Procedimiento para la determinación de las funciones de seguridad y su Nivel de Integridad de la Seguridad (SIL)

Sergio Hilario Gallina
CONICET - GICSAFe
Departamento de Electrónica
FTyCA - UNCA
Catamarca - Argentina
sgallina@tecno.unca.edu.ar

Ariel Lutenberg
CONICET - GICSAFe
Laboratorio Sistemas Embebidos
Facultad de Ingenieria - UBA
Buenos Aires - Argentina
lse@fi.uba.ar

***Abstract*— En este trabajo se presenta una metodología sistematizada en siete pasos para determinar el nivel de integridad de la seguridad de un sistema. Además se presenta una planilla de cálculo que puede ser usada como guía y soporte para la aplicación del método propuesto.**

Keywords—SIL; Seguridad funcional; Función de seguridad; Sistema instrumentado de seguridad

I. Introducción

Una función de seguridad es una función implementada mediante algún dispositivo que actúa sobre un sistema electrónico, eléctrico o electrónico programable (E/E/PE) a los fines de reducir las probabilidades de que tenga lugar un evento indeseado y haya una exposición al riesgo [1].

Una función instrumentada de seguridad funcional (SIF) es un lazo de control que debe llevar o mantener en un estado seguro a un sistema. El conjunto de funciones de seguridad constituye parte del sistema instrumentado de seguridad (SIS). Un SIS comprende normalmente más de un SIF, y un SIF puede incluir uno o más sensores y uno o más actuadores, como se ilustra en la Fig. 1. Las propiedades básicas de las SIF definidas por Varela en [2] son:

- Medición de variables de proceso o ambientales.
- Determinacion de variables que superan los límites establecidos.
- Actuación del elemento final de control (actuador).
- Tiempo de respuesta.
- Nivel de integridad de la seguridad.

Durante el proceso de definicion de requerimientos se analiza para cada función de seguridad los aspectos relacionados con la operación y los objetivos de la SIF. En la Fig. 2 se presenta un resumen de las preguntas más importantes a responder antes de comenzar el desarrollo de una función de seguridad.

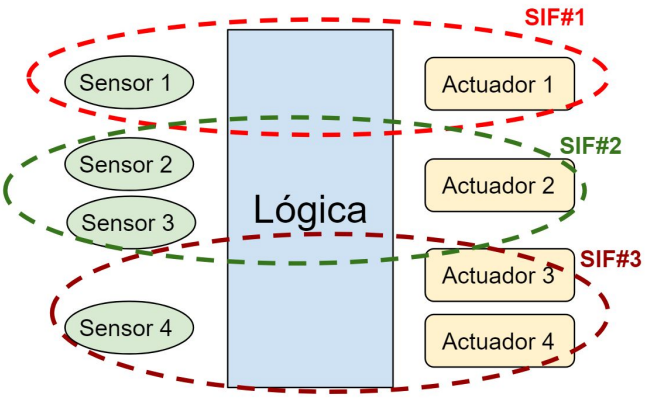

Fig. 1: Ejemplo de un sistema instrumentado de seguridad (SIS) compuesto por tres funciones instrumentadas de seguridad (SIF).

II. DESARROLLO

En este trabajo se propone una metodología de trabajo de siete pasos para el diseño de funciones de seguridad y verificación del SIL obtenido. Estos pasos se ilustran en la Fig. 3 y son los siguientes:

Paso 1: Diseño conceptual del sistema. Definición de los límites (espaciales, temporales, de uso, ambientales, etc.)

Paso 2: Gestión de los riesgos. Análisis, cuantificación, evaluación y documentación de los riesgos asociados al sistema.

Fig. 2: Aspectos a considerar en la definición de una función instrumentada de seguridad funcional (SIF).

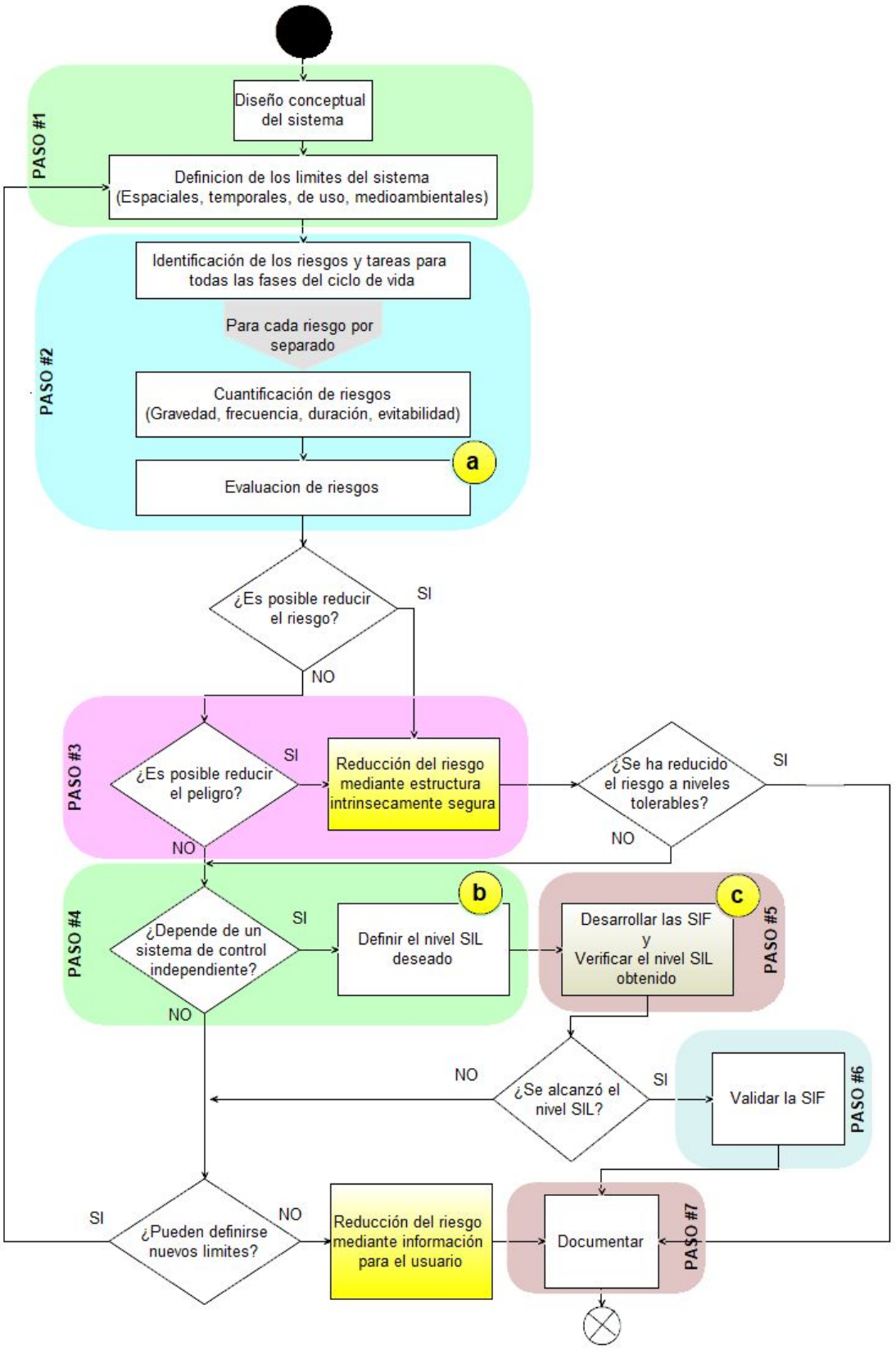

Fig. 3: Metodología propuesta para de desarrollo de una SIF

Paso 3: Seguridad intrínseca. Crear estructuras intrínsecamente seguras para reducir la probabilidad de ocurrencia de un peligro, o lo que es lo mismo reducir los riesgos en todos los casos que sea posible hacerlo.

Paso 4: Definir un sistema de control independiente de la aplicación, para eliminar el riesgo o reducirlo hasta un nivel tolerable. Incluye la determinación del nivel de integridad de la seguridad deseado (SIL)

Paso 5: Diseñar las funciones de seguridad. Definir las arquitecturas de las protecciones técnicas para aquellos riesgos residuales. Verificar el sistema de seguridad funcional para garantizar que el sistema de seguridad cumple los requisitos SIL definidos en el paso 4.

Paso 6: Validar el sistema de seguridad funcional para asegurarse de que el sistema de seguridad cumple con su cometido de reducir los riesgos.

Paso 7: Documentar el sistema de seguridad funcional.

III. Procedimiento Propuesto

Para facilitar los cálculos en los siete pasos propuestos se propone una planilla de cálculo que permite analizar el desempeño de las SIF, a la que se puede acceder en [3].

Las características principales de la planilla son:

- Permite el cálculo del SIL para sistema de bajo demanda y operación contínua.
- Calcula las probabilidades medias de fallo en demanda (PFDavg) de cada uno de los subsistemas y de la SIF completa.
- Calcula el nivel integrado de seguridad de la SIF.
- Permite la comparación de resultados para diferentes arquitecturas para cada uno de los subsistemas de la SIF (1oo1, 1oo2, 1oo3, 2oo2, 2oo3 y 2oo4).
- Compara el resultado de los cálculos SIL obtenidos con la arquitecturas utilizada y el SIL objetivo de la SIF.

Los datos a ingresar en la planilla son:

- Características del riesgo (consecuencia y duración; probabilidad de ocurrencia; posibilidad de prevención y gravedad)
- Cantidad de elementos de entrada (entre 1 y 3 en este trabajo)
- Tipo del elemento de entrada.
- Cantidad de elementos de salida (entre 1 y 3 en este trabajo)
- Tipo del elemento de salida.
- Tasa de falla de cada elemento de entrada y salida.

Los datos que se obtienen como salida de la planilla son:

- Nivel SIL de la entrada para diferentes configuraciones de la arquitectura de votación.
- Nivel SIL de la salida para diferentes configuraciones de la arquitectura de votación.
- Nivel SIL general de la función de seguridad para diferentes arquitecturas de votación.
- Conclusión sobre si se cumple o no con el SIL objetivo.

A. Diseño conceptual del proceso

La gestión de la seguridad se realiza desde la primera fase del ciclo de vida del sistema [4]. En cada fase se debe garantizar el cumplimiento de las normas de seguridad y las normas de gestion de calidad de la serie ISO 9001.

De acuerdo con normas internacionales tales como la IEC 61508 la definición conceptual del proyecto se realiza en la fase 1 del desarrollo e incluye aspectos tales como: finalidad del proyecto, restricciones y supuestos, contexto del proyecto, alcance del proyecto, entorno del sistema, descripción preliminar del sistema, definición preliminar de hitos y plazos, política y objetivos de seguridad.

B. Gestión de los riesgos

En este paso se deben identificar las situaciones físicas que encierran posibilidades de daño (los peligros) y las causas que lo originan. Las normas (IEC 61508, EN 50126, etc.) orientan respecto a los métodos de análisis a utilizar.

Las tareas a documentar en relación a los riesgos son: evaluación de frecuencia y gravedad de cada peligro, valuación y aceptación del riesgo, revisión de la tolerabilidad de riesgo, adopción de medidas para reducir los riesgos a un nivel tolerable, revisión de la efectividad de las medidas de reducción de riesgos, registros de peligros. Todo esto debe quedar documentado en el Registro de Peligros como base para la gestión de riesgos [4].

Algunas de las preguntas que deben formularse en la instancia de evaluación son por ejemplo las siguientes [4]:

- ¿Cuáles son las tareas peligrosas durante la operación del sistema?
- ¿Cuáles son las consecuencias si ocurriese una situacion de falla?
- ¿Deben las fallas en el sistema de seguridad producir paradas de proceso?
- ¿Puede el sistema de seguridad tener fallas que aún no hayan sido detectadas?
- ¿El personal está debidamente entrenado?
- ¿La gerencia apoya y promociona una cultura de la seguridad?

Los métodos de evaluación de riesgos podrán ser cualitativos o cuantitativos. En el primer caso la evaluación es realizada por un experto o panel de expertos que juzgan la frecuencia y las consecuencias de cada riesgo. En el segundo caso la evaluación es realizada utilizando datos de frecuencia de fallas para calcular la probabilidad de falla ante una demanda.

El riesgo es función de la consecuencia o gravedad del daño y la frecuencia de ocurrencia, es decir:

$$Riesgo = f(Gravedad + Probabilidad\ de\ ocurrencia) \quad (1)$$

La frecuencia de ocurrencia (F) está relacionada con el tiempo de exposición al peligro, la probabilidad (P) de poder evitar el evento peligroso y la probabilidad (W) de que sin la adición de un SIS ocurra el evento peligroso.

La planilla de calculo [3] presenta un sistema de cuatro tablas que facilitan la selección de F, W, P y la severidad de las consecuencias, (S), como se muestra en la Tabla I.

TABLA I. SELECCIÓN DE LOS PARÁMETROS F,W,P,S

Frecuencia y tiempo de exposición al peligro (F)		
Frecuencia / Tiempo de exposición	**F > 10 min**	**F ≤ 10 min**
≤ 1 h	5	5
> 1 h ≤ 1 día	5	4
> 1 día ≤ 2 sem	4	3
> 2 sem ≤ 1 año	3	2
> 1 año	2	1

Probabilidad de ocurrencia del evento peligroso (W)	
Probabilidad de evento peligroso	**W**
Muy Alta	5
Probable	4
Posible	3
Raro	2
Insignificante	1

Posibilidad de que el evento sea prevenido (P)	
Prevención	**P**
Imposible	5
Posible	3
Probable	2

Severidad de las consecuencias	
Consecuencia y gravedad	**S**
Intolerable (Muerte)	4
No deseable (Perdida de bienes)	3
Tolerable (Reversible mediante cambio o reparación)	2

C. *Seguridad intrínseca*

Una vez identificados los peligros estos se intentarán eliminar o reducir en la fase de diseño del sistema mediante la supervisión de las tareas de diseño e implementación, la certificación de procesos de diseño bajo normas de calidad y el uso de arquitecturas y métodos aceptados por normas. Para aquellos peligros que no puedan minimizarse mediante estas técnicas, se deberá seguir el paso 4 del procedimiento propuesto en la Fig. 3.

Esto permitirá que los componentes o sistemas posean un modo de falla bien establecido, de tal manera que un sistema así construido no pueda permitir una condición más permisiva que la que existe en ausencia de fallo [5].

El crecimiento exponencial del número de combinaciones de fallas resulta en que un enfoque determinista no es viable para lograr la seguridad intrínseca. Con sistemas complejos podrá utilizarse métodos probabilísticos [5].

Es importante destacar que los sistemas de seguridad incorporados en el sistema de control de procesos, no forman parte del SIS. En las fig. 4 y 5 se muestran estrategias de separación de las funciones de seguridad y de control.

D. *Definir un sistema de control*

Si el peligro no se ha reducido lo suficiente mediante técnicas de seguridad intrínseca y el nivel de riesgo no está en valores aceptables, pero es posible crear un sistema de control mediante una SIF, se debe entonces definir el nivel de integridad de la seguridad. Para ello en primer lugar se debe establecer cuál será el modo de operación: (a) *bajo demanda* u (b) *operación contínua* (también denominado en ocasiones "*alta demanda*").

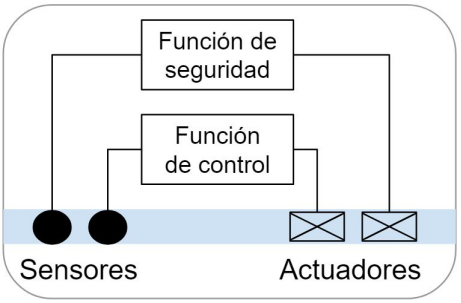

Fig. 4: Funciones de control y seguridad separadas

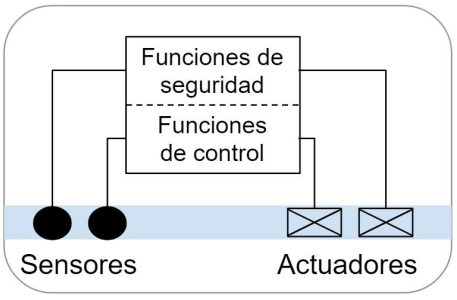

Fig. 5: Funciones de control y seguridad separadas logicamente pero integradas en una unidad de procesamiento

a) *Modo de operación bajo demanda*

En este caso se debe calcular la probabilidad de falla en demanda promedio (PFDavg) que permita reducir el riesgo hasta un nivel aceptable.

$$PFDavg = \frac{Riesgo\ aceptable}{Rf} \quad (2)$$

Dónde *Riesgo aceptable* está dado por el cociente ocurrencias/año, *Rf* es la frecuencia de ocurrencia del riesgo y *PFDavg* es la probabilidad de falla en demanda promedio.

Con el resultado obtenido de la Eq. (2) se determina el nivel SIL objetivo para llevar el riesgo a niveles aceptables. La correspondencia entre SIL y PFDavg se muestra en la norma IEC 61508. Tabla 2 *"Safety Integrity Level – Target failure measures for a safety funtion operating in low demand mode of operation"*.

La planilla de calculo propuesta en [3] presenta una tabla de doble entrada que permite determinar el SIL objeto en forma simple. Esa tabla se ilustra en la Tabla II. El método aplicado se denomina método general de graficas de riesgo [8] y se basa en las tablas mostradas en la Tabla I donde se definieron F, P, C y W.

TABLA II. MATRIZ DE ASIGNACIÓN DEL SIL

Consecuencia y gravedad	**S**	**Clase K = F+W+P**				
		3 - 4	**5 - 7**	**8 - 10**	**11 - 13**	**14 - 15**
Intolerable (Muerte)	4	SIL2	SIL2	SIL2	SIL3	SIL3
No deseable (Perdida de bienes)	3	-	-	SIL1	SIL2	SIL3
Tolerable (Reversible)	2	-	-	-	SIL1	SIL2
Resultado obtenido		**-**	**-**	**-**	**-**	**SIL3**

b) Modo de operación continua

El método para calcular la probabilidad de falla de una función de seguridad para un sistema relacionado con la seguridad E/E/PE en modo contínuo de operación es similar al calculado para un modo de operación de baja demanda, excepto que la probabilidad promedio de falla bajo demanda (PFD_{SYS}) se reemplaza con la frecuencia promedio de falla peligrosa (PFH_{SYS}).

La probabilidad general de una falla peligrosa de una función de seguridad para el sistema de seguridad E/E/PE, PFH_{SYS}, se determina calculando las tasas de falla peligrosa para todos los subsistemas que en conjunto proporcionan la función de seguridad y suman estos valores individuales. Con probabilidades pequeñas [5] esto puede expresarse de la siguiente manera:

$$PFH_{SYS} = PFH_S + PFH_L + PFH_{FE} \quad (3)$$

PFH_{SYS}: frecuencia promedio de falla peligrosa de una función de seguridad;

PFH_S: frecuencia promedio de falla peligrosa para el subsistema de sensores;

PFH_L: frecuencia promedio de falla peligrosa para el subsistema lógico;

PFH_{FE}: frecuencia promedio de falla peligrosa para el subsistema de elemento final.

Dada la tasa de fallas peligrosas (λ) y la tasa de riesgos tolerable (THR), se pueda calcular en forma aproximada el valor del SIL a partir de [15]:

$$SIL = f(S, C, E, P) \quad (4)$$

donde S es la severidad de las consecuencias, C es un medida de la reducción de las consecuencias, E depende del tiempo de exposicion al peligro y P es la probabilidad de poder evitar el evento peligroso.

En la Tabla III se muestran los rangos THR para cada valor de SIL de acuerdo con lo indicado en la norma IEC 61508. En la última columna se indica el valor de SIL obtenido de acuerdo con la ecuación (4) (el ejemplo de la Tabla III corresponde a haber obtenido SIL2).

Para los dos casos, baja demanda u operación contínua, el cálculo del SIL se puede realizar por métodos cualitativos y cuantitativos. Los métodos cualitativos son métodos con cierto rango de incertidumbre. Los métodos cuantitativos proporcionan resultados más objetivos y auditables. El método de tablas propuesto requiere la evaluación cualitativa y cuantitativa de la efectividad de las capas de protección previstas. El resultado será el valor SIL a lograr para un evento en particular.

TABLA III. MATRIZ DE ASIGNACION DEL SIL PARA SISTEMA DE ALTA DEMANDA

THR inicial por hora (Rango)		SIL	Resultado Eq. (4)
1,00E-09	1,00E-08	4	-
1,00E-08	1,00E-07	3	-
1,00E-07	1,00E-06	2	SIL2
1,00E-06	1,00E-05	1	-

E. Diseñar las funciones de seguridad

En esta etapa se desarrollan las SIF y se verifica el nivel SIL logrado. Si no se alcanza el nivel calculado en el paso 4, se deberá modificar la arquitectura o los componentes. Si no es posible crear una SIF adecuada se deberán redefinir los límites o volver al paso de análisis de riesgos, tal como se ilustra en la Fig. 3.

Cada riego se aborda por separado y se crea un lazo de seguridad. Se define la arquitectura para su mitigación y se calcula su nivel de integridad de la seguridad. El cálculo del SIL se realiza para cada una de las funciones de seguridad independientemente de las otras.

Simplificando la situación general presentada en la Fig. 1, se puede asumir que cada SIF se estructura como se ilustra en la Fig. 6. En ella se observa que una SIF debe disponer de elementos de entrada (sensor), elementos de salida (actuador) y una unidad para el análisis la toma de decisiones (controlador lógico). Según esta estructura la PFDavg será la sumatoria de las probabilidades de falla de cada bloque más la probabilidad de falla de causa común, como se observa en la siguiente expresion:

$$PFDavg = PFDs + PFDc + PFDa + PFDss \quad (5)$$

Generalizando para diferentes arquitecturas o diferentes formas de votación, se tiene [9]:

$$PFDsis \approx \sum PFDsensor + PFDcontrolador + \sum PFDactuador + PFDss \quad (6)$$

La tabla IV muestra el formato de la planilla de cálculo implementada [3] que realiza estos cálculos para cada una de las configuraciones posibles en la entrada y la salida.

Además de definir la probabilidad de falla en demanda, el sistema de seguridad deberá cumplir con requerimientos que posteriormente en el paso 6 deben poder ser verificados. Algunos de estos requerimientos se enumeran a continuación:

- Estado seguro del proceso, ¿Cuál es el estado seguro al cual el sistema será llevado por actuación de la SIF?
- Selección del disparo. Límite máximo admisible en las variables de entrada
- Parada manual. ¿Se debe prever un pulsador de parada segura?

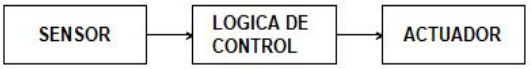

Fig. 6: Estructura simplificada de una función instrumentada de seguridad (SIF)

TABLA IV. CALCULO DEL NIVEL SIL DEL SISTEMA PARA DISTINTAS ARQUITECTURAS DE IMPLEMENTACIÓN

VOTACIÓN	∑PFDs	PFDc	∑PFDa	PFDss	PFDsis	SIL
1oo1						
1oo2						
….						

- Tiempo de respuesta. ¿Existe algún requerimiento especial de velocidad?
- Mantenimiento y prueba. ¿Se implantará un sistema de auto test?
- Separación. ¿El SIS se implementa separado del sistema de control de proceso?
- Redundancia. ¿La arquitectura tiene un nivel de redundancia adecuado?
- Selección de tecnología. ¿Los componentes a utilizar tienen certificación SIL adecuada?

En este paso se indican además los diferentes sensores y actuadores (entradas y salidas), junto con sus correspondientes tasas de fallas obtenidas del manual de cada componente.

En la planilla [3] no se incluye el cálculo del SIL del sistema lógico o controlador. Para ello se requiere el cálculo de la probabilidad de falla en demanda del microcontrolador, memoria y otros componentes. En cambio se toman valores típicos para un controlador lógico programable.

F. Validar el sistema de seguridad funcional

Una vez determinado el SIL objetivo y diseñado el sistema para cumplir con este requisito, el objetivo de esta etapa es el de validar el SIS a los efectos de determinar si cumple con todos los requisitos de seguridad en términos de funciones instrumentadas de seguridad y nivel de integridad de la seguridad asociado.

Esta validación se realiza contrastando el SIL obtenido con el SIL objetivo. En la planilla de calculo propuesta [3] se realiza mediante la tabla V.

G. Documentar el sistema de seguridad funcional

El último paso, que en realidad se debe ir haciendo a medida que se avanza con los distintos pasos, consiste en documentar el proceso de seguridad. Los documentos mínimos a disponer finalizado el desarrollo de las SIF serán:

- Detalle de la metodología de análisis de riesgo.
- Criterios de tolerancia al riesgo adoptada.
- Los supuestos y limitaciones.
- Los peligros identificados, inherentes al sistema.
- Detalle de los subsistemas de seguridad
- Elaborar un caso de seguridad en base al caso generico
- Manuales de mantenimiento y testeo de los dispositivos del SIS

TABLA V. VALIDCIÓN DEL NIVEL SIL OBTENIDOSEGÚN LA ARQUITECTURA DE VOTACIÓN UTILIZADA

	SIL = log10 PFD		SIL = f(RRF)		
VOTA-CIÓN	**PFDsis**	**SIL**	**RRF = 1/PFDsis**	**SIL**	**CONCLU-SIÓN**
1oo1					
1oo2					
…					

IV. CONCLUSIONES

El presente trabajo se presenta una metodología de trabajo para la determinación y verificacion del SIL de las funciones de seguridad, de acuerdo con los estándares de seguridad funcional (IEC 61508).

La metodología utilizada es cuasi-cuantitativa, las matrices de riesgo se basan en criterios de analisis de riesgo claros y las formulas utilizadas se basan en funciones simplificadas por lo que el sistema es dependiente de la experiencia del diseñador.

La planilla de calculo desarrollada [3] es de simple aplicación y proporciona datos confiables por lo que podrá ser utilizada tanto en la enseñanza como en la practica profesional. En este artículo no hay suficiente espacio para publicar ejemplos de uso. Dichos ejemplos serán publicados en [16].

REFERENCIAS

[1] ABB 3AUA0000081820. “Seguridad y seguridad funcional”. Copyright 2010 ABB

[2] R. E. Varela. “Introducción a la Seguridad Funcional”. AADECA, Buenos Aires. Marzo 2007.

[3] S. H. Gallina (2018) Planilla para el calculo de funciones instrumentadas de seguridad (SIF) [Online]. Disponible: https://goo.gl/3FA9pQ

[4] UNE-EN 50126. “Especificacion y demostracion de la fiabilidad, la disponibilidad, la mantenibilidad y la seguridad (RAMS)”. 2005

[5] International Standard IEC 61508-6, . “Functional safety of electrical /electronic/programmable electronic safety-related systems2 – Part 6. Edition 2.0 2010-04

[6] IEC 61511-01:2003. “Functional safety – Safety instrumented systems for the process industry sector”

[7] G. Sosa, M. Krenek. “Diseño E Implementación De Un Sistema De Seguridad De Procesos En Instalaciones Nuevas”. TECNA Estudios y Proyectos de Ingeniería. Capital Federal – Argentina

[8] B. McLendon. “Comprendiendo los niveles de integridad de seguridad (SIL)”. P.E. 2013/06/13.

[9] Galindo Diez, Xavier. “Sistemas instrumentados de seguridad”. Junio 2012.

[10] García Pecsén, Luis. “Sistemas instrumentados de seguridad (SIS)” http://larevistadelgasnatural.osinerg.gob.pe/articulos_recientes/files/archivos/50.pdf

[11] Gastelbondo, W; Tarantino, R; Aranguren, S. “Metodología para el cálculo del nivel integrado de seguridad (SIL), aplicada al caso: estudio de un sistema instrumentado de seguridad (SIS) de nivel en calderas industriales de alta presión”. IIDTA. Universidad de Pamplona. Junio 2008.

[12] Machiavelo Salinas, V. “Determinación del PFDavg (SIL) de un sistema instrumentado de seguridad”. Risk software SA

[13] PILZ. Seguridad funcional mediante EN/IEC 62061 y EN ISO 13849-1 https://es.rs-online.com/es/pdf/Pilz.pdf. Germany © Pilz 2008.

[14] Rodríguez P., Oswaldo A. “Determinación de un sistema instrumentado de seguridad (SIS) y su nivel de integridad de seguridad (SIL)”. Venezuela 2005

[15] Sven Scholz. "Modular Urban Transport Safety and Security Analysis" - Final Conference MODSafe. Cologne. June 2012

[16] S. H. Gallina (2018) Desarrollo de Sistemas E/E/EP Bajo Normas Ferroviarias [Online]. Disponible: https://goo.gl/irdtxP