El análisis de RAMS (Reliability, Availability, Maintainability & Safety) y la CEM (Compatibilidad Electromagnética)

leedeo ENGINEERING
www.leedeo.es

CEMDAL
www.cemdal.com

Autor: Francesc Daura Luna, Ingeniero Industrial. Director de la Consultoría Leedeo Engineering

La ingeniería basada en análisis RAMS (Reliability, Availability, Maintainability & Safety: fiabilidad, disponibilidad, mantenibilidad y seguridad) es una de las técnicas que mayor interés y auge está viviendo en los últimos años. Su uso e implantación en los departamentos técnicos y de calidad de los sectores ferroviario, aviónica, automoción y náutico, permite el diseño y análisis de equipos o sistemas complejos en términos de seguridad y disponibilidad. El análisis RAMS se realiza a nivel de sistema considerando todos los componentes de forma holística, por lo que en RAMS pueden converger mecánica, electricidad, química, electrónica, software, firmware, etc. De este modo, la ingeniería RAMS, con su análisis y metodología, persigue analizar y predecir de forma cualitativa y/o cuantitativa la capacidad de un sistema, instalación o equipo para desempeñar correctamente su actividad y sus funciones para las que ha sido diseñado y fabricado, a nivel técnico, logístico y económico.

El reto de la ingeniería RAMS es encontrar el balance entre la seguridad del sistema y su disponibilidad para funcionar ya que, por norma general, ambos conceptos van en detrimento el uno del otro. A modo de ejemplo simplificado, podríamos decir que, a más seguridad, más mantenimiento y a más mantenimiento, menos disponibilidad del sistema. Esto significa que un buen análisis RAMS puede tener implicaciones económicas importantes de cara a la viabilidad de un producto o sistema.

Así, dentro del ejercicio de encontrar dicho balance, la ingeniería RAMS analiza los sistemas de forma transversal. Y esto incluye el estudio de los parámetros de compatibilidad electromagnética (CEM) del sistema. Los ingenieros RAMS están cada vez más concienciados sobre la necesidad de estudiar la CEM en los sistemas, por lo que se trata de un tema de creciente interés dentro de la disciplina.

Las interferencias electromagnéticas (EMI) son amenazas que afectan la fiabilidad, la disponibilidad y la seguridad de los sistemas de señalización ferroviaria, los ferrocarriles, los aviones y los automóviles, sin olvidar la náutica y la electromedicina. En consecuencia, la identificación de los requisitos de fiabilidad, seguridad y disponibilidad, que dependen de las condiciones ambientales, es un problema importante para los diseñadores de sistemas electrónicos y, por lo tanto, para los evaluadores y los organismos de prueba y certificación. Los requisitos de fiabilidad y seguridad se establecen a consecuencia del entorno electromagnético (EM), es decir, a los campos radiados y conducidos, que son una combinación de todas las amenazas EM circundantes de un sistema electrónico. Así, la CEM afecta a los requisitos de fiabilidad y seguridad de un equipo, sistema o instalación.

Los equipos electrónicos que pueden ser críticos desde el punto de vista de RAMS dependen del estudio de los aspectos funcional, térmico, mecánico y de la CEM. La variación de algún aspecto podría resultar en un incumplimiento de los requisitos de fiabilidad, disponibilidad y seguridad. Tradicionalmente, los problemas térmicos o de CEM solo se consideraban una vez que se terminaba el diseño del equipo o instalación. Hoy en día este proceder es desaconsejable.

El estudio RAMS promueve aplicar metodologías para evaluar de antemano, en la medida de lo posible, la afectación que puede tener el mal funcionamiento de un subsistema o equipo sobre el sistema completo. Para ello, el análisis se basa en la definición de "amenazas", definiéndose éstas como "escenarios que pueden llevar potencialmente a un accidente". Asimismo, una posible amenaza a considerar para un sistema podría ser la "Existencia de perturbaciones CEM sobre el sistema/subsistema/equipo/instalación".

Los requisitos y los parámetros de diseño de cada área y la relación entre ellos se definen cualitativa y/o cuantitativamente, dependiendo del proyecto. En base a estas dependencias entre todas las áreas, se demuestra la influencia cruzada de cada variación de parámetros en los requisitos de otras áreas. Los resultados obtenidos están destinados a ayudar al cumplimiento de los requisitos del diseño de cualquier equipo crítico para la seguridad y a ayudar a los diseñadores a conocer de antemano las consecuencias de cualquier cambio

Safety Integrity Level (SIL)	Probabilidad promedio de un fallo peligroso por hora	Tiempo medio equivalente a un fallo peligroso en horas	Factor de confianza requerido por cada 10.000 horas de funcionamiento continuo
4	$\geq 10^{-9}$ a $<10^{-8}$	$>10^{8}$ a $\leq 10^{9}$	99,99 a 99,999%
3	$\geq 10^{-8}$ a $<10^{-7}$	$>10^{7}$ a $\leq 10^{8}$	99,9 a 99,99%
2	$\geq 10^{-7}$ a $<10^{-6}$	$>10^{6}$ a $\leq 10^{7}$	99% a 99,9%
1	$\geq 10^{-6}$ a $<10^{-5}$	$>10^{4}$ a $\leq 10^{5}$	90 a 99%

Figura 1. Los niveles de seguridad SIL. Probabilidad de fallo en modo continuo.

en el diseño, ahorrando tiempo y dinero. Para la prevención de fallos sistemáticos, se debe recurrir a la identificación y aplicación de normas de CEM correspondientes que prevengan el mal diseño de los sistemas desde un punto de vista CEM. Sin embargo, para el estudio de los fallos aleatorios se debe recurrir a un análisis probabilístico de la ocurrencia de dichos fallos. Cabe destacar la importancia de haber identificado pues dichos fallos de forma correcta y exhaustiva. Como ejemplo, se muestra la aplicación de esta metodología en una radio de comunicaciones de seguridad en un ferrocarril. Esta radio tiene el requisito de tener un nivel SIL 2 relacionado con sus funcionalidades de transmisión, y se expone el empeoramiento de este requisito en función de la CEM.

Una vez determinado que la CEM es importante desde un punto de vista RAMS, se debe tener en cuenta cómo abordar el problema. Lo primero será analizar los fallos en el sistema que pueden conllevar la presencia de perturbaciones EM. Para ello, desde el punto de vista RAMS pueden usarse diferentes estrategias, siendo la más extendida (a modo subjetivo) la realización de un estudio FMECA (Failure Mode and Effect Critical Analysis) (AMFEC: Análisis de los Modos de Fallo, sus Efectos y Criticidad). Una vez definidos dichos posibles fallos, se deberá tratar de asegurar, en la medida de lo posible, que no ocurran. Para ello hay que tener en cuenta que existen dos tipos de fallo:

- Un fallo aleatorio es aquel que puede preverse mediante una probabilidad estadística.
- Un fallo sistemático, en cambio, ocurrirá siempre que se cumplan ciertas condiciones en el sistema.

Para el estudio de la CEM cabe considerar ambos tipos de fallo, ya que por un lado un mal diseño puede hacer incurrir el sistema sistemáticamente en un problema de CEM… pero también es posible que ciertos fallos aleatorios desencadenen dicha reacción.

El nivel SIL

El nivel SIL (Safety Integrity Level: Nivel de Integridad de Seguridad) se define como el nivel relativo de reducción del riesgo que proporciona una función de seguridad. Es una medida de la seguridad de un determinado dispositivo electrónico o sistema completo. Dentro de un mismo sistema podemos encontrar distintos niveles de seguridad. La asociación de una función a un determinado nivel SIL, está basada en un análisis denominado análisis de riesgos. Hay cuatro niveles SIL, cada uno correspondiente a un rango de probabilidades de ocurrencia, como se muestra en la figura 1 que indican cuales son las probabilidades permitidas de fallo dependiendo de la frecuencia de utilización de las funciones en modo continuo. La probabilidad de ocurrencia permitida para una función que se utiliza de forma constante es mucho más baja que para otra función cuya frecuencia de utilización es muy baja. Los componentes con un uso irregular se denominan como "baja demanda", y son tratados en la norma IEC 61508.

El concepto SIL se aplica a diferentes funciones de seguridad en un mismo sistema completo que incluye electrónica, electromecánica y mecánica. Generalmente, tratar de anticipar los ratios de incidencia de las EMI, es inapropiado cuando se trata de lograr un determinado nivel SIL. Por ejemplo, incluso si una EMI en particular sucede una vez cada diez años en promedio, el nivel SIL corresponde al nivel de confianza en que la función de seguridad resistirá esta EMI sin fallar, siempre que suceda.

Los sistemas

Los sistemas de señalización, comunicación y control son parte de los sistemas críticos para la seguridad incluidos en varios medios de transporte, como aviones, barcos, trenes y automóviles. Generalmente, desde la perspectiva del diseño, hay tres áreas clave a considerar en el proceso de diseño de la seguridad de sistemas críticos: funcionalidad, temperatura y CEM.

En los sistemas críticos de fiabilidad y seguridad, deben incluirse los requisitos de temperatura y CEM Las tres áreas deben considerarse en paralelo, avanzando en la misma dirección; considerando de los requisitos multidisciplinarios y su cumplimiento de manera controlada. El objetivo principal es establecer una metodología de diseño para definir y cuantificar la relación entre los parámetros y requisitos de diseño RAMS con las características funcionales, térmicas y CEM (figura 2).

La funcionalidad de un sistema electrónico puede verse afectada por la CEM y por la temperatura. Estos parámetros se identifican en este artículo por el acrónimo FCT (Funcionalidad, CEM, Temperatura). El término FCT → RAMS está relacionado con los parámetros de diseño de las áreas FCT y el análisis de los requisitos de RAMS, mientras que el término RAMS → FCT se relaciona con los parámetros de diseño de los requisitos RAMS y el análisis de requisitos FCT.

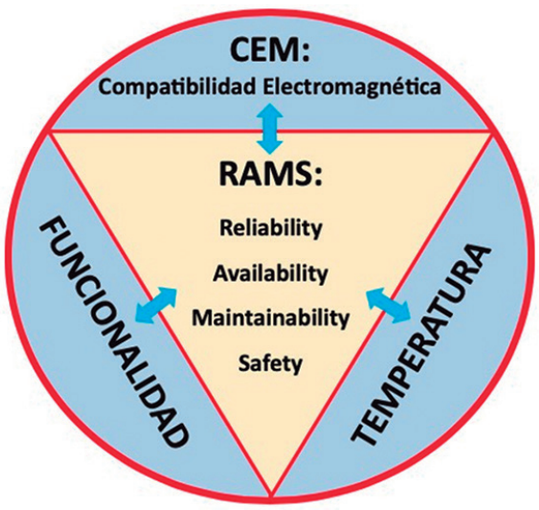

Figura 2. Relaciones entre las características de RAMS, la compatibilidad electromagnética, la funcionalidad y la temperatura.

Diseño de parámetros y requisitos

El estudio de los fallos de un sistema debe conllevar tomar medidas de contención para que éstos no sucedan. Dichas medidas de contención se trasladan al sistema en forma de requisitos. En caso de que ciertos fallos sean críticos para la seguridad o disponibilidad del sistema, es posible que sea necesario incurrir en la definición de requisitos de fiabilidad y seguridad. Dichos requisitos pueden hacer referencia (a modo de ejemplo) a la demostración de que un determinado equipo tenga una probabilidad de fallar (tasa de fallo) inferior a un cierto valor, por ejemplo 10^{-5} fallos/h.

Para obtener la relación entre los parámetros funcionales, térmicos, de CEM y RAMS, primero es necesario definir los requisitos del sistema y los parámetros de diseño de cualquier equipo. El requisito de fiabilidad es el tiempo medio hasta el fallo (MTTF: Mean Time To Failure). Es la media aritmética entre fallos de un sistema y es el tiempo en que el sistema está activo, cumpliendo las funcionalidades por las cuales ha sido diseñado.

El requisito de seguridad se define como la tasa de riesgo tolerable (THR: Tolerable Hazard Rate). Los dos parámetros de diseño RAMS son la tasa de fallo de los componentes y el uso de técnicas de mejora de seguridad, como define por ejemplo la norma EN 50129 (Adaptación de la IEC 61508 a electrónicas de señalización ferroviarias). Dos de estas técnicas son la auto-prueba integrada y la redundancia. La auto-prueba integrada es un proceso que permite a un sistema hacerse una prueba a si mismo para tener alta fiabilidad y menores tiempos de ciclo de reparación. La auto-prueba integrada reduce la complejidad de la configuración de la prueba, al reducir la cantidad de señales de E / S que se deben examinar. La auto-prueba integrada agrega un parámetro adicional para el diseño: el tiempo medio de detección del fallo (MDT: Mean Detection Time: tiempo medio de detección) y, evidentemente, deben considerarse los datos de fiabilidad de los componentes de la topología agregada.

Los parámetros y requisitos funcionales dependen en gran medida del tipo de equipo diseñado. El parámetro de diseño que más afecta a la fiabilidad es la arquitectura térmica del equipo. Los requisitos son las temperaturas ambiente máxima y mínima de funcionamiento. Los requisitos de CEM se dividen en inmunidad y emisiones. Los límites de las emisiones y los parámetros de inmunidad se definen en las normas de CEM correspondientes. Las mejoras de diseño de CEM consisten en la inserción de componentes, como filtros y otras técnicas como el buen diseño del circuito impreso y el cableado.

El análisis RAMS define la relación entre los parámetros RAMS y los requisitos comentados. En la mayoría de los casos, el transmisor o el receptor de la radio de seguridad del tren consta de una cadena principal y se supone que un solo fallo causa un fallo en el sistema completo. El requisito de fiabilidad MTTF es inversamente proporcional a esta tasa de fallo (fallos/h).

Análisis FCT → RAMS y RAMS → FCT

Recordar el significado de acrónimo FCT (Funcionalidad, CEM, Temperatura). Una vez que se definen todos los requisitos, la primera etapa en el diseño del sistema es la definición de la arquitectura para cumplir con los requisitos funcionales.

La funcionalidad del sistema se puede lograr mediante diferentes arquitecturas. La tasa de fallo del sistema depende de la tasa de fallo de cada uno de sus componentes. Esta información se puede obtener de los fabricantes o de las bases de datos de fiabilidad en la norma MIL-HDBK-217F, entre otras. Estos valores proporcionan la información para saber si el equipo cumple con los requisitos de RAMS.

Los problemas térmicos también afectan a los requisitos de RAMS del sistema porque, dependiendo de la temperatura de funcionamiento de los componentes, su tasa de fallo varía. La tasa de fallo de un componente semiconductor depende exponencialmente de la temperatura de la unión de silicio. Por ello es necesario usar disipadores de calor de forma adecuada.

Una posible solución desde el punto de vista de la arquitectura es añadir redundancia. Para cumplir con los requisitos de CEM, las interferencias deben eliminarse mediante la inclusión de componentes adicionales. Se necesitan protecciones y filtros contra las descargas electrostáticas (ESD) y sobretensiones externas en todos los conectores externos del sistema. La inserción de estos componentes empeora el sistema MTTF.

Es crucial saber que las variaciones debidas a los aspectos de RAMS afectan a las características del sistema con respecto al rendimiento de FCT (RAMS → FCT). Los cambios orientados a la mejora de la seguridad no deben variar la funcionalidad principal del sistema, pero las características de los bloques del sistema pueden variar si la nueva arquitectura los necesita. Hay dos posibilidades para mejorar la seguridad del sistema: la auto-prueba integrada y la redundancia. Ambas técnicas afectan al consumo y a la potencia de la señal de RF transmitida por la radio.

La necesidad de incluir componentes en la cadena del transmisor da como resultado una reducción de la potencia transmitida. Por lo tanto, las características del equipo deben cambiarse para obtener la misma potencia de salida que en ausencia de estas mejoras. La auto-prueba integrada o la redundancia implican

			Requisitos RAM	
			THR	MTTF
Funcionalidad	Arquitectura elegida		⇩	⇩
CEM	Filtros	+	⇩	⇩
	Condensadores	+	⇩	⇩
	Protecciones contra ESD	+	⇩	⇩

Figura 3. Efecto de los requerimientos de RAMS. Las columnas muestran los requisitos y las filas definen los parámetros de diseño. La tendencia de los parámetros se define mediante el símbolo +. El símbolo ⇩ en las columnas muestra el empeoramiento del requisito.

	MTTF (horas)
Tx a 25º C	$3{,}66 \cdot 10^6$
Tx a 50º C	$7{,}54 \cdot 10^5$
Tx a 50º C + CEM	$6{,}59 \cdot 10^5$
Tx a 50º C + CEM + BIST	$6{,}56 \cdot 10^5$

Figura 4. Datos de confiabilidad (realiability) para cuatro casos. Tx: Transmisor.

la inserción de nuevos componentes en el sistema y, por lo tanto, nuevas señales. Estas señales pueden generar dos tipos de problemas de CEM: EMI en el entorno electromagnético y EMI en los componentes del sistema; ambos deben ser evitados.

Resultados del análisis RAMS

Una vez que se han analizado las causas y las consecuencias entre las características FCT y RAMS, se recopilan los resultados de los análisis RAMS → FCT y FCT → RAMS. La figura 3 muestra las tendencias FCT → RAMS centradas en la CEM y la funcionalidad. En el caso de la tecnología de la auto-prueba integrada, la disminución del MDT (parámetro cuantificable) mejora el THR, pero, al mismo tiempo, el uso de nuevos componentes (no cuantificables) empeora algunos requisitos. El sistema MTTF es inversamente proporcional a la suma de la tasa de fallo de los componentes. Por lo tanto, cuanto menor sea la tasa de fallo de los componentes de la auto-prueba integrada y la CEM, menor será su efecto en el sistema MTTF.

Aunque estos componentes generalmente tienen una tasa de fallo muy baja, la tasa de fallo de los componentes incluidos en el sistema se agrega directamente a la tasa de fallo del sistema. Entonces, debe considerarse un equilibrio entre la tasa de fallo de los componentes usados y el MDT.

Radio de comunicaciones de seguridad

La metodología, basada en el estudio funcional, térmico de CEM y RAMS desde el principio, se aplica al diseño de un transmisor de RF, con funcionalidades SIL 2. Como ejemplo veamos una radio de comunicaciones de seguridad para un sistema de señalización ubicado en un tren de alta velocidad (ejemplo tomado a nivel de datos del artículo 1 de la lista de referencias). Los requisitos de RAMS están definidos por los requisitos de seguridad ferroviaria. El límite mínimo de MTTF se define como 5×10^5 horas. Mientras que el requisito de seguridad del transmisor viene dado por el THR relacionado con el fallo de la funcionalidad relacionada con la seguridad. Este THR para el transmisor es $2{,}2 \times 10^{-8}$ fallos hora.

Resultados del análisis FCT → RAMS

La arquitectura básica del transmisor en la radio se basa en un generador de señal y diferentes etapas de amplificación. Mediante la tasa de fallo de cada componente a 25ºC y un nivel de confianza del 60%, se puede obtener el cálculo de los datos de fiabilidad. La arquitectura propuesta (primera línea de la figura 4) cumple con el requisito del MTTF.

Las condiciones ambientales de temperatura empeoran los datos de fiabilidad, como se muestra en la segunda línea de la misma figura 4. Además, otro efecto que debe incluirse en los cálculos de RAMS es la inclusión de los componentes para mitigar las EMI. El efecto de estos componentes se muestra en la tercera línea de figura 4, donde el MTTF es un 12,5% peor. Debido a esta razón, se introduce la auto-prueba integrada (la tasa de ocurrencia de peligro es de 400 veces por hora y el MDT usado es de 40 ms (cuarta línea de la figura 4). Ambos requisitos se cumplen, aunque el MTTF es ligeramente peor. Todos los valores cumplen el requisito, pero el MTTF disminuye con el aumento de temperatura, la auto-prueba integrada y la CEM.

Resultados del análisis RAMS → FCT

Desde el punto de vista del análisis RAMS → FCT, la técnica de la auto-prueba integrada implica la inserción de un detector de potencia, que genera una pérdida de potencia. Por lo tanto, es necesario aumentar la potencia de salida. El consumo de energía aumenta debido a los componentes añadidos. Las características térmicas de los componentes añadidos incluidos no cambian significativamente porque el aumento del consumo de potencia es bajo. La última consecuencia de la técnica de la auto-prueba integrada es la variación de las características de CEM. La autocomprobación se realiza mediante sistemas digitales, que pueden alterar el funcionamiento del transmisor. Para evitar cualquier mal funcionamiento, se deben incluir los filtros de CEM necesarios.

La seguridad funcional

Las directivas de seguridad de la Unión Europea con respecto al mar-

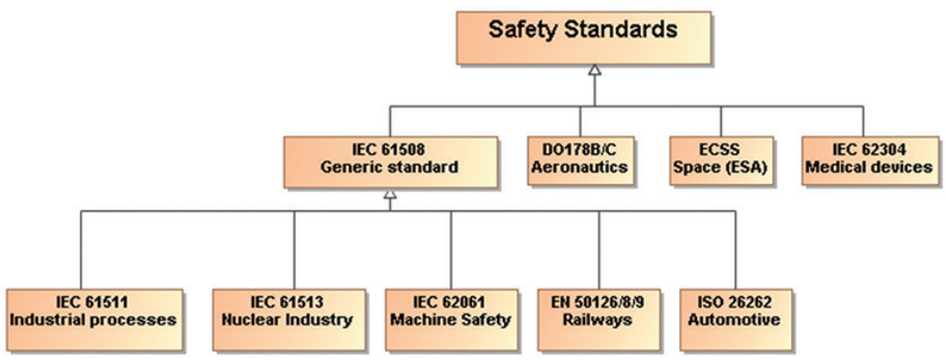

Figura 5. Normas de seguridad.

Figura 6. Incremento de los riesgos en un sistema complejo debido a las EMI.

cado CE son directivas de "seguridad total", lo que significa que cubren todos los problemas de seguridad funcional causados por las EMI, pero no dicen cómo se debe lograr esto. La directiva de CEM y sus normas o el Reglamento 10 de automoción no cubren problemas de seguridad y la norma IEC 61508 (norma IEC básica para la seguridad funcional en sistemas eléctricos / electrónicos) requiere que se tenga en cuenta la CEM, pero tampoco dice cómo debe hacerse. La figura 5 muestra un árbol de relación de las normas derivadas de la norma IEC 61508. Por lo tanto, es importante que la comunidad de expertos de CEM se acerque a la comunidad de expertos de seguridad funcional y viceversa.

El término seguridad funcional se define como: "Seguridad de que la función del sistema no causa ningún estado de peligro intolerable", lo que implica que el sistema debe ser a prueba de fallos. Hasta ahora, la norma IEC 61508 ha sido la única norma disponible para la prueba de seguridad funcional de un sistema. Sin embargo, el uso de la norma IEC 61508 no está totalmente libre de problemas. Algunos de los inconvenientes al emplearla son:

- El ciclo de vida de seguridad (secuencia de fases que proporcionan una ruta lógica a través de la puesta en marcha, operación, mantenimiento y finalmente desmantelamiento) está diseñado para la industria de procesos y automatización.
- El diseño y prueba de sistemas embebidos no se trata muy a fondo en la norma IEC 61508.
- Muchos de los componentes electrónicos en la industria solo están disponibles por un corto tiempo, lo que hace que sea difícil encontrar datos probabilísticos para una prueba de seguridad antes del inicio de la producción.

Una estrategia de seguridad debe considerar no solo todos los elementos dentro de un sistema individual sino también todos los aspectos relacionados con la seguridad de los sistemas que componen la funcionalidad. Todas las tecnologías electrónicas son inherentemente propensas al mal funcionamiento por imprecisión, mal funcionamiento o incluso daños permanentes cuando están afectados por EMI en sus entornos EM operativos.

Los circuitos integrados digitales actuales van disminuyendo sus tiempos de conmutación y aumentando su ancho de banda en frecuencia. Su nivel de integración obliga a disminuir las tensiones de alimentación, disminuyendo así el margen de ruido. En consecuencia, tienen más emisiones y más susceptibilidad. Los fabricantes que emplean dispositivos electrónicos en sistemas críticos de seguridad han tenido pocas normas y regulaciones y, dado que muchos de ellos apuntan al menor costo posible y al cumplimiento de los requisitos reglamentarios mínimos, los problemas de seguridad funcional son cada vez más probables, como se muestra en la figura 6.

La norma IEC / TS 61000-1-2 es una norma que cubre la CEM para la seguridad funcional, proporcionando los requisitos de CEM que faltan en la norma IEC 61508. Esta norma usa el enfoque de los peligros y los riesgos basada en la evaluación. Las pruebas de CEM son inadecuadas cuando se usan como el único medio para demostrar que se ha logrado un nivel aceptable de rendimiento de seguridad funcional relacionado con la CEM.

La CEM de los equipos ha sido tradicionalmente verificada probando usualmente una sola muestra de un nuevo producto. El rendimiento de seguridad de los equipos se verifica tradicionalmente por medios muy diferentes:

- El diseño se inspecciona según una serie de criterios de diseño de seguridad, probados para proporcionar un nivel suficiente de protección durante el ciclo de vida previsto, teniendo en cuenta del entorno físico (por ejemplo, temperatura y vibración) y un uso razonablemente previsible.
- Las muestras se prueban para ver si un fallo único previsible puede resultar en una condición peligrosa ("seguridad de fallo único").
- Cada elemento del equipo que se fabrica se somete a pruebas básicas que verifican si las piezas defectuosas o el montaje incorrecto han socavado las características básicas de seguridad diseñadas.

Claramente, el enfoque tradicional del conjunto de pruebas de CEM (doméstico, comercial, industrial, automotriz, ferroviario, marítimo, aeroespacial, médico o militar) es bastante diferente del enfoque adoptado por el enfoque de la seguridad. Las pruebas de inmunidad solo cubren una perturbación EM a la vez. En la vida real y en funcionamiento normal, el equipo está sujeto a una serie de EMI simultáneamente, por ejemplo: campos radiados de dos o más transmisores que transmiten simultáneamente; un campo radiante continuo más una ráfaga de transito-

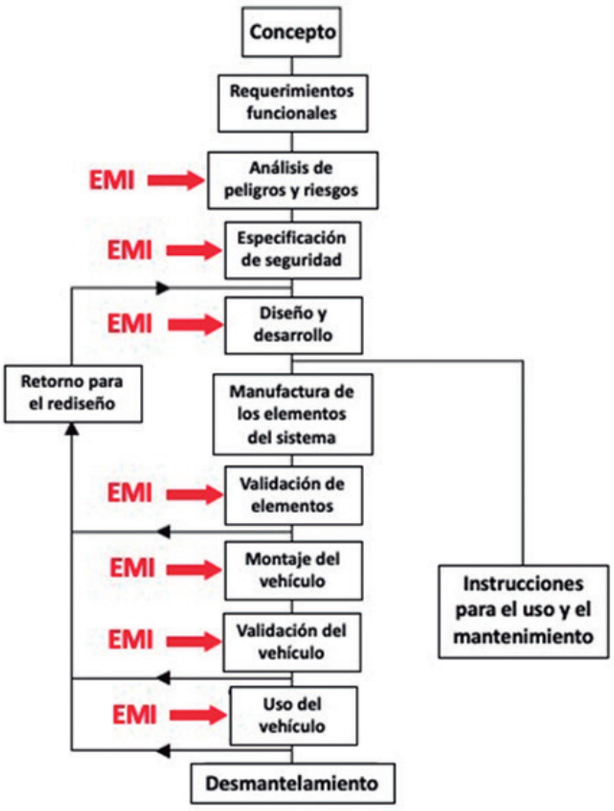

Figura 7. Ciclo de vida de seguridad.

rios rápidos o descargas electrostáticas. Las perturbaciones simultáneas de radiofrecuencia pueden causar problemas inesperados de EMI más exóticos, al intermodular dentro de los dispositivos electrónicos.

CEM y seguridad funcional

Las normas utilizadas como marco para las pruebas de CEM solo intentan cubrir un entorno EM típico y no cubren las EMI de baja probabilidad, que podrían afectar a la seguridad funcional del equipo o instalación. Por lo tanto, es importante hacer un análisis de riesgo de CEM para descubrir a qué tipo de EMI podría estar expuesto el equipo.

Además, no hay exigencias para probar la inmunidad de un vehículo cuando hay fallos eléctricos comunes en su interior. Estos fallos podrían ser, por ejemplo, un cortocircuito en un filtro, fijaciones sueltas en un blindaje o una junta conductora faltante o deteriorada. Los mazos de cables en los vehículos, los trenes y las instalaciones son sistemas que pueden funcionar como emisores de EMI o ser sensibles a las perturbaciones externas.

Si una prueba de inmunidad debe ser incluida en una norma de CEM o en una norma de seguridad depende del criterio de aprobación. La prueba debe ser incluida en una norma de CEM si se requiere que durante o después de la prueba, el vehículo o el equipo debe continuar funcionando según lo previsto. Si se requiere que no ocurran situaciones inseguras (pero el rendimiento puede verse degradado incidental o permanentemente) durante o después de la prueba, la prueba debe incluirse en una norma de seguridad.

CEM en el ciclo de vida de seguridad

El marco de una norma de seguridad que incluya todas las actividades de seguridad desde la fase conceptual hasta el desmantelamiento del equipo, vehículo o tren es el ciclo de vida de la seguridad. En el ciclo de vida de seguridad, el análisis de seguridad es la base para la especificación de los requisitos de seguridad. La validación de la seguridad se realiza antes de la puesta en servicio. Para lograr la seguridad funcional, los aspectos de CEM deben considerarse a lo largo del ciclo de vida del equipo. En la figura 7 se muestra un ciclo de vida de seguridad para un vehículo

Las acciones específicas que deben llevarse a cabo en el ciclo de vida de la seguridad para lograr la seguridad funcional con respecto a las influencias de las EMI comienzan con una definición de la estructura, el diseño y las funciones previstas de un equipo. Entonces es importante describir el entorno EM relevante. Hay algunos fenómenos EM s que ocurren con poca frecuencia, que no se mencionan en las normas, pero deben considerarse en algunos casos. Un ejemplo de tales fenómenos son las perturbaciones conducidas o radiadas en el rango de frecuencia por debajo de los 150 kHz.

Cuando se describe el entorno EM, la seguridad se debe especificar en los requisitos y también los criterios de fallo. En primer lugar, la seguridad funcional de un equipo en el sistema en sí no se verá afectada indebidamente por el entorno EM en el lugar donde se utiliza el equipo. En segundo lugar, cualquier perturbación electromagnética generada en un sistema no afectará indebidamente la seguridad funcional de otras partes del sistema. Es importante realizar un análisis de fiabilidad para identificar los peligros, que pueden causar riesgos de seguridad debido a las EMI. Los peligros deben identificarse en términos de eventos y las partes correspondientes del sistema. Los métodos para identificar los peligros se basan en general en dos métodos: metodologías ascendentes o descendentes.

Las pruebas de CEM para la seguridad funcional requieren consideraciones especiales con respecto a la selección de tipos de pruebas de inmunidad y sus niveles de prueba. Cuando se realizan las pruebas de CEM, el diseño puede modificarse para reducir los riesgos a valores aceptables. El diseño final debe ser validado para demostrar que el equipo funciona de acuerdo con los requisitos de seguridad especificados.

Métodos de análisis para la CEM y la seguridad funcional

Para controlar correctamente la seguridad funcional relacionada con la CEM para un equipo, se necesitan evaluaciones de peligros y riesgos. Durante este trabajo, se deben considerar los siguientes problemas:

- ¿A qué perturbaciones EM poco frecuentes, podría estar expuesto el equipo?
- ¿Cuáles son los efectos razonablemente previsibles de tales perturbaciones EM en el equipo?
- ¿Cómo podrían emitirse las EMI por parte del equipo para afectar al entorno EM circundante?
- ¿Cuáles podrían ser los efectos razonablemente previsibles de las perturbaciones mencionadas anteriormente?
- ¿Qué nivel de confianza o prueba se requiere para demostrar que los problemas mencionados anteriormente se han considerado completamente y que se han tomado todas las medidas necesarias para lograr el nivel deseado de seguridad?

Metodología ascendente

La metodología ascendente (o Bottom-up), de abajo hacia arriba de un estudio de fiabilidad o seguridad empieza a nivel de componente y muestra el efecto del fallo de diferentes componentes individuales en el sistema. Un método común que utiliza la metodología ascendente, El FMEA (Failure Mode and Effects Analysis) o AMFE (Análisis Modal de Fallos y Efectos) es un método de análisis que originalmente tenía como objetivo predecir la fiabilidad de los sistemas. El propósito del método es implementar requisitos en el sistema para la prevención de los efectos críticos derivados de los fallos de los componentes o funciones. La ventaja del método es que el análisis es muy detallado a nivel de componente y puede usarse para identificar fallos individuales o la necesidad de cambios en el diseño, implementando tecnología redundante o a prueba de fallos.

Se puede realizar un FMEA utilizando un enfoque de hardware o un enfoque funcional. El enfoque de hardware considera el modo de fallo de componentes en el hardware. Los efectos de las EMI suelen ser el resultado de perturbaciones en las condiciones de funcionamiento (corrientes y tensiones) de los componentes, en lugar de fallos de los propios componentes. La metodología ascendente normalmente no se considera un enfoque apropiado para analizar los efectos de las EMI.

El enfoque funcional de un análisis FMEA es más apropiado para investigar los efectos de las EMI. Con el enfoque funcional, el método se hace la pregunta "¿De qué maneras puede esta función desviarse del requisito especificado?". Este enfoque identifica las funciones más críticas y, por lo tanto, requerirá un mayor nivel de inmunidad. Desde la metodología ascendente se consideran todos los modos de fallo, incluidos los modos de fallo no relevantes para las EMI. Es un método innecesariamente extenso y complicado para sistemas complejos.

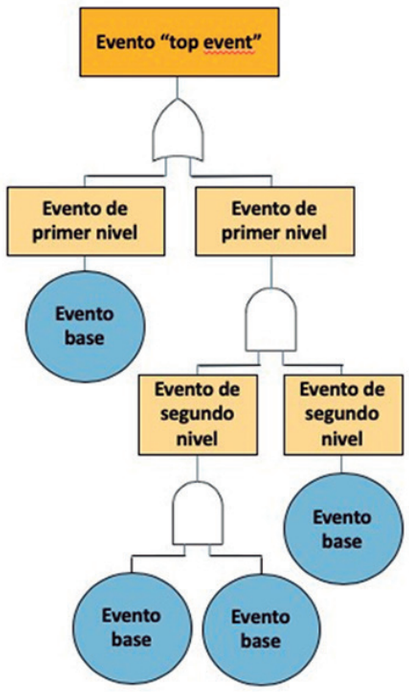

Figura 8. Ejemplo de árbol de fallos.

Metodología descendente

En un estudio de fiabilidad, la metodología descendente (o Top-down), de arriba a abajo es un método orientado a eventos, que permite al usuario identificar los niveles y componentes del equipo responsable para cada evento superior especificado. El usuario comienza con un evento superior en el nivel más alto de interés y desciende hasta el nivel donde ocurre la operación no deseada del sistema. El método descendente más conocido es el análisis del árbol de fallos, que ofrece algunas ventajas con respecto a la CEM.

El FTA (Fault Tree Analysis: Análisis de árbol de fallos) es una técnica que permite identificar las combinaciones de fallos que originan un determinado suceso (llamado top event). La figura 8 muestra un ejemplo de árbol de fallos. Un FTA emana de un evento no deseado que se investiga para encontrar posibles causas. Cuando se encuentran las posibles causas en un evento superior, éstas se investigan. Finalmente, se construye un árbol lógico que comienza a nivel de sistema y desciende hasta las causas principales.

Las causas independientes que interactúan en el árbol de fallos se expresan con puertas "Y" y las causas alternativas se expresan con puertas "O". Las puertas "O" son las partes

más críticas y deben ser atendidas primero, ya que corresponden a las probabilidades adicionales de las causas de fallo y, por lo tanto, con un mayor riesgo. La fortaleza de un análisis FTA es que es una búsqueda estructurada de causas de un evento específico con el propósito de eliminar las amenazas a la seguridad.

Debajo de los eventos de primer nivel se encuentran los eventos de segundo nivel, que son los eventos que podrían causar el evento de primer nivel. El análisis continúa con varios niveles hasta que se encuentran los eventos base. En el caso de usar el método FTA para analizar el circuito desde un punto de vista de la CEM, las EMI se consideran eventos base. Para un sistema grande como un tren, los árboles de fallo son a menudo muchos, grandes y complejos. Por lo tanto, es importante limitar el FTA a los principales eventos críticos de seguridad.

Existen algunas ventajas al usar el análisis FTA para evaluar CEM. El método puede manejar tanto fallos de causa común como tasas de fallo variables en el tiempo, lo cual es importante cuando se analiza el comportamiento durante la presencia de EMI en un equipo. Otra ventaja es que los eventos en un análisis FTA no se limitan solo a fallos, sino que también pueden implicar degradación en el rendimiento u otros factores externos al sistema.

Conclusiones

Es importante tener en cuenta la CEM en el análisis RAMS. Los ingenieros de RAMS deben trabajar juntamente con los ingenieros de CEM. RAMS y CEM deben acercarse para mejorar los sistemas actuales, cada vez más complejos. Ω

REFERENCIAS

- *Jon del Portillo, Jaizki Mendizabal, Iñigo Adin, Juan Melendez, Joaquin de No and Unai Alvarado, "Functional, Thermal And CEM Analysis For A Safety Critical Analogue Design Applied To A Transportation System" CEIT and Tecnun, University of Navarra.*
- *Reinaldo J. Pérez, "Handbook of Aerospace Electromagnetic Compatibility", IEEE Press, Wiley, 2019*
- *Qamar Mahboob, Enrico Zio, "Handbook of RAMS in Railway Systems, Teory and Practice", CRC Press, 2018*
- *Keith Armstrong, "Why increasing immunity test levels is not sufficient for high-reliability and critical equipment", August 2009, IEEE*
- *Keith Armstrong, "Why CEM immunity Testing is inadequate for Functional Safety", 2004 IEEE*
- *Keith Armstrong, "Introduction to CEM for Functional Safety, sometimes called Risk Management of EMC", Cherry Clough consultants, 2011*
- *Normas: IEC 61508, IEC TS 61000-1-2, IEC 62061, IEC 62511 , ISO 13849, ISO 26262, MIL-HDBK-217F, EN 50159, EN 50129, EN 50128, EN 50126-1, EN 50126-1, EN 50155*
- *Francesc Daura Luna, "La CEM y la seguridad funcional", Revista Española de Electrónica", Mayo 2014*
- *Francesc Daura Luna, "La gestión conjunta de la CEM y la seguridad funcional", Revista Española de Electrónica", Mayo 2014*
- *Diversos artículos sobre RAMS en la web de Leedeo: www.leedeo.es/publicaciones*