EL SIL Y COMO LOGRARLO

Eduardo Cao
TECHINT Compañía Tecnica Internacional
ecao @techint.com

Resumen: El concepto de SIL como una medida de la robustez de una función de seguridad es cada vez más utilizado en los proyectos de ingeniería, pero si bien las empresas suelen definir claramente el SIL deseado, muchas veces no se tiene conciencia de todo lo que las normas exigen para alegar el cumplimiento del SIL. El logro de un determinado SIL no es simplemente el resultado de una cuidadosa ingeniería de la función de seguridad. Las normas IEC 61508 y 61511 exigen la existencia de un gerenciamiento de la Seguridad Funcional que debe contemplar todas las etapas del ciclo de vida del sistema.

1-Funciones Instrumentadas de Seguridad

Una Función Instrumentada de Seguridad (SIF = Safety Instrumented Function) es una protección que actúa en forma automática cuando una variable de proceso se desvía peligrosamente de su valor. Básicamente cada una de las relaciones de una matriz causa-efecto constituye una SIF.

Consisten en un sensor encargado de detectar la desviación de la variable, un ejecutor de lógica (usualmente un PLC) y un sistema de actuación, por ejemplo una válvula de emergencia actuada por una solenoide o un relé que detiene un motor.

Dado que se trata de una función vinculada a la seguridad del proceso, se la construye empleando elementos de alta confiabilidad. Se utilizan cableados dedicados, PLCs muy robustos, elementos duplicados etc. Sin embargo ningún sistema es infalible y una Función Instrumentada de Seguridad también tiene una probabilidad de falla.

La confiabilidad que debe tener una SIF depende del riesgo que está protegiendo. Por ejemplo una función encargada de apagar una bomba ante un bajo nivel del tanque para evitar la cavitación no necesita tener la misma robustez que una protección que evita que se exceda la presión de diseño en una planta de tratamiento que recibe gas de un pozo con alta presión de shut off.

La robustez de una SIF se mide por su Probabilidad de Falla en Demanda (PFD). Esto es la probabilidad que la función no actúe en el momento en que se requiere su

acción protectora. Se la suele expresar con términos como 10^{-2}, 10^{-3}, etc. Si la PFD de una SIF es 10^{-2} significa que en promedio fallará una vez de cada 100 demandas.

A la inversa de la PFD se la llama Factor de Reducción de Riesgo (FRR) . En el ejemplo anterior el FRR de la función de seguridad es 100 dado que esta función reduce 100 veces la frecuencia de ocurrencia del daño.

El riesgo de un evento de proceso que produce una cierta severidad de daño (por ejemplo la muerte de un operador o un determinado monto de pérdida económica) se mide por su frecuencia probable de ocurrencia.

Por ejemplo si la falla de un lazo de control puede provocar la rotura violenta de un recipiente y esto tiene suficiente severidad como para provocar fatalidades, podemos medir el riesgo por la frecuencia de ocurrencia de explosión o por la frecuencia de ocurrencia de la muerte del operador. La frecuencia no es la misma dado que la explosión puede ocurrir sin que el operador se encuentre presente.

Las empresas deben definir un criterio de aceptación de riesgo. Por ejemplo puede definirse que es inaceptable que ocurra una explosión de suficiente severidad como para provocar víctimas con una frecuencia anual mayor que 10^{-3} (o sea una probabilidad en 1000 de que ocurra durante el año). Si estimamos que la frecuencia de falla del lazo de control que provoca la rotura es 10^{-1}, significa que debemos reducir 100 veces esta frecuencia para llevarla a un valor aceptable. Necesitamos un FRR = 100.

Esto lo podríamos lograr con una SIF cuya PFD sea 10^{-2}. Sin embargo también existen otras capas de protección que pueden evitar el evento. Por ejemplo se pueden instalar alarmas que adviertan al operador del peligro, válvulas de seguridad, barreras mecánicas etc. Cada una de estas capas de seguridad tiene una PFD. Normalmente se acepta que la PFD de una válvula de seguridad (PSV) es 10^{-2}, de modo que en nuestro caso una PSV sería protección suficiente.

Cuando se instalan múltiples capas de protección, la PFD de todo el sistema se obtiene multiplicando las PFDs de todas las capas de protección. Así si instaláramos una válvula de seguridad y además una SIF con una PFD=10^{-2} se lograría una PFD del conjunto de 10^{-4}, es decir que se reduciría 10000 veces el riesgo, ya que para que ocurra la explosión deberían fallar simultáneamente ambas protecciones.

2-SIL (Safety Integrity Level)

Hace aproximadamente 15 años aparecen las normas IEC 61508 (Functional safety of electrical/electronic /programmable electronic safety related systems) y 61511 (Safety instrumented systems for the process industry sector).

La norma IEC 61508 es una norma genérica que fija lineamientos para cualquier aplicación que utilice sistemas eléctricos o electrónicos para cumplir funciones de seguridad. La IEC 61511se refiere específicamente a los Sistemas Instrumentados de Seguridad de las plantas de procesos y está dirigido a los usuarios de estos sistemas y a las empresas responsables de su diseño, construcción e instalación

Estas normas definen los requerimientos para lograr los distintos niveles de FRR de las funciones instrumentadas de seguridad.

Se define un parámetro llamado SIL que está directamente relacionado con la PFD a través de la siguiente tabla

PFD	10^{-1} a 10^{-2}	10^{-2} a 10^{-3}	10^{-3} a 10^{-4}
SIL	1	2	3

Según la importancia del riesgo a proteger cada función de seguridad tendrá asignado un valor de este parámetro y se deberán tomar los recaudos necesarios para lograr la probabilidad de falla que corresponda a su valor de SIL.

Es decir que se deben resolver dos cuestiones

1) Qué nivel SIL requiere una Función de Seguridad teniendo en cuenta la magnitud del riesgo que está protegiendo
2) Qué debemos hacer para asegurarnos que la Función de Seguridad cumple con el SIL requerido

3-Asignación de SIL

La primera de estas dos cuestiones es relativamente simple. Existen distintas técnicas para efectuar este análisis, pero básicamente se trata de estimar el riesgo asociado al escenario que la función protege y evaluarlo frente a un criterio de aceptación de riesgo.

El más popular de estos métodos es el de la Matriz de Riesgo Calibrada. Se define el riesgo con un conjunto de parámetros que permiten clasificar el escenario en función de la frecuencia probable de ocurrencia de la causa, severidad de las consecuencias, probabilidad de presencia humana en el área y posibilidad de evitar el

peligro. La combinación de todos estos parámetros permite decidir cual es el factor de reducción de riesgo necesario a través de un sencillo gráfico.

Conociendo los FRR de las capas de protección existentes se puede calcular cual es el FRR que debe tener la función de seguridad para llegar al FRR total requerido por el escenario

El método también se adapta para incluir riesgos económicos o ambientales.

Esta mecánica ya se ha popularizado en muchas empresas y se realiza luego del Hazop cuando se encara un nuevo proyecto.

4-Como lograr el SIL

La segunda cuestión es bastante más compleja. Las normas de seguridad funcional definen los requerimientos que se deben cumplir para lograr un determinado SIL.

Existe en muchas personas la equivocada creencia de que el logro del SIL es una cuestión de Ingeniería. Se le informa a los ingenieros de instrumentación y control cual es el SIL asignado a cada función y se piensa que ellos a través de una adecuada selección del hardware lograrán en cada SIF el FRR necesario y que éste se mantendrá durante toda la vida de la planta.

Pero si bien es necesario que los elementos que componen la Función de Seguridad y la arquitectura de la misma hayan sido seleccionados teniendo en cuenta el SIL requerido, muchos de los requisitos para poder pretender un determinado SIL tienen que ver con el Sistema de Gestión de Seguridad de la empresa que va a operar la planta como se verá mas adelante.

5-Sistema de Gestión de Seguridad

El principal requerimiento de la IEC 61511 es que las actividades vinculadas a aspectos de seguridad deben estar gerenciadas. Debe existir un Planeamiento de la Seguridad definido a través de procedimientos que permitan garantizar y demostrar que la seguridad se va a gestionar y mantener durante toda la vida del sistema.

Se debe establecer un marco de trabajo en el que deben desarrollarse todas las actividades de la Gestión de la Seguridad y que permita demostrar que todas las personas , Departamentos u Organizaciones involucradas en las tareas de gestión de la seguridad conocen las responsabilidades y funciones que les han sido asignadas, y

tienen el nivel de capacitación adecuado para desarrollarlas y tienen la capacidad de liderazgo necesaria para hacer cumplir todos los procedimientos .

Los procedimientos deben definir quienes serán los encargados de cada tarea , como deben demostrar su capacidad, como se realizarán y documentarán todas las actuaciones vinculadas a la gestión de la seguridad, quienes recibirán la documentación, y cuales serán sus responsabilidades.

Se exige que todos los proveedores y empresas involucradas en actividades relacionadas con el sistema de seguridad posean un sistema de calidad

6-Ciclo de Vida del Sistema de Seguridad

La norma define un Ciclo de Vida del Sistema Instrumentado de Seguridad (SIS), formado por una serie de etapas que deben llevarse a cabo desde la concepción del sistema hasta su desmantelamiento. Estas etapas son

1-Evaluación de Riesgos y Peligros

2-Asignación de las funciones de seguridad a capas de protección

3´-Especificación de los Requerimientos de Seguridad del SIS

4-Ingeniería del SIS

5-Instalación, comisionado y validación

6-Operación y Mantenimiento del SIS

7-Modificación del SIS

Estas etapas se deben llevar a cabo obligatoriamente y en ese orden. Se establecerá la información de entrada y de salida de cada una de las etapas de modo que el producto de cada etapa sea el input de la siguiente

7-Verificaciones, Evaluaciones y Auditorías

Este ciclo de vida estará sujeto a Verificaciones, Evaluaciones (Assessments) y Auditorías

7.1-Verificaciones.

Las verificaciones deben llevarse a cabo en **cada una** de estas etapas y deben permitir demostrar por revisión, análisis o prueba que el producto de esa etapa responde a todos los requerimientos de entrada. En el planeamiento de la seguridad se debe identificar para cada etapa

Que actividades se desarrollarán

Procedimientos y técnicas que se utilizarán

Cuando se realizarán

Responsables

Información contra la que se realizará la verificación

Manejo de no conformidades

7.2-Evaluaciones (Assesments)

Un assessment, en el contexto de la Norma, es similar a una auditoría de calidad. A diferencia de las verificaciones, no se entra en el detalle técnico de lo que se realizó sino más bien en el cómo se realizó. El objetivo es comprobar que se está cumpliendo con el planeamiento y los procedimientos definidos para la gestión de la seguridad, que se están siguiendo las etapas del ciclo de vida, realizando las verificaciones, que todas las sugerencias realizadas en cada etapa fueron implementadas, y que se cumplen los procedimientos de cambio.

No se realizan en todas las etapas del Ciclo de Vida sino en algunos hitos puntuales. Como mínimo se debe realizar un assessment antes de comenzar la operación.

7.3-Aditoría

Es similar al assessment pero se realiza periódicamente cuando el sistema está funcionando. Comprueba que se siguen cumpliendo los procedimientos y que no se degradó el SIL

8-Etapas del Ciclo de Vida

Veremos a continuación como debe desarrollarse cada una de estas etapas en relación al logro del SIL

8.1-Etapa 1 Análisis de Peligros

Si bien existen otras técnicas lo más usual es que la identificación de peligros de una planta de proceso se realice con un Hazop.

La técnica del Hazop ya se encuentra arraigada y cuenta con larga tradición de modo que resulta raro en un proyecto de ingeniería que no se realice un Hazop.

Como resultado del mismo se ponen en evidencia los peligros de la instalación y suele hacerse una evaluación de los riesgos involucrados y de las capas de protección existentes. No entraremos en detalle ya que suele ser una técnica bien conocida.

Pero es conveniente remarcar que como cualquier etapa del Ciclo de Vida, el Hazop debe ser objeto de una verificación y los procedimientos deben definir quienes serán los responsables de esta verificación y cómo se realizará

8.2-Etapa 2 Asignación de las Funciones de Seguridad a Capas de Protección

Normalmente nos referimos a esta etapa como Asignación de SIL, dado que la mayoría de las capas de protección son funciones instrumentadas de seguridad. La forma de realizar esta etapa ya se ha explicado en la Sección 3.

Al igual que el Hazop, la mecánica de asignación de SIL ya está instalada en muchas empresas y se practica usualmente en los proyectos

8.3-Etapa 3. Especificación de los Requerimientos de Seguridad

La Especificación de Requerimientos de Seguridad es un documento fundamental en el proyecto y un requisito de la norma, aunque muchas veces no se le presta la debida importancia y en otros casos ni siquiera se elabora.

Esta especificación debe definir los requerimientos para realizar la ingeniería del software y del hardware y ser lo suficientemente clara y completa para que el producto (SIS) responda a los requisitos de seguridad y funcionalidad , que sus interfaces sean las esperadas por el personal de operaciones, que permita el mantenimiento y que permita una adecuada y segura comunicación con el DCS u otros sistemas instrumentados

Para ello la especificación debe definir para cada una de las funciones de seguridad toda la información que se requiere para desarrollar la ingeniería. Esto incluye:

-Frecuencia esperada de demanda de cada SIF

-Valores de trip

-Estado Seguro del sistema

-Nivel SIL con el que debe ejecutarse la función

-Tiempo en el que debe actuar

-Tiempo de seguridad del proceso

-Intervalos de mantenimiento y tests periódicos

-Tiempo de reparación de las fallas detectadas por los sistemas de autodiagnóstico

-Posibilidad de implementación de by passes de mantenimiento u operación

-Tiempos de validez del by pass y acción a tomar si el tiempo se excede

-Degradación de lógicas de votación ante un by pass

-Degradación de lógicas de votación ante fallas detectadas

-Existencia de diagnóstico externo a través de otro instrumento

-Modos de efectuar el reset

-Niveles de pre alarma

-Requerimientos de hardware (botoneras locales, paneles,luces etc)

-Requerimientos de interfase con el operador (HMI) :

-Tolerancia a falla espuria

-Jerarquías y permisos de acceso

-Requisitos de comunicación con el DCS u otros sistemas

-Condiciones ambientales particulares

Las lógicas más complejas deben describirse con todo detalle indicando permisivos, confirmación de actuación por fines de carrera, acción en caso de falla etc.

8.4-Etapa 4 Ingeniería del SIS

Una función instrumentada de seguridad está formada por tres subsistemas:

-Subsistema de detección .Son los transmisores que detectan el desvío del proceso

-Subsistema lógico: Usualmente un PLC que ejecuta la lógica

-Subsistema de actuación (relés solenoides válvulas)

Cada uno de los componentes de un sistema de seguridad puede fallar en forma peligrosa (no actuar cuando se requiere) o en forma espuria (actuar cuando no se requiere). Las fallas peligrosas afectan la seguridad. Las fallas espurias pueden provocar paradas de planta no deseadas.

Cualquiera de estos tres subsistemas que presente una falla en demanda hará que la función no actúe

A su vez, la probabilidad de falla de cada subsistema puede reducirse empleando elementos que tengan baja tasa de falla o por medio de redundancia, es decir instalando elementos duplicados o triplicados con lógicas de votación.

En la etapa de ingeniería se seleccionarán los elementos a utilizarse para el armado de la SIF y se definirán las lógicas de votación que permitan el logro del SIL

La probabilidad de que un elemento falle cuando se requiere su acción depende de la calidad del elemento y de la frecuencia con que se lo controla. Es evidente que si revisamos anualmente el estado de un elemento de seguridad, la probabilidad de que lo encontremos en falla en el momento que lo necesitamos será menor que si lo revisamos cada cinco años.

Cada elemento de seguridad debe ser inspeccionado al cabo de un período TI (Test interval) que no debe ser mayor que el tiempo esperado entre dos demandas de actuación. Entonces La probabilidad que en el momento que ocurre la demanda encuentre al elemento en falla es

$$PFD = \lambda_D.TI/2 \qquad (1)$$

Donde λ_D. es la tasa de fallas peligrosas del elemento (frecuencia esperable de fallas por año). Este valor está entre de 10^{-2} a 10^{-3} para un transmisor y depende de su calidad.

Puede observarse de la ecuación 1 que tiene tanta importancia la calidad del elemento ($\lambda_{D)}$ como el tiempo de testeo (TI). Cuando se realiza la ingeniería del SIS suele prestarse gran importancia a la selección de los elementos que se utilizarán, pero se descuida la calidad del test periódico.

Dentro de los procedimientos de seguridad debe haber una especificación detallando como se debe llevar a cabo esta inspección, quienes serán sus responsables, que elementos y técnicas se usarán, como se documentarán los resultados, cuales serán las tolerancias de aceptación, manejo de fallas detectadas etc

La selección de los elementos que se utilizarán para conformar la SIF es otro aspecto a tener en cuenta. La norma IEC 61508 define una serie de medidas que los fabricantes de equipamiento deben adoptar para evitar fallas sistemáticas en el diseño y para controlar las fallas aleatorias cuando se produzcan . Estas medidas dependen del nivel SIL de la función de seguridad en que el elemento será instalado.

Es evidente que el usuario final no tiene forma de saber si el elemento ha sido fabricado teniendo en cuenta estas medidas. Entonces se recurre a empresas certificadoras. Son empresas que , a través de inspeccionar los procedimientos del fabricante emiten un certificado diciendo que el elemento fue diseñado y fabricado según los procedimientos de la norma.

No existen requisitos para actuar como empresa certificadora. La validez de estos certificados radica en la confianza que la empresa certificadora inspire al usuario.

El certificado indica que el elemento puede ser utilizado en funciones de seguridad de determinado SIL.

Pero esto no significa que instalando elementos certificados por ejemplo para SIL 2 es suficiente para alegar el SIL 2 de la función.

La norma exige que se pueda demostrar por cálculo que con la frecuencia de testeo que se empleará para controlar todos los elementos la PFD de la función de seguridad estará dentro de los límites que definen el SIL 2. Existen varias técnicas para realizar estos cálculos y estas técnicas están detalladas en la norma IEC 61508. Para arquitecturas sencillas existen fórmulas simplificadas . Para las arquitecturas más complejas se utilizan árboles de falla, ya sea estáticos o dinámicos, diagramas de confiabilidad o modelos de Markov

Estos cálculos, además del TI, dependen de la redundancia y arquitecturas de votación , de las tasas de falla peligrosa y espuria de los elementos empleados , de los tiempos de reparación y de la cobertura de autodiagnóstico de los instrumentos.

Un tema importante es la tasa de falla de cada elemento que se empleará en el cálculo. Los certificados emitidos por las empresas certificadoras contienen el valor de la tasa de falla teórica del elemento. Pero esta tasa de falla se obtiene por cálculo y no representa la tasa real de falla del elemento en condiciones instaladas y en el ambiente de la planta, con condiciones de altas temperaturas, lluvias, ambientes corrosivos, fluctuaciones de tensión y con los procedimientos de mantenimiento propios del usuario. Por eso la norma IEC 61511 exige que se disponga de un sistema de recolección de datos que permita comprobar que la tasa de falla de los distintos componentes coincide con la asumida en el cálculo.

Los elementos empleados en las funciones de seguridad pueden sufrir fallas sistemáticas. Estas son fallas que afectan a todos los elementos de un mismo tipo y que pueden deberse a errores de especificación, errores en la selección de materiales, errores de instalación o mantenimiento etc. y que no responden a la estadística. Por eso la norma también exige que se disponga de un sistema que permita detectar las fallas sistemáticas a través de un análisis estadístico de fallas

También se exige un sistema de recolección de datos que permita comprobar que la frecuencia de demanda de la SIF es la asumida en el diseño.

Adicionalmente a todo lo anterior las normas presentan tablas de redundancia mínima para cada nivel SIL que exigen duplicar o triplicar los elementos a instalar

según el SIL pretendido y que tienen por objeto evitar abusos en la selección de tasas de falla irreales.

Durante la etapa de ingeniería también debe preparase el procedimiento a utilizarse en la validación del sistema

También, como cualquier otra etapa del ciclo de vida la ingeniería debe estar sujeta a verificación y los procedimientos de gestión de seguridad deben definir los encargados y procedimientos para efectuarla

8.5-Etapa 5 Instalación, Comisionado y Validación

Una vez instalado el sistema y antes de la puesta en marcha se debe realizar la validación, normalmente conocida como SAT (Site Acceptance Test).

Este se debe llevar a cabo siguiendo un procedimiento minucioso preparado y verificado en la etapa de ingeniería. Es usual que previo a éste se haya realizado un test de la lógica del sistema en fábrica (FAT), de modo que el SAT se concentra más en el chequeo de direcciones, ajuste de lazos, calibración de transmisores etc.

Pero es importante que las lógicas sean probadas en su totalidad. El procedimiento de testeo debe simular los diferentes caminos lógicos que permitan comprobar que la reacción del sistema es la esperada. Se controlarán los tiempos de respuesta , interfases con el operador, lógicas de reset, detección de fallas por los sistemas de autodiagnóstico, by passes de lógicas, etc.

Se debe documentar cuidadosamente las pruebas efectuadas y la acción adoptada ante no conformidades y prepara un legajo que resulte comprensible y sirva de referencia durante toda la operación del sistema.

8.6-Etapa 6 Operación

Los procedimientos de seguridad deben establecer las medidas que se deben adoptar durante la fase de operación para asegurar que el SIL se va a mantener durante toda la vida del sistema.

Resulta fundamental adherir a la frecuencia de testeo periódico adoptada para el cálculo de la PFD y los procedimientos indicarán los responsables de realizarlos, forma de documentarlos, manejo de fallas y criterios de aceptación.

Se explicitarán las acciones que se deben realizar durante el mantenimiento para mantener el sistema en operación segura.

Se definirá que información debe recolectarse para chequear las frecuencias de falla y cual será la acción si la misma difiere de la esperada.

Se definirán los planes de capacitación de operarios y personal de mantenimiento.

Se definirá la frecuencia y alcance de las auditorías

8.7-Etapa 7 Decomisionado

Cuando el sistema sea decomisionado y puesto fuera de servicio las tareas deben estar cuidadosamente planificadas. Se requiere un estudio que identifique las tareas a efectuar y los peligros a los que pueden dar origen y que permita garantizar la seguridad durante el procesos de decomisionado

9- Conclusiones

Como puede verse, el logro de un determinado SIL requiere que el usuario final de la instalación posea un sistema de gerenciamiento de la seguridad y que el mismo se encuentre operativo. El logro de la seguridad funcional no es exclusivamente una cuestión de ingeniería sino que los procedimientos involucran actividades a lo largo de todo el Ciclo de Vida para garantizar que la seguridad se va a gestionar y mantener durante toda la vida del sistema

Referencias

1)IEC-615011 Safety Systems for the Process Industry Sector 1st Edition 2003
Part 1: Framework, definitions, system, hardware and software requirements
Part 2: Guideliness on the application of Part 1
Part 3: Guidelines for the determination of the required safety integrity level
2)IEC 61508 Functional Safety of electrical/electronic/programmable electronic safety related systems
Part 1:General requirements
Part 2: Requirements for of electrical/electronic/programmable electronic safety related systems
Part 3: Software Requirements
Part 4: Definitions and abreviations
Part 5: Examples of methods for the determination of SIL
Part 6: Guidelines on the application of IEC 61508-2 and 61508-3

Part 7: Overview of techniques and measures

Autor: Eduardo Cao

Ingeniero químico de UBA. Asesor de Seguridad de Procesos de Techint SA .

Anteriormente en Skanska, Tecnor, CNEA. Es Profesor Titular de la UBA y el ITBA.

Ingeniero en Seguridad Funcional TUV Sud