números,
3) Semi-cuantitativa: una mezcla de palabras y números.

¿Quién realiza el Risk Assessment?

- El Risk Assessment DEBE ser realizado por un Equipo Profesional Multidisciplinario
  - Permite contar con experiencia técnica diversa
  - Permite una mejor percepción y análisis
  - Genera un efecto sinérgico

¿Quiénes deben formar parte del Equipo?

- Líder del grupo (y secretario técnico)
- Grupo de análisis
  - Responsable de Higiene, Seguridad y M. A. +
  - Ingeniero/s de Proyecto o Diseño +
  - Ingeniero/s de Proceso, Químico, Mecánico, etc.+
  - Responsable/s de Puesta en Marcha +
  - Responsable/s de Mantenimiento +
  - Responsable/s de Operaciones +
- Auxiliares
  - Consultores específicos
  - Proveedores de equipamiento
  - Contratistas

Análisis de Peligros y Riesgos

- Existen diferentes metodologías, generalmente relacionadas con el tipo de proceso y/o industria de la que se trate
- Las más utilizadas son: WHAT-IF, FMEA, FTA, HAZID, HAZOP
- Todas ellas permiten:
  - Descubrir dónde están los peligros
  - Evaluar la probabilidad de que se produzcan eventos peligrosos
  - Evaluar las eventuales consecuencias
  - Calcular el riesgo inicial y determinar la reducción de riesgo necesaria (usando, por ejemplo, una Matriz de Riesgos)
  - Elegir salvaguardas
  - Determinar acciones a seguir

Análisis de Peligros y Riesgos

- Todas las metodologías requieren información:
  - Del ambiente físico, incluyendo su vecindad
  - Del equipamiento bajo control
  - Del sistema básico de control de procesos (BPCS) y sus funciones
  - De los peligros propios de las sustancias del proceso (toxicidad, condiciones de explosividad, corrosividad, reactividad, inflamabilidad, etc).
  - De la normativa de de aplicación (leyes, estándares, guías, etc.)

Análisis de Peligros y Riesgos

- FMEA
  - Identifica peligros relacionados con fallas del equipamiento (sólo para fallas simples)
- FTA
  - Identifica peligros relacionados con fallas del equipamiento (fallas múltiples en el equipamiento o combinación de fallas de distintos equipamientos)
- HAZID
  - Identifica peligros relacionados con el ambiente
- HAZOP
  - Identifica peligros relacionados con el proceso y su operación
- Matrices y Gráficos de Riesgo
  - Permiten calcular la reducción de riesgo necesaria para conseguir niveles de riesgo aceptables y, eventualmente, tolerables

WHAT IF como Técnica de Identificación

- Es común hallar que las empresas usen WHAT-IF como técnica de identificación de peligros
  - Es simple de implementar
  - Permite evaluar escenarios de todo tipo
  - Permite elegir algunas salvaguardas
- Sin embargo, su uso encierra un riesgo que puede ser grande
  - Al no ser una técnica sistemática, el grupo puede “olvidar” hacer una pregunta clave para la seguridad del proceso

FMEA – Análisis de Modos de Fallas y sus Efectos

- A nivel del equipamiento
  - Es un método de análisis diseñado para descubrir los efectos que pueden producir, individualmente, cada una de las fallas de cada uno de sus componentes
  - Permite determinar cuáles de esos efectos podrán ser peligrosos durante la ejecución de la función para la cual el equipamiento fuera diseñado
  - Para la realización del estudio se requiere tener conocimientos específicos (mecánica, neumática, hidráulica, electricidad, electrónica)
    - Suele ser realizado por empresas dedicadas a estudios de confiabilidad

FTA – Análisis de Árbol de Fallas

- A nivel del equipamiento
  - Es un método de análisis diseñado para descubrir los efectos de la combinación de las diferentes fallas de sus componentes
  - Permite determinar cuáles de esas combinaciones podrán producir efectos peligrosos durante la ejecución de la función para la cual el equipamiento fuera diseñado
  - Para la realización del estudio se requiere tener conocimientos específicos (mecánica, neumática, hidráulica, electricidad, electrónica)
    - Suele ser realizado por empresas dedicadas a estudios de confiabilidad

HAZID

- Se la utiliza para descubrir los peligros internos (por ejemplo, sustancias peligrosas) y externos (por ejemplo, la caída de rayos) a los que puede estar sujeta una determinada instalación, en un determinado lugar
- Utiliza WHAT-IF y “Palabras Clave” (predefinidas)
  - ¿Qué pasa si “cae un rayo”?
  - ¿Qué pasa si “falta la energía eléctrica”?
  - ¿Qué pasa si “existe una atmósfera explosiva”?
  - etc.
- Permite determinar el uso de algunas salvaguardas (protección contra descargas eléctricas, fuentes auxiliares de alimentación, equipamiento “a prueba de explosión”, etc.)

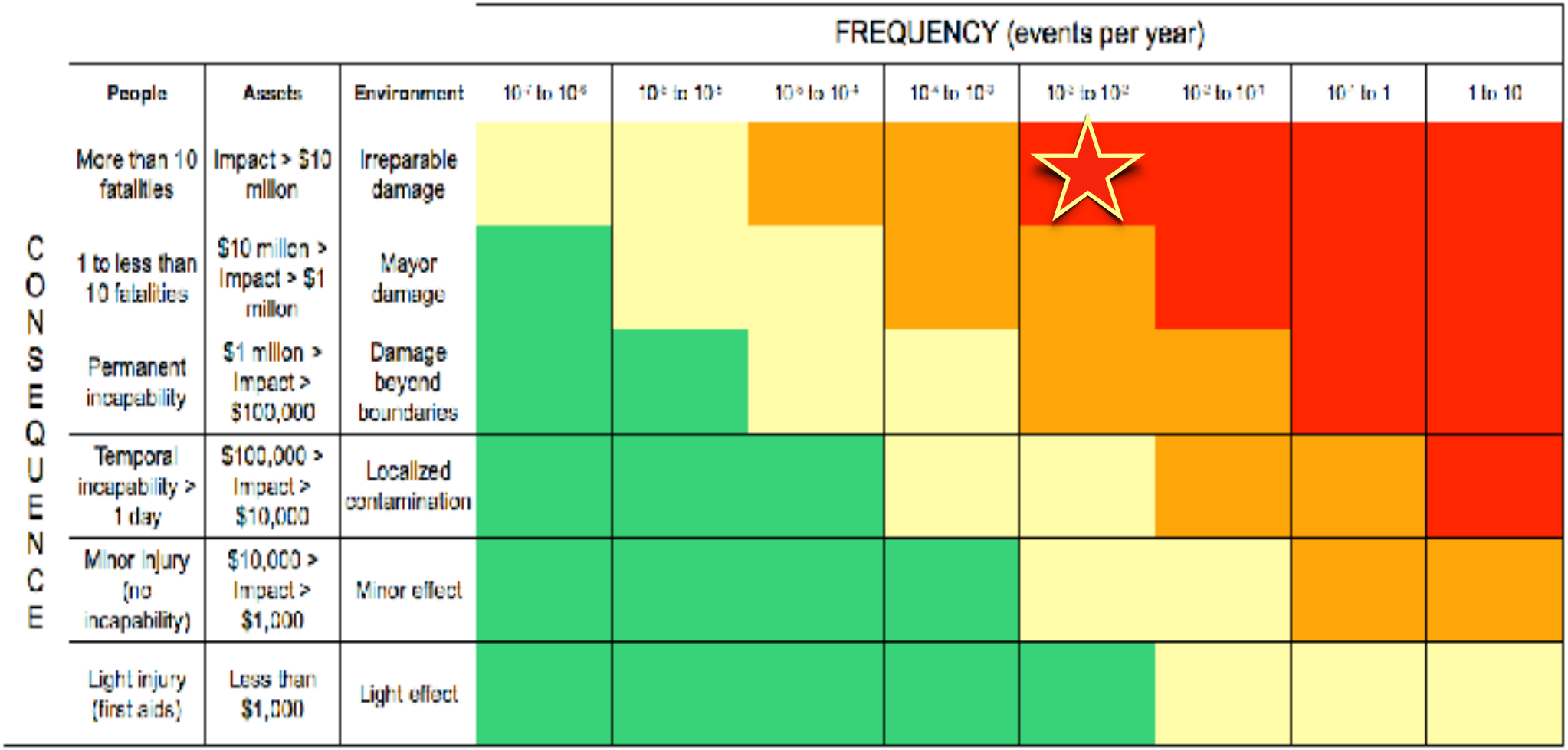
HAZOP – Análisis de peligros y operabilidad

- Se lo utiliza para:
  - Descubrir los peligros inherentes a las desviaciones, de las variables del proceso (presión, temperatura, nivel, etc.), de sus valores normales de operación (o “intención de diseño”).
    - Incluye el análisis de los efectos de acciones humanas equivocadas durante el proceso
    - Utiliza palabras clave (“guide words”)
  - Identificar los eventos peligrosos que pueden producirse para cada desviación
  - Identificar y analizar las posibles consecuencias
  - Elegir salvaguardas (lazos de control y de seguridad, procedimientos, dispositivos de seguridad, etc.)

Cálculo del Riesgo

- Después de la identificación de peligros, el paso que sigue es su análisis pues:
  - A menudo, lo que se debe hacer una vez identificado el peligro resulta claro
  - Para algunos peligros no es claro cuáles son realmente sus consecuencias y su probabilidad
- El análisis de los peligros, al permitir establecer su frecuencia y nivel de eventuales daños, ayuda a entender cuál es la medida menos costosa a tomar para protegerse del peligro.
  - De esta forma de calculan los Riesgos de cada escenario
  - Una de las herramientas más comunes es la Matriz de Riesgos

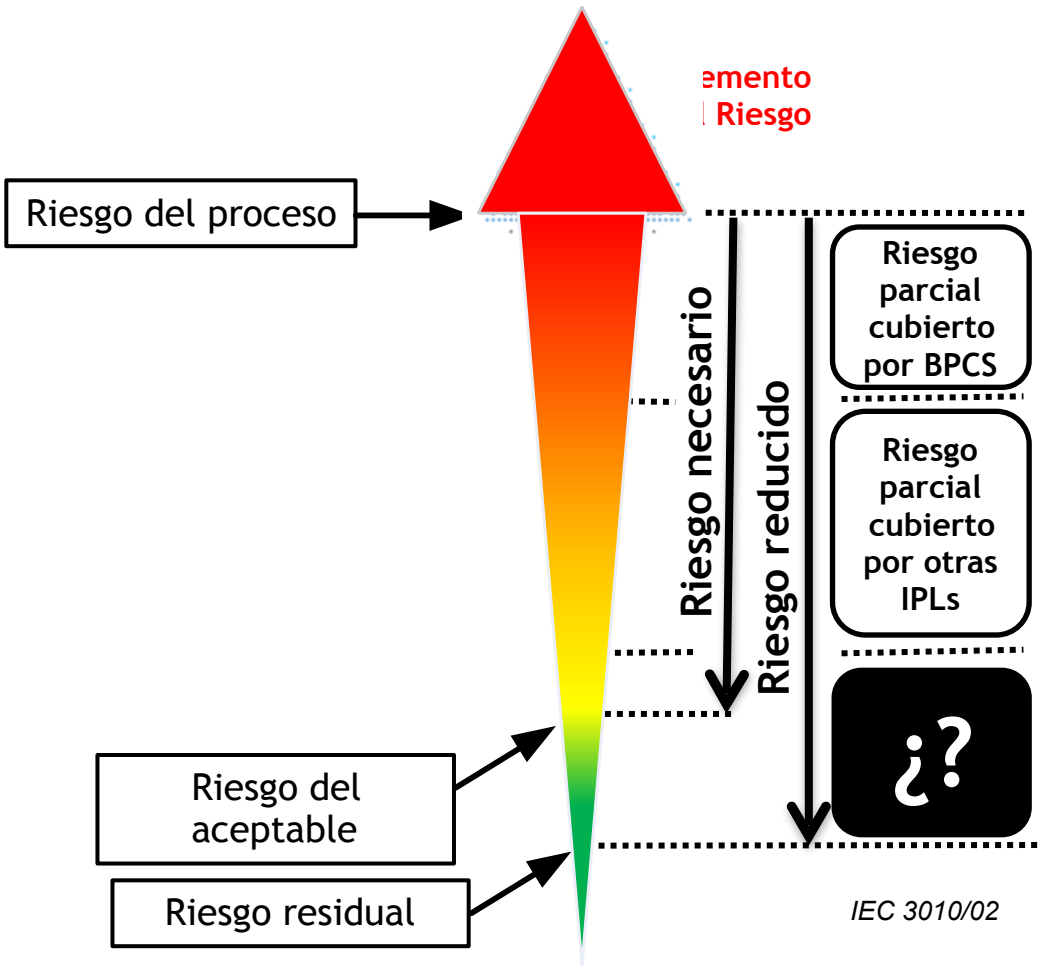
Reducción del riesgo



Reducción del Riesgo

El riesgo puede ser reducido

- En ese caso, la seguridad existirá sólo cuando la reducción de riesgo pueda ser garantizada
- Cuando no podamos llegar al riesgo aceptable podremos conformarnos con estar en riesgo tolerable, pero en éste la seguridad no estará totalmente garantizada (no estaremos tan seguros)

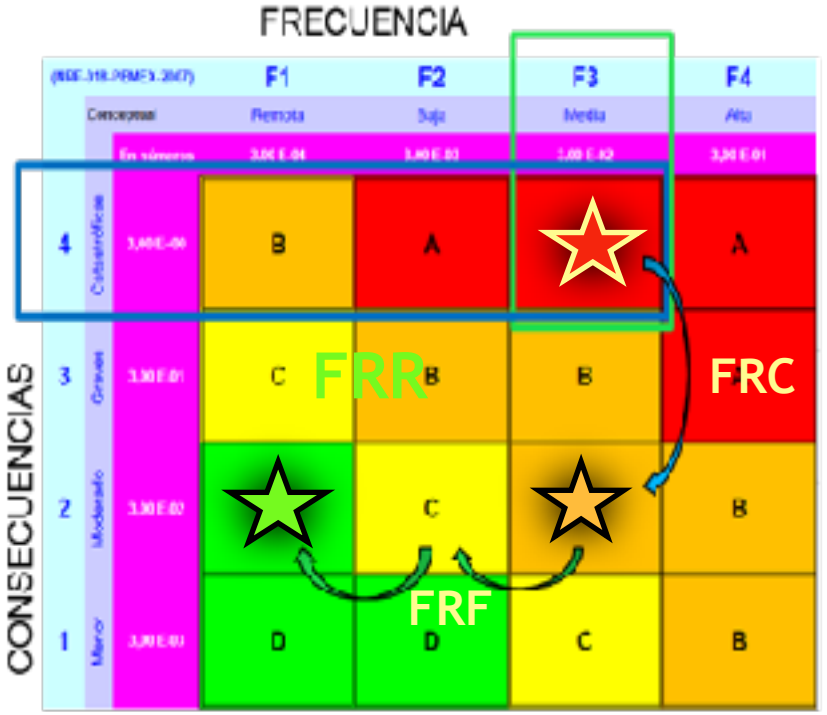


El riesgo puede ser reducido

- Si se divide el valor calculado para el Riesgo por un factor que lo hace menor, a este factor se lo llama “factor de reducción de riesgo” (FRR)
  - FRR = Riesgo Inicial / Riesgo Final
- El FRR se expresa como la “cantidad de veces” en que reduce el riesgo
  - Por ejemplo, un FRR = 100 quiere decir que reduce el riesgo 100 veces
- El FRR puede usarse para reducir la frecuencia (FRF), la consecuencia (FRC) o ambas
  - FRR = FRF * FRC
  - FRR = (Frec. Inicial / Frec. Reducida) * (Consec. Inicial / Consec. Reducida)

Reducción del Riesgo

ANALISIS de SEVERIDAD y FRECUENCIA: → **RIESGO**



1. ¿Tenemos capas de protección que reduzcan el **RIESGO a un valor ACEPTABLE**?
2. Por ejemplo, tenemos válvulas de alivio en la descarga del sistema de impulsión a un valor de presión inferior al de la MAOP del ducto.
3. ¿Esta capa de protección (válvula de alivio), se considera suficiente para bajar el RIESGO a un valor ACEPTABLE ?

SI → **FIN ANALISIS**

NO → **SE DEFINE UNA SIF**

Risk Assessment

Reducción de Riesgos

- Métodos simplificados (Risk Graph, LOPA)
- Métodos Cuantitativos (ETA, FTA)

Capas Independientes de Protección (IPLs)

- Una “capa independiente de protección” (IPL, del inglés “Independent Protection Layer”) es un “medio independiente para reducir el riesgo”.
- Cada una de las IPLs debe ser:
  - **Especifica** (previene o mitiga un evento peligroso determinado)
  - **Independiente** (no se ve influenciada por la falla de ninguna otra IPL)
  - **Confiable** (su confiabilidad está determinada cuantitativamente por su PF)
  - **Auditable** (está sujeta a auditorías periódicas de su función protectora)
- Las IPLs pueden ser:
  - Protecciones mecánicas
  - Alarmas con acción correctiva del operador
  - Funciones de control
  - Funciones de seguridad

IPLs en la industria de Procesos

Las Funciones de Control y de Seguridad

- Los sistemas de control y de seguridad desarrollan funciones
  - Se las llama funciones porque
    - DETECTAN un EVENTO
    - ACTÚAN para evitar una CONSECUENCIA
- Estas funciones podrán ser consideradas IPL (ver características de una IPL)
- Para un escenario de riesgo se podrán usar una o varias funciones como IPL
  - Se podrán usar varias funciones si éstas son ejecutadas en sistemas diferentes
    - BPCS + SIS de prevención + SIS de mitigación
  - No se podrá usar más de una función de un sistema para un mismo escenario

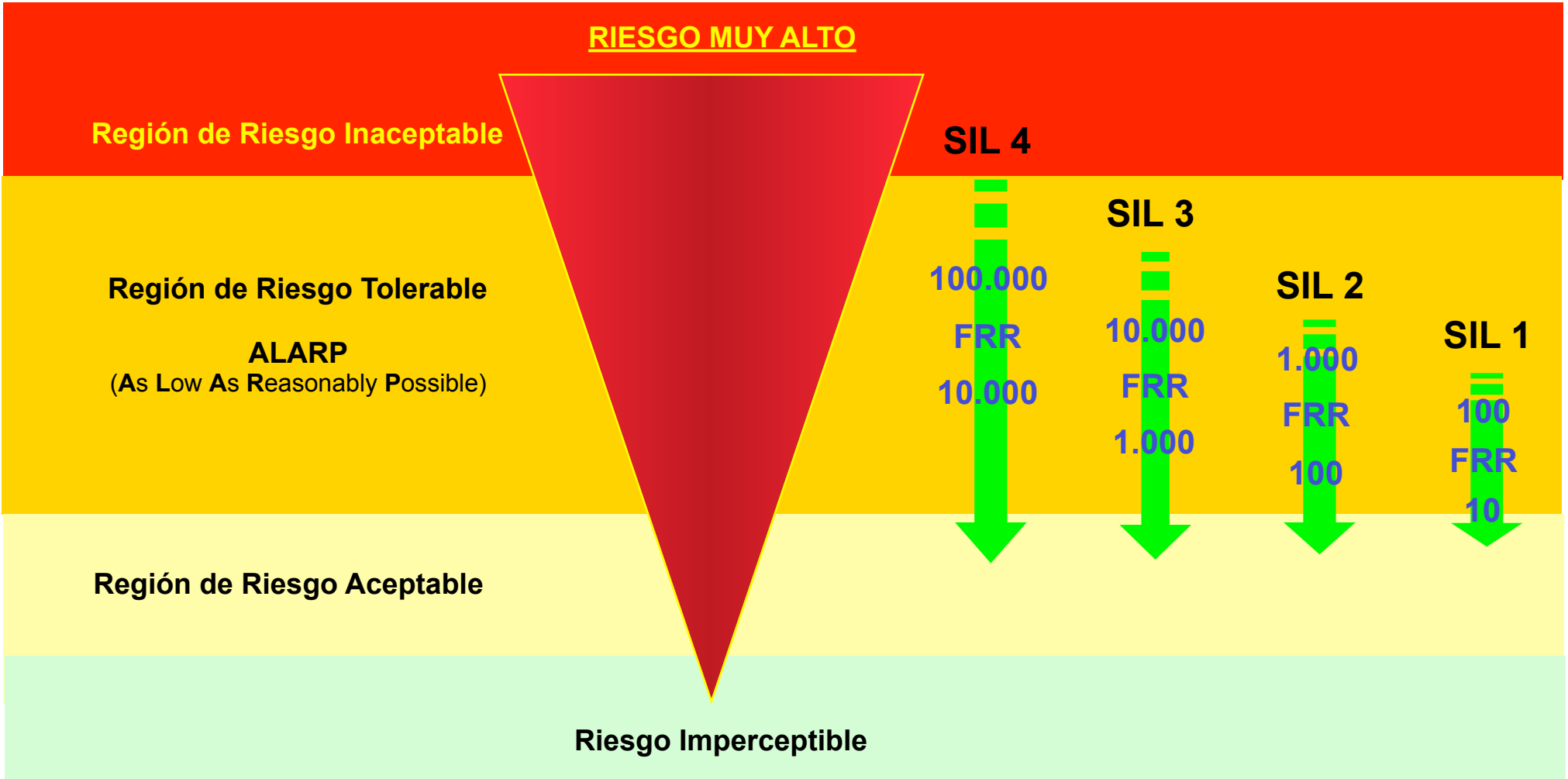
Las Funciones de Seguridad (FS)

- Una FS es toda función a ser implementada en cualquier sistema de seguridad (eléctrico, electrónico, electrónico-programable o de otra tecnología) destinada a conseguir y/o mantener el estado seguro del equipo bajo control y/o del proceso

FRR de una SIF - Nivel de Integridad de la Seguridad

- El FRR de una SIF se clasifica, según su orden de magnitud, en cuatro niveles, a los que se denomina Niveles de Integridad de la Seguridad (SIL)
  - FRR > 10 → SIL 1
  - FRR > 100 → SIL 2
  - FRR > 1000 → SIL 3
  - FRR > 10000 → SIL 4
- El FRR de una SIF se considera como FRF, pues su probabilidad de falla es “apreciable”
- En la etapa de diseño a este SIL se lo conoce como 'SIL Objetivo’
  - Es el orden de magnitud de la reducción de frecuencia requerida
  - Una vez que la SIF se halle lista para funcionar, habrá que demostrar que el FRR (FRF) finalmente obtenido por ella, esté, efectivamente, dentro del SIL Objetivo diseñado

FRR y SIL Objetivo



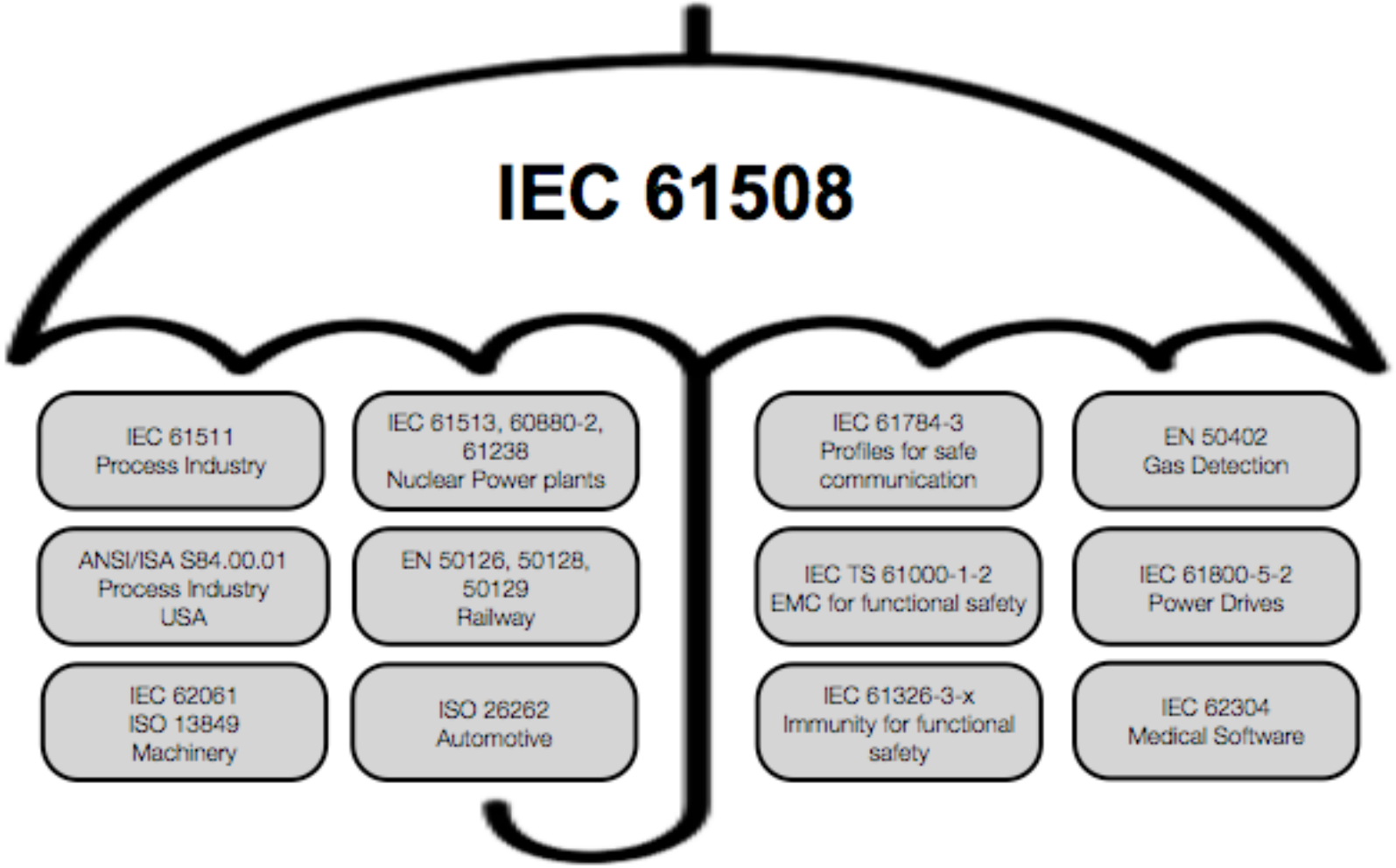
Nivel de Integridad de la Seguridad (SIL)

- Qué es el Nivel SIL?
  - Ante todo, es una medida cualitativa de la Seguridad
  - En segundo lugar es una medición cuantitativa de la confiabilidad

Qué es Seguridad Funcional?

- Seguridad Funcional se refiere a conseguir el comportamiento seguro de las funciones de seguridad, manteniendo bajo control, o evitando, cualesquiera de las fallas que éstas puedan tener
- Es decir que sólo obtendremos Seguridad Funcional
  - Cuando ninguna falla de ninguna función de seguridad pueda llevar a
    - Heridas o muerte de seres humanos
    - Contaminación del medio ambiente
    - Pérdidas en el equipamiento o en la producción
  - Y cuando este comportamiento seguro pueda mantenerse durante todo el ciclo de vida de esas funciones
- El 100% de funcionamiento seguro es imposible de obtener, pero los niveles SIL nos permiten aproximarnos a este valor, en la medida en que sea necesario para cada circunstancia.
  - A mayor SIL menor PF y, por lo tanto, mayor porcentaje de funcionamiento seguro

La Seguridad Funcional necesita Normas



Visión de IEC 61508 (SF en general)

- **Parte 1:**
  - **Requerimientos generales**
- **Parte 2:**
  - **Requerimientos para Sistemas Eléctricos, Electrónicos y Electrónicos Programables (E/E/PES)**
- **Parte 3:**
  - **Requerimientos del Software**
- **Parte 4:**
  - **Definiciones y abreviaturas**
- Parte 5:
  - Ejemplos de métodos para la determinación de los niveles SIL
- Parte 6:
  - Guías para la aplicación de las partes 2 y 3
- Parte 7:
  - Visión general de las técnicas

Visión de IEC 61511 (SF en procesos)

- **Parte 1:**
  - **Entorno de aplicación, definiciones, requerimientos de los sistemas (hardware y software)**
- **Parte 2:**
  - **Guía para la aplicación de IEC 61511-1**
- Parte 3:
  - Guía para a determinación de los niveles SIL requeridos

Fallas en las Funciones de Seguridad

Fallas y Seguridad

- Como ya dijimos, la seguridad funcional tiene que ver con poder controlar y evitar las fallas en las funciones de seguridad
- Existen tres tipos de fallas que pueden afectar a las funciones de seguridad
  - Fallas aleatorias del hardware
  - Fallas de causa común en el hardware
  - Fallas sistemáticas en el hardware y en el software
- Cualquiera de estas fallas pondrá a la función de seguridad en un estado específico de falla:
  - Seguro (falla segura o espuria, que produce el disparo de la función)
  - Peligroso (falla peligrosa, que impide el disparo de la función)
  - Intermedio (falla que no es ni segura ni peligrosa, todavía...)

Fallas Aleatorias del Hardware

- Son fallas espontáneas que pueden ocurrir en cualquier momento y en cualquier componente de hardware
- Sabemos que van a aparecer, pero no sabemos cuándo
  - Si son permanentes, existen hasta ser reparadas
  - Si son dinámicas, existen sólo bajo ciertas circunstancias
- Pueden ser caracterizadas por su frecuencia de aparición (en forma estadística):
  - λ (tasa de fallas)
  - λ puede ser constante o variable en función del tiempo

Probabilidad de Falla en Demanda

- La PFD depende generalmente de la suma de todas las tasas de fallas peligrosas.
  - Cuando el autodiagnóstico haga que las fallas DD disparen la acción protectora, la tasa de éstas ya no formará parte de la PFD. En ese caso, la PFD sólo dependerá de la tasa de las fallas peligrosas no detectadas
- Como la única forma de descubrir las fallas DU es realizar pruebas de comprobación, la PFD también dependerá del intervalo entre esas pruebas (PTI). Ver Descubriendo Fallas
  - La PFD es considerada entonces como un valor medio en ese intervalo

$$\mathbf{PFD = f (\lambda_{DU}, PTI)}$$

PFD = Probability of Failure on Demand

λ_{DU} = Failure Rate Dangerous Undetected

PTI = Proof Test Interval

PFD de la Función de Seguridad

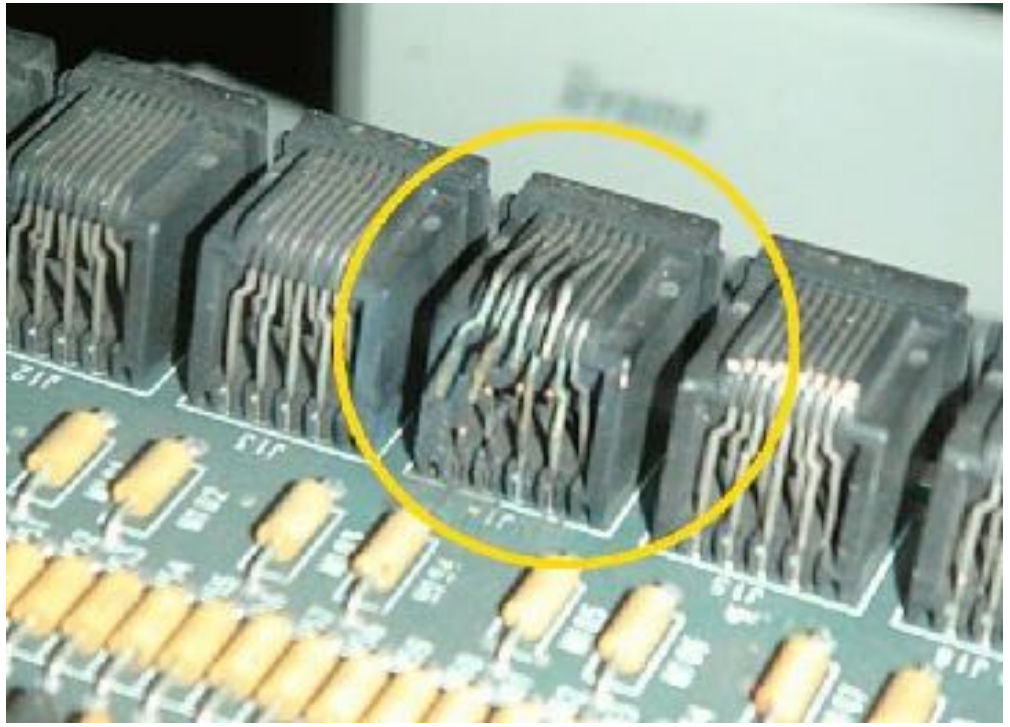
- En una SIF, cualquier falla peligrosa en uno de sus sub-sistemas (el de detección, el de lógica, el del actuador), hará que la seguridad se pierda
- Dicho de otra forma, la PFD de la SIF será igual a la suma de las PFDs de cada sub-sistema
  - $PFD = PFD_D + PFD_L + PFD_A$
- La PFD total deberá estar dentro del SIL Objetivo determinado para la función
  - Un cierto SIL implica que una cierta PFD debería ser alcanzada, pero una cierta PFD no significa que ese SIL será alcanzado
  - Para alcanzar el SIL, las fallas sistemáticas también tienen que corresponder a ese nivel

Probabilidad de Falla en Demanda de la SIF

- Relación entre la PFD, el FRR y el SIL

SIL	Probability of Failure on Demand (PFD)	Risk Reduction
4	$\geq 10^{-5}$ to $< 10^{-4}$	10000 to <100000
3	$\geq 10^{-4}$ to $< 10^{-3}$	1000 to <10000
2	$\geq 10^{-3}$ to $< 10^{-2}$	100 to <1000
1	$\geq 10^{-2}$ to $< 10^{-1}$	10 to <100

Fallas de Causa Común en el Hardware



- Son fallas que resultan de eventos que afectan de forma simultánea a varios componentes del hardware, llevando a un estado de falla general

- Estos eventos se relacionan con acontecimientos ambientales (calor, emisión electromagnética, caída de rayos, inundación, etc)

Fallas Sistemáticas

- Son fallas ocultas en el diseño o en la implementación de hardware o de software
- En cuanto aparecen se propagan en el ciclo de vida afectando
  - Especificaciones de diseño del sistema
  - Manual del Usuario
  - Procedimientos
  - En los SIS con controladores programables las fallas sistemáticas en el software son difíciles de evitar

Ciclo de Vida y Gestión de la Seguridad Funcional

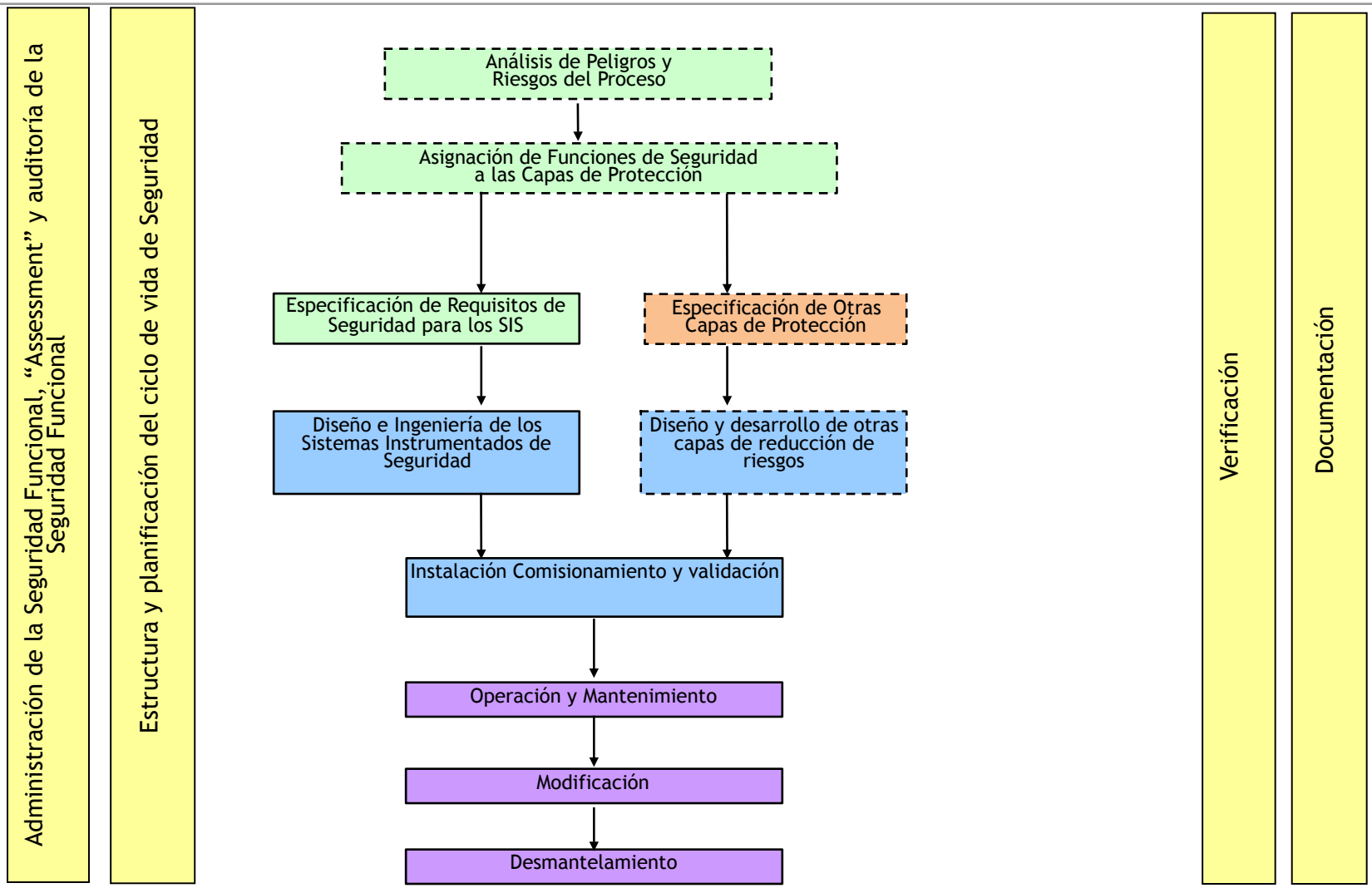
Concepto de Ciclo de Vida

- Un ciclo de vida nos ayuda sistemáticamente a:
  - Hacernos cargo de actividades necesarias
  - Asumir las responsabilidades
  - Identificar la pericia requerida para cada fase
  - Identificar las necesidades de documentación
  - Ocuparnos de las actividades de gestión (verificación, validación y assessment)
- Pueden definirse diferentes ciclos de vida
  - Diferentes aplicaciones (procesos, máquinas, etc.)
  - Usuarios, integradores, fabricantes de hardware, desarrolladores de software, etc.

Gestión de un ciclo de vida de seguridad

- Usar un ciclo de vida de seguridad sólo tendrá sentido cuando éste sea gestionado adecuadamente. Para eso es necesario:
  - Planear cómo deben ser hechas las cosas
  - Obtener y proveer la documentación necesaria
  - Hacer las cosas como estén indicadas
  - Verificar a cada paso que éstas hayan sido bien ejecutadas
  - Juzgar a cada paso si el nivel de seguridad requerido fue alcanzado
  - Auditar regularmente para comprobar si la seguridad se mantiene invariable con el transcurso del tiempo

Ciclo de Vida de IEC 61511



RISKNOWLOGY®

Gestión de la Seguridad Funcional

- La Gestión de la Seguridad Funcional (FSM) es el medio de garantizar que la seguridad va a poder ser mantenida durante todo el ciclo de vida
  - Define todas las actividades técnicas y de gestión
    - Establece cuáles son las tareas y cómo hacerlas
    - Determina cuáles son los requerimientos de planificación, documentación, verificación, validación y juzgamiento
    - Provee el control de modificaciones (MOC)
  - Especifica las responsabilidades y actividades para personas, departamentos y organizaciones, tanto internos como externos
- Para gestionar la Seguridad Funcional hace falta un Gerente

Hemos llegado al final

- Alguna pregunta más?
- Último pero no menos importante
  - Por favor completen nuestra hoja de evaluación
  - Queremos mejorar cada vez más este entrenamiento
- Ahora pueden irse... ¡pero esperamos que vuelvan!