Desarrollo de sistemas E/E/EP para Sistemas Relacionados con la Seguridad

Sergio H. Gallina[1], Daniel Villagran[2], Marcos Aranda[3], Adrian Laiupa[4]
(1) Departamento de Electrónica, Facultad de Tecnología y Ciencias Aplicadas, UNCa.
sgallina@tecno.unca.edu.ar
(2) Departamento de Electrónica, Facultad de Tecnología y Ciencias Aplicadas, UNCa.
dvillagran@tecno.unca.edu.ar
(3) Departamento de Electrónica, Facultad de Tecnología y Ciencias Aplicadas, UNCa.
maranda@tecno.unca.edu.ar
(4) Departamento Electrónica, Universidad Tecnológica Nacional – Regional Bahía Blanca.
alaiuppa@gmail.com

Fecha de recepción del trabajo: 06/10/2018
Fecha de aceptación del trabajo: 05/12/2018

RESUMEN: Las personas y bienes, cada vez más, dependen del buen funcionamiento de sistemas E/E/EP (eléctricos, electrónicos o electrónicos programables). El aseguramiento de la calidad y la seguridad de estos sistemas han cambiado considerablemente, la ocurrencia de un accidente pasó de ser considerada como una situación normal, a ser inaceptable y perseguido. La sociedad y el cuidado del medioambiente exigen la mitigación de aquellos peligros que lleve asociada nuestra actividad, cualquiera sea esta (usar un cajero bancario – Operar una máquina – Viajar). Por lo dicho es que resulta necesario adoptar medidas en el desarrollo de sistemas, que garanticen una mayor seguridad. En el presente artículo se presentan consideraciones y normativas para ser aplicadas al diseño bajo normas de seguridad funcional.

PALABRAS CLAVE- E/E/EP, Sistemas Críticos, Seguridad funcional, Funciones de seguridad.

DEVELOPMENT OF E / E / EP SYSTEMS FOR SECURITY RELATED SYSTEMS

ABSTRACT: People and goods, increasingly, depend on the good functioning of E / E / EP systems (electrical, electronic or programmable electronic). The assurance of the quality and safety of these systems have changed considerably, the occurrence of an accident went from being considered a normal situation, to being unacceptable and prosecuted. Society and environmental care require mitigation of those dangers associated with our daily activities (using an ATM, operating a machine, travelling). Therefore, in the development of systems, it is necessary to adopt measures that guarantee greater security. This article introduces considerations and regulations to be applied to the design under functional safety standards.

KEYWORDS: E / E / EP, Critical Systems, Functional safety, Safety functions.

1. INTRODUCCIÓN

La norma IEC 61508:2010 "*Seguridad Funcional de Sistemas E/E/EP (Eléctricos/Electrónicos/Electrónicos Programables) Relacionados con la Seguridad*", se basa en el principio fundamental de que existe un proceso que puede suponer un riesgo a la seguridad de las personas, los bienes o al medio ambiente, si algo pudiera ir mal.
La norma da por supuesto que se deben facilitar funciones de seguridad para reducir dichos riesgos. Las funciones de seguridad pueden formar en conjunto un sistema instrumentado de seguridad (SIS), y su diseño y funcionamiento deben estar basados en la evaluación y la comprensión de los riesgos (Rockwell, 2013).
Un objetivo secundario de la norma IEC 61508 es permitir el desarrollo de sistemas E/E/PE relacionados con la seguridad cuando no existan normas de aplicación en el sector. Esta norma ha dado lugar a normas de segundo nivel específicas para diferentes aplicaciones, tales como IEC 62061 Maquinas, ISO 26262 Automóviles, IEC 61511 Procesos, entre otras.

2. RAMS

La sigla RAMS corresponde al acrónimo en inglés de las palabras Fiabilidad, Disponibilidad, Mantenibilidad y Seguridad (Reliability, Availability, Maintainability, and Safety), une cuatro conceptos claves en la gestión de sistemas seguros:

Fiabilidad: asocia a la probabilidad que tiene un elemento de realizar una función requerida dentro de un rango y tiempo. Para el análisis se observará:

- Todos los posibles modos de falla del sistema
- La probabilidad de ocurrencia de estas fallas
- El efecto de la falla sobre la funcionalidad del sistema

Mantenibilidad: indica la probabilidad que, bajo condiciones y procedimientos establecidos, el mantenimiento de un activo se realice en el tiempo esperado. Para el análisis se observarán:

- El tiempo de realización del mantenimiento planeado.
- El tiempo de detección, identificación y localización de defectos
- El tiempo de reparación.

Disponibilidad: corresponde a la probabilidad de que un elemento se encuentre en situación de realizar una función requerida (operativo) durante un periodo de tiempo dado.

Seguridad: vela por evitar cualquier riesgo inaceptable a las personas. Se basan en un conocimiento de:

- Todos los posibles peligros que puedan darse en el sistema
- Las características de cada peligro
- Los fallos de la seguridad
- La operación y el mantenimiento

RAMS representa un indicador, tanto cualitativo como cuantitativo, del grado de confianza que ofrece un sistema para comportarse de acuerdo a la funcionalidad especificada, de forma segura y con una alta disponibilidad.

Tabla 1: RELACIÓN ENTRE EL NIVEL DE INTEGRIDAD DE LA SEGURIDAD Y LA PROBABILIDAD DE FALLA

SIL		PFH (2)
1	$\geq 10^{-2}$ a $< 10^{-1}$	$\geq 10^{-6}$ a $< 10^{-5}$
2	$\geq 10^{-3}$ a $< 10^{-2}$	$\geq 10^{-7}$ a $< 10^{-6}$
3	$\geq 10^{-4}$ a $< 10^{-3}$	$\geq 10^{-8}$ a $< 10^{-7}$
4	$\geq 10^{-5}$ a $< 10^{-4}$	$\geq 10^{-9}$ a $< 10^{-8}$

(1) – PFDavg – Probabilidad de que una función de seguridad falle bajo demanda. (2) PFH - Probabilidad de un fallo peligroso por hora.

3. INTEGRIDAD DE LA SEGURIDAD

Se define como "*La Probabilidad de que un Sistema relacionado con Seguridad realice adecuadamente la totalidad de las Funciones de Seguridad requeridas bajo todas las circunstancias establecidas y durante el Período de Tiempo Especificado*" (Fernández, 2012). La Integridad de la Seguridad viene determinada por la Integridad del Hardware y la Integridad del Software; en el primer caso la IEC61508 establece los fallos del hardware indicando el objetivo a cumplir en función del nivel de integridad de la seguridad buscado (SIL-Safety Integrity Level) Tabla 1.

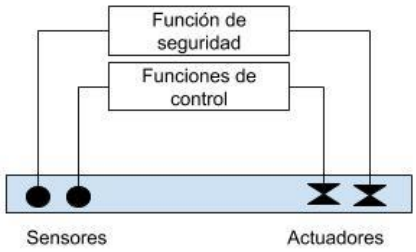


Figura 1: Sistema Instrumentado de Seguridad aplicado a un proceso.

4. SISTEMA INTEGRADO DE SEGURIDAD (SIS) – FUNCIÓN DE SEGURIDAD (SIF)

Una función de seguridad, es una función a ser implementada en un sistema electrónico, eléctrico o electrónico programable (E/E/PE); es una medida que se toma para reducir las probabilidades de que tenga lugar un evento indeseado y haya una exposición al riesgo (ABB, 2010).
Una función instrumentada de seguridad funcional (SIF) es simplemente un lazo de control y contendrá un cierto número de dispositivos y todos esos dispositivos constituyen parte del sistema instrumentado de seguridad (SIS). Un SIS comprende normalmente más de un SIF y esta puede incluir muchos sensores y un único actuador o un sensor y más de un actuador de seguridad. Cualquier combinación es posible.
Las propiedades básicas (Varela, 2007) de las SIF son: Medición; Lógica; Actuación; Tiempo de respuesta; Integridad de la Seguridad; Otras.
Para cada función se deben analizar los siguientes aspectos: ¿Qué hay que proteger? ¿Cómo se hace? ¿Qué variable hay que medir? ¿Sobre qué hay que actuar? ¿Cuándo hay que hacerlo? ¿Cuál debe ser el tiempo de respuesta?
La figura 1 muestra una configuración simple de un sistema instrumentado de seguridad compuesto por una única función de seguridad, relacionado con un proceso.
La función instrumentada de seguridad, implementada independientemente del sistema de control, supervisa determinados parámetros y adopta una acción ejecutiva para que el proceso resulte seguro aun en caso de aparición de fallas.
Una función de seguridad puede actuar bajo demanda o en modo continuo.
La función bajo demanda se caracteriza por:

- En general son independientes del proceso
- Una falla de la función de seguridad tiene como resultado la perdida de protección, pero no es en sí peligroso
- La frecuencia de demanda es baja, generalmente menos de una vez al año

El SIL asignado para estas funciones depende de unas bandas del valor de la probabilidad de falla en demanda (PFD) Tabla 1.

Una función de modo continuo tiene como características:

- Por lo general proporcionan algunas funciones de control
- El fallo de una función de seguridad provoca una situación peligrosa
- La frecuencia de las demandas es alta, más de una vez al año o en forma continua.

Para este tipo de funciones, el cálculo del SIL se realiza mediante la valoración de la probabilidad de falla peligrosa por hora (PFH) Tabla 1.

Como ejemplo de estos tipos podemos ejemplificar: a) los airbags de un vehículo proporcionan una valiosa función de seguridad e interesar conocer su probabilidad de fallo cuando se los demande la ocurrencia de un accidente, lo que indica que se trata de una función en modo a demanda. b) Los frenos de un vehículo, la métrica significativa sería una tasa de fallo o una probabilidad de fallo por hora, lo que es indicativo de que se trata de una función en modo continuo.

4.1. Parámetros de una SIF

Describimos brevemente otros parámetros de una SIF:

- Cobertura de diagnóstico (DC): tasa de fallas detectadas sobre tasa de fallas total

- Falla de causa común: Es la falla del resultado de uno o más eventos, causando fallas coincidentes de dos o más componentes separados conduciendo a la falla del sistema. Es una falla simple que es capaz de producir la falla completa de un sistema redundante. La falla de causa común se expresa a través de "β", la cual indica el porcentaje o fracción del total de fallas que es debido a causa común.

- SFF (Safe Failure Fraction): Fracción de falla segura. Proporción de fallos seguros del número total de fallos. La fracción de todas las tasas de fallas de un equipo que resulta en una falla segura o no segura pero diagnosticada.

$$SFF = 1 - (\lambda du / \lambda) \qquad (1)$$

Donde: λdu: Tasa de fallas peligrosas no detectada
λ: Tasa de falla total

- HFT (Hardware Failure Tolerance): Tolerancia de falla de hardware. Es el máximo número de fallas en un subsistema, resultante de fallas aleatorias de hardware, que pueden ocurrir sin llevar a la SIF a un estado de falla peligroso.

4.2. Especificaciones de integridad

Los requerimientos de nivel de integridad, nivel de confiabilidad de cada función de seguridad servirán para establecer una arquitectura aceptable del sistema para lograr el nivel de desempeño, seguridad e integridad requerida para que efectúe las operaciones necesarias. Los requerimientos de integridad de seguridad deben incluir una definición de los siguientes parámetros:

- La tasa de demanda objetivo, SIL objetivo, para cada una de las funciones de seguridad.
- Una descripción de todas las funciones de seguridad para lograr el SIL objetivo.
- El factor de reducción de riesgos (RRF) para cada función
- Requerimientos de diagnóstico para lograr el SIL objetivo.
- Requerimientos de confiabilidad en caso de presentarse disparos en falso
- Las condiciones ambientales extremas probables a ocurrir durante todo el ciclo de vida.
- Los límites de inmunidad electromagnética requeridos.

5. DISEÑO E IMPLEMENTACIÓN

El diseño y la implementación de sistemas bajo criterios de seguridad funcional es una de las fases del desarrollo de Sistemas Críticos, en esta fase se deben realizar tareas tales como:

- Diseñar los subsistemas que componen el Sistema, con ajuste a las políticas RAMS definidas.
- Demostrar que los subsistemas cumplen con las políticas RAMS definidas.
- Establecer un plan para la instalación.
- Establecer un plan para la operación y mantenimiento.
- Elaborar un caso de seguridad genérico de la aplicación.

5.1. Diseñar

El proceso para diseñar subsistemas que se ajusten a los requisitos RAMS del sistema se debe llevar a cabo después de la especificación de requisitos y de la distribución de esos requisitos en los diferentes subsitemas. Si hacemos una lista de tareas a realizar podríamos encontrar una como la siguiente:

- Definir ciclo de vida de diseño de SW y HW
- Definir la arquitectura de SW del sistema
- Diseñar a alto nivel el SW de los subsistemas
- Modelar el SW de los subsistemas
- Seleccionar los estándares del software.
- Codificación del software.

- Implementar pruebas de validación de subsistemas
- Integrar subsistemas software.
- Validación de integración de software.
- Definir la arquitectura de hardware del sistema
- Especificar la arquitectura de hardware del sistema
- Diseñar a alto nivel de hardware de los subsistemas
- Modelar y sintetizar el hardware de los subsistemas
- Seleccionar la tecnología de semiconductores.
- Desarrollar prototipos de PCB, Gabinete, etc.
- Realizar pruebas de validación de hardware
- Integrar subsistemas hardware-software.
- Realizar pruebas de validación de integración de H-S
- Definir la arquitectura de seguridad funcional
- Seleccionar la arquitectura de la seguridad
- Fabricar los subsistemas de seguridad
- Instalar el sistema de seguridad
- Verificación del SIL del sistema de seguridad

Las tareas no necesariamente se realizan en el orden enumerado, corresponde aquí definir un ciclo de vida para el desarrollo y la implementación. Un modelo podría ser el ciclo mostrado en la figura 2, pudiéndose

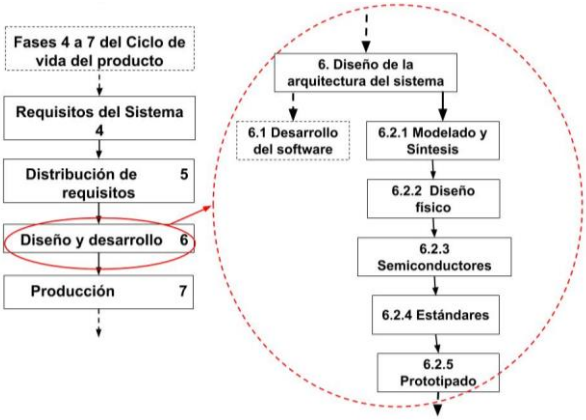


Figura 2: Ciclo de vida del diseño y desarrollo en paralelo del hardware y software. (Fuente: propia)

definir ciclos de vida separados para el diseño del hardware y para el diseño del software.

Muy someramente repasaremos algunos de estos procesos para el sistema, el hardware y el software.
Para el sistema, debemos definir los requerimientos de la arquitectura, del hardware y del software, estos últimos en una descripción de alto nivel.
Para el desarrollo del hardware deberemos trabajar sobre:

- La definición de la tecnología, que podrá variar por ejemplo entre: a) Microprocesadores / Microcontroladores; b) System-on-a-Chip processor (SoC); c) Field Programmable Gate Arrays (FPGA); d) Application-Specific Integrated Circuit (ASIC). e) Digital Signal Processor (DSP)
- El Prototipado de Hardware. Este proceso considera por ejemplo: a) Printed Circuit Board (PCB); b) Construcción del Prototipo; c) Gabinete; d) Verificación y Pruebas

Para el desarrollo del software, se consideran la coexistencia de cuatro componentes: a) Sistema Operativo; b) Middleware; c) Firmware; d) Aplicación.
Para su desarrollo se deberá trabajar sobre: Modelado, Generación de Código, Prototipo, Verificación y Pruebas.
Las normas nos brindan información sobre herramientas y métodos de diseño aceptados o no recomendados. Ponemos a modo de ejemplo las tablas A.2 y A.6 (figura 3) de la norma EN 50128 “sistemas electrónicos relacionados con la seguridad en ferrocarriles”, donde se mencionan métodos de trabajo recomendado o no recomendados.

TÉCNICA/MEDIDA	SIL0	SIL1	SIL2	SIL3	SIL4
1- Métodos formales, incluyendo por ejemplo CCS, CSP, HOL, LOTOS	-	R	R	AR	AR
2- Métodos semi-formales	R	R	R	AR	AR
3- Metodologías estructuradas, incluyendo por ejemplo JSD, MASCOT, SADT, SSADM	R	AR	AR	AR	AR

NOTA: [R] Recomendado [AR] Altamente recomendados

Figura 3: Modelo de tabla de criterios para la selección de técnicas para especificación de requisitos (Fuente: EN-50128)

5.2. Demostrar

El proceso para demostrar que los subsistemas se ajustan a los requisitos RAMS del sistema se describe en la Figura 4.
Durante el diseño del software de aplicación se lo somete a diferentes pruebas con el propósito de eliminar errores que después inhiban al sistema de responder a una demanda.

Las diferentes cuestiones que deben responderse son, al menos:

- ¿La especificación es correcta?
- ¿El programa desarrollado es correcto?
- ¿Las pruebas realizadas son correctas?

Las pruebas de aceptación de fábrica (FAT, Factory Acceptance Test) del sistema lógico y su software asociado tienen como objetivo asegurar que se satisfacen lo requerimientos definidos en las especificaciones de seguridad, antes de su instalación definitiva.

El número de participantes de las pruebas dependerá del tamaño del sistema, pero en términos generales participa el personal involucrado con el diseño y la implementación, debiéndose definir las responsabilidades.

En estas pruebas FAT se debe probar:

• Todo el hardware del sistema lógico, módulos de entrada y salida, terminales, cableado, procesadores, módulos de comunicación, redundancia, interfaz del usuario, etc.

• Software (Sistema Operativo - firmware – aplicación)

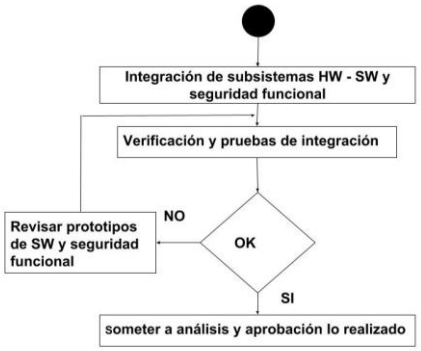


Figura 4: Proceso para la demostración de los requisitos RAMS. (Fuente propia)

Las pruebas deben ser documentadas. Los criterios más usuales (no únicos) para la realización de las pruebas, podemos mencionar:

- Inspección visual
- Inyectar señales de entrada y observar las respuestas del sistema
- Forzar valores de salida analógicos o digitales
- Crear diferentes escenarios de falla para ver las respuestas.
- Simulación lógica para probar la funcionalidad del sistema.

Si durante las pruebas FAT se detectan errores y se requieren modificaciones, se debe estudiar el impacto de estas sobre la integridad del sistema de seguridad y se deberá recalcular la probabilidad de falla en demanda (PFD).

La importancia de realizar unas pruebas de la lógica antes de la instalación, conlleva una serie de beneficios:

- El software y hardware es probado en un ambiente libre de stress.
- Cualquier problema encontrado puede resolverse con más facilidad
- Las pruebas FAT suponen un entrenamiento del personal involucrado en las mismas.
- Se adquiere conocimiento del sistema.

5.3. Verificación del nivel de integridad de seguridad (SIL).

Para cumplir con el SIL objeto no basta con adquirir componentes con el distintivo “SIL certified” y asumir que de este modo se consiga la conformidad predefinida (Rockwell, 2013).

Una propuesta de plan de cara al cumplimiento normativo es la de cumplir con los requisitos de las normas directa o indirectamente relacionadas. Esto incluye verificar (entre otras):

• Requisitos de comportamiento del sistema al detectar un fallo: Debe especificarse el comportamiento del sistema al detectar un fallo.

• Tolerancia a fallos de hardware: Se requiere una evaluación cuantitativa respecto a la fracción de fallos seguros (SFF) y a las restricciones arquitectónicas.

• Selección de componentes y de subsistemas: La selección de componentes y de subsistemas puede basarse en una evaluación de idoneidad.

• Dispositivos de campo: La documentación de especificación debe mostrar que el componente cumple con los requisitos específicos en términos de funcionalidad para todos los procesos y todas las condiciones medioambientales y la especificación de diseño funcional debe confirmar esto en tal caso.

Los sensores inteligentes deben contar con protección frente a escritura para evitar la modificación inadvertida desde una ubicación remota.

• Interfaces del usuario, de mantenimiento y de comunicación con el sistema instrumentado de seguridad: El diseño de la interfaz de comunicación del sistema instrumentado de seguridad debe garantizar que cualquier fallo de esta interfaz no afecte de forma negativa la capacidad del sistema instrumentado de seguridad de llevar el proceso a un estado de seguridad.

La documentación también debe confirmar:

- La tasa de error pronosticada de la red de comunicación;
- Que la comunicación con el sistema básico de control y los periféricos no tenga impacto sobre las funciones instrumentadas de seguridad (SIF);
- Que la interfaz de comunicación sea lo suficientemente robusta para resistir las interferencias electromagnéticas;
- La interfaz de comunicación sea adecuada para la comunicación entre los dispositivos referenciados a distintos potenciales eléctricos de conexión a tierra;
- Requisitos de diseño relativos al mantenimiento o a las pruebas;
- Probabilidad de fallo de las funciones instrumentadas de seguridad;
- Software de aplicación: Se debe verificar y garantizar que:
  - Todas las actividades requeridas para desarrollar el software de aplicación estén definidas;
  - Las herramientas de software que se utilizan para desarrollar y verificar el software de aplicación,

es decir, el software de utilidad este totalmente definido;
- Se ha adoptado un plan para cumplir con los objetivos de seguridad funcional.

Para la verificación del nivel de integridad de la seguridad (SIL) alcanzado en una función de seguridad podemos analizar la misma en función de la Probabilidad de falla bajo demanda o la probabilidad de falla por hora, según sea el caso en estudio.
Para ello nos basaremos en la relación entre SIL – PFD o SIL-PFH.

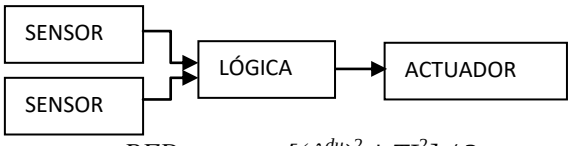
Para el caso de baja demanda se calcula la probabilidad de falla promedio (PFDavg) como:

$$PFD_{avg}=PFD_{sensor}+PFD_{logica}+PFD_{actuador}+PFD_{causa\_comun} \quad (2)$$

Obtenido el valor PFDavg y mediante la Tabla I, obtendremos el valor de SIL alcanzado, esto se coteja con el SIL objetivo o deseado para verificar si se cumple o no con las especificaciones de seguridad.
Para el cálculo del PFD las normas nos dan una serie de ecuaciones dependientes de la arquitectura de votación del sistema. Sin entrar en mayores detalles sobre cómo se llega a estas ecuaciones, en la figura 5 se muestra un ejemplo de ecuaciones simplificadas (ISA 2002) para la arquitectura 1oo2.

5.4. Plan de Instalación

Es necesario que el sistema se instale de forma



$$PFDsensor = [(\lambda^{du})^2 * TI^2] / 3$$

Figura 5: Calculo de la PFD para dos configuraciones de la arquitectura de sensores:

adecuada para evitar un posible fallo común a causa de un cableado indebido, por razones medioambientales o por otros factores. Un sistema de seguridad que no realiza su tarea correctamente por culpa de una instalación deficiente carece de utilidad, e incluso puede llegar a suponer un riesgo (ABB, 2014).
El procedimiento de instalación relacionado con sistemas E/E/PE debe garantizar que se logre la seguridad funcional requerida. Se parte de un plan para la instalación de los sistemas relacionados con la seguridad E/E/PE, donde está especificado:
- El cronograma de instalación;
- Los responsables de las diferentes partes de la instalación;
- Los procedimientos para la instalación;
- La secuencia en que se integran los diversos elementos;
- Procedimientos para la resolución de fallas e incompatibilidades.

El proceso para poner en práctica las tareas de montaje e instalación de los componentes y subsistemas se detallan a continuación mediante una enumeración de tareas secuenciales que definen este proceso.

- Verificar el plan de instalación
- Verificar la puesta a tierra y tensiones disponibles
- Verificar que los dispositivos a instalar estén libres de daño físico
- Montaje e instalación de subsistemas y componentes
- Someter a test de aceptación

La mayoría de los problemas relacionados con la instalación son de sentido común y la técnica más sencilla para evitar problemas es seguir todas las instrucciones de instalación, sin embargo hay formas de minimizar los riesgos y uno de los aspectos más destacados es el de utilizar personal con experiencia comprobada. La norma IEC 61511 proporciona una lista de actividades que deben ser atendidas y que aquí resumimos:

- La conexión a tierra física se haya realizado correctamente.
- Las conexiones de alimentación funcionen correctamente.
- Los embalajes no hayan sido violados
- Los dispositivos están libres de daño físico
- Las conexiones de los sensores y actuadores se realizó tal cual lo indica el diseño.
- Documentar el proceso de instalación.

El proceso para documentar el montaje y la instalación es fundamental para las futuras fases de la vida del sistema. Se describe este proceso como la mera escritura de un informe de instalación, en el mismo se detallarán los problemas encontrados y las soluciones adoptadas.

Además de las tareas mencionadas, el proceso de instalación incluye: revisar y actualizar el plan de seguridad y establecer mecanismos de apoyo a las fases de operación y mantenimiento (capacitar al personal, evaluar métodos y herramientas, entre otros).

5.5. Plan de Mantenimiento

En esta tarea se debe desarrollar un plan de mantenimiento del sistema E/E/EP para asegurar que la seguridad funcional requerida se mantenga durante toda la etapa de operación.

El alcance del mantenimiento, en todas sus variantes, preventivo, correctivo y predictivo, se desarrolla en el correspondiente Plan de Mantenimiento.
Dependiendo de las características del sistema, será necesario definir algunos parámetros tales como:

- Disponibilidad: Es la fracción de tiempo en la que un sistema está operativo en un instante de tiempo.

$$Disponibilidad = MTTF / (MTTF + MTTR) \quad (3)$$

- MTBF (Mean time between failure): Tiempo medio entre dos fallos consecutivos. Medida básica de fiabilidad sobre partes reparables de un equipo, pudiendo ser expresado en horas o año.

$$MTBF = MTTR + MTTF \quad (4)$$

- MTTR (mean time to recover): Tiempo promedio de reparación. Es el valor esperado de la variable aleatoria "tiempo para reparar". Al igual que MTTF, MTTR es típicamente un valor promedio.

- MTTF (mean time to failure); Tiempo promedio para fallar. Es el índice que señala el "tiempo promedio de falla" de un dispositivo. Es la evaluación de la integral de la función de confiabilidad R(t).

$$MTTF = E(t) = \int_0^{(+\infty)} R(t)\, dt \quad (5)$$

$$R(t) = e^{(-\lambda t)} \qquad MTTF = \int_0^{(+\infty)} e^{(-\lambda t)}\, dt$$

$$MTTF = -(1/\lambda)\, [e^{(-\lambda t)}] = 1/\lambda. \quad (6)$$

Para una correcta tarea de mantenimiento es imprescindible la redacción e implantación de un Protocolo de Actuación en caso de averías. La rápida actuación, la eficacia en la coordinación de las diversas partes implicadas y la optimización de recursos disponibles son los puntos de referencia para el desarrollo del plan de mantenimiento.

5.6. Caso de seguridad

Un caso de seguridad es la demostración documentada de que un producto cumple con los requisitos de seguridad especificados (EN 50126, 2005).

El caso de seguridad es un documento estructurado para demostrar o evidenciar la seguridad de un producto genérico, una aplicación genérica o específica. Es necesario cuando un peligro no puede ser corregido de inmediato y un análisis deberá demostrar si el riesgo es aceptable. En caso contrario, se demostrará que con una solución alternativa mantendrá el nivel de seguridad operacional dentro de los límites aceptables y no afectará excesivamente la capacidad operacional del sistema o producto.

En base a las consideraciones previas, un Caso de Seguridad, abarcando los siguientes aspectos:

- Evidencia de la gestión de la calidad.
- Evidencia de la gestión de la seguridad.
- Evidencia de la seguridad técnica y funcional.

Los casos de seguridad son evidencias documentales que indican que se han cumplido las normas, procedimientos y requisitos asociados al proyecto bajo revisión. Esta evidencia se prepara con el fin de ser presentada a la autoridad ferroviaria competente para obtener la aprobación de la seguridad de un producto genérico.

Los casos de seguridad se estructuran en 6 partes según el siguiente detalle:

Parte 1: Definición del Sistema (o Subsistema o equipo)
Parte 2: Informe sobre la gestión de la calidad
Parte 3: Informe sobre la gestión de la seguridad
Parte 4: Caso de seguridad técnica
Parte 5: Referencia a informes de seguridad
Parte 6: Conclusiones.

La extensión del documento no permite extenderse sobre las diferentes partes del caso de seguridad. Haremos un resumen respecto de las conclusiones que deben realizarse al finalizar el caso de seguridad y para ello nos valdremos de la figura 6, donde se muestra una secuencia de diferentes conclusiones parciales y la conclusión final de cierre del caso de seguridad

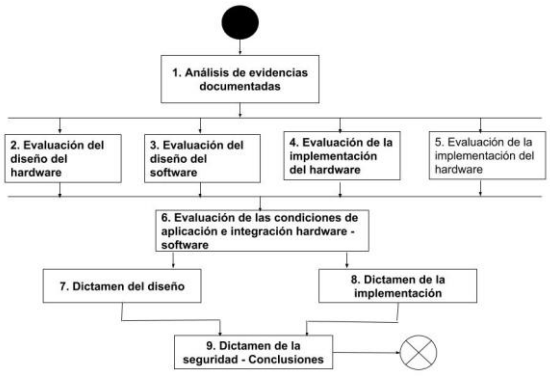


Figura 6: Conclusiones en un caso de seguridad (Fuente: propia)

6. CONCLUSIONES

El presente trabajo muestra una secuencia completa de pasos para el desarrollo de sistemas E/E/EP relacionados con la seguridad, constituyendo un documento que permitirá a quienes se inician en el desarrollo de estos sistemas, tener una visión general de los trabajos a realizar y una secuencia lógica en los pasos.

Siguiendo la secuencia descripta, se lograra el desarrollo de sistemas que mitiguen los peligros innerentes al sistema y se garantizar seguridad para personas y bienes.

La profundización en el entendimiento de las ecuaciones matemáticas y los procesos, requerirá del lector remitirse a las normas de referencia y a bibliográfica especifica relacionada con la temática.

REFERENCIAS

ABB Guía Técnica N°10 "*Seguridad Funcional*". 2014.

ABB. "*Seguridad y seguridad funcional*". Folleto 3AUA0000081820. © Copyright 2010 ABB

EN 50126 "*Especificación y demostración de la fiabilidad, la disponibilidad, la mantenibilidad y la seguridad (RAMS)*" 2005.

Fernández I.; Camacho A.; Gasco C. y otros. "*Sistema Instrumentado de seguridad y análisis SIL*" Ediciones Diaz de Santos. Madrid ISBN 978-84-9969-210-4 Año de publicación 2012 http://literature.rockwellautomation.com/idc/groups/literature/documents/rm/safebk-rm003_-es-p.pdf

ISA (Instrumentation,Systems, andAutomation Society). *Safety Instrumented Functions (SIF) - Safety Integrity Level (SIL) Evaluation Techniques Part 2: Determining the SIL of a SIF via Simplified Equations*. Technical Report Part 2. 2002

Rockwell. "*Manual De Seguridad De Procesos 1- Seguridad funcional en la industria de proceso*" Marzo 2013.

Varela, Roberto E. "Introducción a la Seguridad Funcional". AADECA, 2007.

NOTA: Mayor información se podrá ver en el sitio WEB https://sites.google.com/tecno.unca.edu.ar/sistemas-ferroviarios-e-e-ep/p%C3%A1gina-principal