La compatibilidad electromagnética y la seguridad funcional

Artículo cedido por Cemdal

CEMDAL
www.cemdal.com

Autor: Francesc Daura Luna, Ingeniero Industrial, experto en compatibilidad electromagnética. Director de CEMDAL

La complejidad electrónica en todos los sectores va aumentando continuamente sin que se vean cambios importantes en la tendencia a corto plazo. El uso de la electrónica en aplicaciones de seguridad también crece muy rápidamente. Desde el punto de vista de la seguridad, se ha llegado al punto en que la aproximación normal para la obtención de la conformidad con la compatibilidad electromagnética (CEM), solo en base a la realización de los ensayos de CEM normales, es totalmente inadecuada cuando se trata de la seguridad funcional en máquinas complejas, como en los automóviles o en los aviones, por ejemplo. La consecuencia inevitable de todas estas tendencias es que no tener en cuenta la CEM en el análisis de la seguridad funcional de las máquinas o sistemas complejos, puede generar riesgos de seguridad no controlados para el usuario. Además los fabricantes pueden tener riesgos económicos no controlados. Ver la figura 1.

La seguridad funcional en sistemas electrónicos previene la probabilidad de daños físicos, o riesgos en la salud de las personas, como resultado de fallos en la funcionalidad de los dispositivos electrónicos. La seguridad funcional es una parte de las medidas de segundad que se implementan en los equipos, para que respondan correctamente a sus señales de control. Ejemplos de funciones de seguridad serían el apagado seguro de una planta de proceso si las temperaturas o presiones exceden ciertos límites, parar una máquina rotativa si se abre su puerta de protección, la detención de un brazo de un robot si una persona se acerca a su trayectoria programada, el cambio a un sistema alternativo cuando el sistema de control principal de vuelo de una aeronave falla, etc

En los años 90, como respuesta a un gran incremento en el número de accidentes industriales, la Instrument Society of América (ISA) promulgó la norma ISA S84.01 para determinar en EEUU la clasificación de sistemas de instrumentos seguros introduciendo el concepto de nivel de integridad de seguridad, SIL (Safety Integrity Level). Luego la IEC publicó la norma de seguridad funcional IEC 61508 (Seguridad funcional de los sistemas eléctricos/electrónicos programables relacionados con la seguridad). Desde el año 2000, la norma IEC 61508 ha recomendado varias decenas de pruebas y medidas para los sistemas, hardware y software, para la detección y/o recuperación de errores, mal funcionamiento o fallas en señales y fuentes de alimentación. Las pruebas y medidas recomendadas en la norma IEC 61508 son especialmente eficaces para hacer frente a las interferencias electromagnéticas EMI. Los ingenieros de CEM tienen que diseñar y construir equipos que continúen cumpliendo con sus normas de prueba de CEM pertinentes durante toda su vida útil en sus entornos reales (no sólo cuando son nuevos o en un laboratorio de CEM). Así, un nuevo enfoque fue aceptado ampliamente. Este nuevo enfoque tiene tres partes, que se muestran en la figura 2.

Figura 1: Incremento de los riesgos en un sistema complejo debido a las EMI

Las buenas prácticas de ingeniería de CEM ayudan a obtener la conformidad con las directivas de CEM y de seguridad así como a la reducción de los riesgos de seguridad siguiendo la norma IEC 61508. Todo ello tiene como resultado global no tener que comprometer la seguridad funcional por culpa de las EMI durante todo el ciclo de vida del equipo.

Esto se aplica a las medidas de seguridad en las industrias petrolíferas, de gas y empresas productoras de equipos electrónicos incorporados a trenes, aviones, barcos o automóviles, etc. La fiabilidad analiza el riesgo de fallo en los componentes electrónicos de un sistema complejo y como consecuencia, el sistema deje de realizar la funcionalidad prevista. Este fallo puede ser debido a la CEM, a la degradación de los componentes, a un fallo de instalación, etc. La seguridad funcional cuantifica la posibilidad de que estos mismos componentes, fallen en una función considerada de seguridad y por tanto pueda producirse un accidente. En todas las disciplinas de la ingeniería de seguridad se considera insuficiente confiar totalmente en las pruebas de producto. Sin embargo, los riesgos aceptables de seguridad son validados usando una variedad de métodos, sin limitarse solo a las pruebas para verificar el diseño de seguridad. Las perturbaciones electromagnéticas inusuales o extremas que exceden la protección que se logra mediante el cumplimiento de las normas de inmunidad, causarán EMI en el equipo. Esta EMI causará errores, mal funcionamiento

o fallos en las señales de los equipos y / o fuentes de alimentación.

Los niveles SIL y PL

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. Se usa el término ASIL ("Automotive Safety Integrity Level") para el sector de la automoción. Es una medida de la seguridad de un determinado proceso, dispositivo electrónico o sistema completo. Dentro de un mismo sistema podemos encontrar distintos niveles de seguridad. Una de las funciones puede tener un nivel de SIL y otra función otro nivel distinto. La asociación de una función a un determinado nivel SIL, está basada en un análisis denominado análisis de riesgos. El análisis de riesgos es la tarea de evaluar el riesgo de tener un fallo en una función segura, cuantificarlo y definirlo como aceptable o inaceptable. Los riesgos aceptables son aquellos que moralmente, económicamente o por cualquier otra causa son justificables.

Por el contrario, los riesgos inaceptables son aquellos que tienen consecuencias graves o costosas. El típico análisis de riesgos puede ser como se indica a continuación. Una vez elegido el nivel de seguridad SIL y por tanto asignado el nivel de fiabilidad esperado como punto de partida, cada uno de los componentes, procesos y software que intervienen en la función deben ser analizados. Acto seguido hay que comprobar si la suma del grado de fiabilidad del conjunto cumple con las expectativas de fiabilidad requerida en la función. Cuando la suma de riesgos es mayor que el riesgo esperado, entonces se impone realizar alguna modificación para reducir este riesgo de fallo.

A cada función de seguridad se le asigna un nivel SIL sobre la base de la aceptabilidad de la tasa de fallos peligrosos (es decir, el nivel aceptable de riesgo) para lo que se pretende controlar. Hay cuatro niveles SIL, cada uno correspondiente a un rango década de tasa de fallos peligrosos, como se muestra en las tablas 1 y 2 que indican cuales son las probabilidades permitidas de fallo, dependiendo de la frecuencia de utilización de las funciones. La probabilidad de fallo

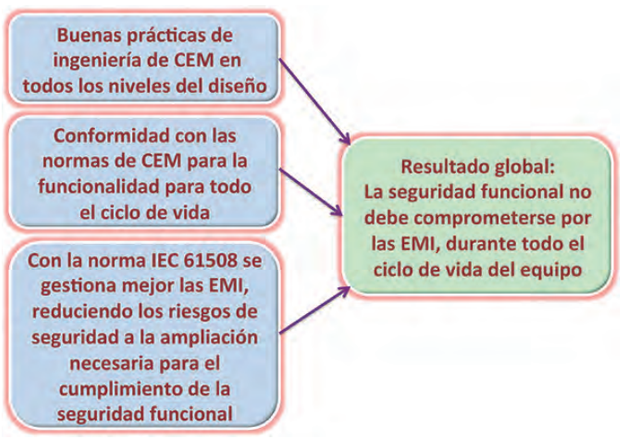

Figura 2 : Visión general de la aproximación tomada por la nueva estrategia

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. El riesgo de los procesos o las funciones pueden ser optimizados, utilizando componentes considerados adecuados dentro de un determinado nivel SIL. Por ejemplo, si el nivel de seguridad requerido para una función es SIL2, podemos alcanzar este nivel, utilizando componentes electrónicos y procesos cuya suma total esté dentro del riesgo fallo de nivel SIL2.

Una función de seguridad "continua" es una función que está trabajando todo el tiempo. Un nivel SIL4 corresponde a una función más segura que otra de SIL1. El nivel SIL4 se asocia con las menores tasas de fallo peligroso (niveles bajos de riesgo aceptable), y así exige el nivel más alto de confianza, tanto en el diseño de la seguridad funcional como en su validación independiente. Típicamente, el nivel SIL4 se utiliza para la electrónica de sistemas de control de vuelo de las aeronaves, señalización ferroviaria, el paro seguro de las centrales nucleares y similares. Una función de seguridad "a demanda" es una función que solo opera cuando es necesaria, tal como una parada segura cuando una máquina sufre un fallo de sobre-velocidad o sobre-temperatura. El nivel SIL3 permite un rango diez veces mayor de fallos peligrosos que el SIL4 (unas diez veces mayor de rango de riesgo aceptable), y así requiere diez veces menos de nivel de confianza del diseño y su validación. El nivel SIL3 se suele aplicar a los equipos fabricados en grandes volúmenes, por ejemplo: sistemas de control de la conducción de automóviles (acelerador, frenos, dirección, etc); maquinaria; control de procesos, etc, donde las consecuencias de un fallo son graves, pero no tanto como en el nivel SIL4. En el otro extremo de la escala, el nivel SIL1 se utiliza para los sistemas que deben ser algo más seguros que lo conseguido normalmente mediante la aplicación de las prácticas normales de un buen diseño y verificación.

Otra forma de ver los niveles SIL: el nivel SIL1 es requerido por sistemas con niveles de riesgo equivalente a un buen diseño habitual y sus prácticas

Safety Integrity Level (SIL)	Probabilidad promedio de un fallo en demanda en 1 año	Tiempo medio equivalente a un fallo peligroso en años**	Factor de confianza equivalente requerido por cada demanda en la función de seguridad
4	$\geq 10^{-5}$ a $<10^{-4}$	$>10^{4}$ a $\leq 10^{5}$	99,99 a 99,999%
3	$\geq 10^{-4}$ a $<10^{-3}$	$>10^{3}$ a $\leq 10^{4}$	99,9 a 99,99%
2	$\geq 10^{-3}$ a $<10^{-2}$	$>10^{2}$ a $\leq 10^{3}$	99% a 99,9%
1	$\geq 10^{-2}$ a $<10^{-1}$	>10 a $\leq 10^{2}$	90 a 99%

Tabla 1: Niveles de seguridad SIL (IEC EN 61508): Probabilidad de fallo en demanda. ** Aproximadamente 1 año = 10.000 horas de funcionamiento

Tabla 2: Los niveles de seguridad SIL (IEC EN 61508). Probabilidad de fallo en modo continuo

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%

de verificación y validación, pero reducido por diez ; el nivel SIL2 requiere que los niveles de riesgo se reduzcan 100 veces ; el nivel SIL3 requiere una de reducción del riesgo en 1.000 veces, y el nivel SIL4 requiere una reducción del riesgo de 10.000 veces, es decir, a 1/10.000 ó 0,01 % del nivel de riesgo alcanzado por las buenas prácticas normales de ingeniería. El concepto SIL se aplica al funcionamiento de un sistema completo que incluye electrónica, electromecánica, mecánica, trabajos de construcción y la gestión del personal (por ejemplo, restringiendo el acceso al área de trabajo) . Por lo general, la contribución de las EMI a cualquier nivel SIL no es más de un 10 % del riesgo total. Las EMI se identifican como un "modo de fallo sistemático", lo que significa que no es al azar, pero en cambio es una característica de un diseño determinado, de la misma manera que los "errores " de software son considerados como una característica de un diseño de software dado, en lugar de considerar que los errores se producen al azar. Así, para considerar el nivel de confianza solo del diseño de CEM, los números para los diferentes niveles SIL en las tablas 1 y 2 necesitan reducirse por lo menos diez veces. Tratar de anticipar los ratios de incidencia de las perturbaciones EM, generalmente 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 perturbación EM sin fallar, siempre que suceda. La norma europea EN ISO 13849-1 clasifica los diferentes circuitos funcionales de seguridad en cinco niveles de prestaciones PL ("Performance Level": Nivel de prestaciones) (tabla 3) : a,b,c,d,e, en función de su fiabilidad y su capacidad de detectar fallos, valorando básicamente su tiempo medio entre fallos peligrosos (MTTF) y su cobertura de diagnóstico. La evaluación del nivel de prestaciones requerido por un sistema de seguridad, PLr servirá para determinar si el sistema de seguridad adoptado es adecuado o si se requieren modificaciones o medidas adicionales. Debe hacerse una estimación del nivel de prestaciones PL requerido para cada riesgo en la vida útil de la máquina. El sistema de evaluación de nivel PL es más sencillo de aplicar que el sistema de nivel SIL. La figura 3 muestra la relación entre los niveles SIL y los niveles PL. Como segunda derivada, la norma EN ISO 13849 es más sencilla al simplificar y limitar las posibles soluciones, es menos ambiciosa en lo referente al software y está armonizada. Es la más idónea para el fabricante de maquinaria. Está previsto para el año 2018 integrar las normas EN IEC 62061 y la EN ISO13849. La figura 4 resume las normas que explican los niveles SIL, PL y ASIL para sistemas eléctricos, control de proceso, máquinas y automoción.

Performance Levels (PL)

PL	Probabilidad promedio de fallos peligrosos por hora (1/h)
a	$\geq 10^{-5}$ a $< 10^{-4}$
b	$\geq 3 \times 10^{-6}$ a $< 10^{-5}$
c	$\geq 10^{-6}$ a $< 3 \times 10^{-6}$
d	$\geq 10^{-7}$ a $< 10^{-6}$
e	$\geq 10^{-8}$ a $< 10^{-7}$

Tabla 3: Los niveles de seguridad PL (ISO 13849)

Desafíos y riesgos

Conviene distinguir lo que son las acciones destinadas a la seguridad funcional, de otras que son empleadas para la seguridad en general, aunque en ocasiones, ambas pueden conseguir el mismo objetivo. Por ejemplo: si en el radiador de una fuente de alimentación colocamos un sensor de temperatura, para limitar la corriente de esta fuente a un valor máximo cuando el radiador adquiere valores de temperatura demasiado elevados, esto es una protección de seguridad funcional. Mientras que si calculamos el radiador para que nunca alcance una temperatura excesiva que pueda provocar quemaduras al usuario, ésta es una protección de seguridad. El aumento de la complejidad en los sistemas electrónicos hace que, en la práctica, crear productos totalmente seguros, donde los comportamientos de seguridad de todos estos circuitos sea predecible, es casi imposible. El desafío consiste en diseñar sistemas de tal manera que se pueda prever y evitar fallos peligrosos o por lo menos controlarlos cuando éstos ocurran. Estos fallos pueden tener su origen en: especificaciones incorrectas del sistema, omisiones de seguridad en la especificación, fallos aleatorios de hardware, errores de hardware, software e integración, errores humanos de diseño, interferencias electromagnéticas, fluctuaciones en la alimentación eléctrica y problemas de CEM (emisiones o inmunidad)

Las tecnologías electrónicas están en todas las esferas de la actividad humana, incluyendo aquellas en las que los errores o el mal funcionamiento de la tecnología pueden tener implicaciones para su seguridad funcional. Las actividades afectadas incluyen, entre otras: comercio, industria en general, banca, administración, seguridad, medicina, agricultura, defensa, energía y eficiencia energética, ocio, transporte, vehícu-

los, carreteras, ferrocarriles, náutica, aviación, espacio, etc.

El funcionamiento de un dispositivo electrónico que proporciona una o más funciones que tienen un impacto directo en la seguridad puede tener errores o un mal funcionamiento que podría tener implicaciones para la seguridad funcional. Para evitarlo se requiere ingeniería de CEM adecuada para el control de los riesgos de seguridad. La seguridad funcional significa el logro de un nivel aceptable de riesgos debido a errores operacionales (funcionales) o mal funcionamiento durante toda la vida esper ada de un producto. Todas las tecnologías electrónicas son susceptibles de sufrir errores o mal funcionamiento causados por las EMI.

Además de las fuentes naturales de EMI, como los rayos y las descargas electrostáticas (ESD), todos los componentes electrónicos son fuentes y receptores de EMI y tienden a emitir más EMI en las frecuencias más altas. Además, hay una gran tendencia hacia el aumento del uso de las comunicaciones inalámbricas de datos (RFID, WIFI, Bluetooth, zigbee, Wireless USB, …) y el uso de fuentes de alimentación conmutadas y convertidores conmutados (en ahorro de energía, energía "verde", vehículos eléctricos e híbridos, ordenadores, …). Todas estas tecnologías son inherentemente ruidosas.

Cem para la seguridad funcional

La ingeniería de la seguridad y la ingeniería de la CEM se han desarrollado por separado. Esto significa que ahora los ingenieros de seguridad funcional por lo general no tienen un conocimiento profundo de la CEM y los ingenieros de CEM por lo general no tienen una buena comprensión de la seguridad funcional. Además, la mayoría de los ingenieros de seguridad "tradicionales" a menudo tienen una mala comprensión de la seguridad funcional, al tratarse de una relativa nueva disciplina que empezó a desarrollarse en la práctica a partir del 2000 con la publicación de la norma IEC 61508. La norma IEC 61508 está enfocada básicamente para componentes electrónicos y no considera los componentes mecánicos, hidráulicos ni neumáticos. Requiere bastante conocimiento y aplicación de técnicas estadísticas.

Figura 3 : Relación entre los niveles SIL y los niveles PL

Riesgos responsabilidades y metodología

Está generalmente aceptado en la ingeniería de seguridad que los niveles de riesgo aceptable deben ser mantenidos razonablemente a pesar del uso previsible o indebido. Es imposible hacer alguna cosa perfectamente segura, pero puede ser previsible el comportamiento del usuario. Se sabe que las personas se comportan de una cierta manera, lo que incluye la propensión a cometer errores en formas conocidas. La ingeniería de seguridad lo debe tener en cuenta. Por ejemplo, tradicionalmente las pruebas de CEM asumen que los vehículos son operados perfectamente todo el tiempo, y que no están dañados ni modificados. En la realidad los vehículos se deterioran con el tiempo, sufren averías, accidentes, modificaciones, … Estos cambios no deberían afectar gravemente a la seguridad.

La identificación de riesgos ("Risk Assesment") determina el comportamiento de la función segura para realizar el trabajo requerido con una tasa de fallos máxima, previamente establecida. En el análisis e identificación de riesgos interviene también la frecuencia de operación de la función segura. Para un mismo nivel de peligro, en las funciones que se usan con poca frecuencia se permiten tasas de fallos mayores que en funciones que tienen una frecuencia de utilización más elevada. El análisis de peligros ("Hazard analysis") analiza cuales son las consecuencias para los usuarios de los fallos en las funciones de seguridad. Los peligros más graves son los que, como consecuencia de un fallo, pueden causar un accidente.

Si no se controla bien la seguridad funcional pueden presentarse riesgos económicos para el fabricante debido a las leyes de responsabilidad de los productos defectuosos y a las regulaciones de los fallos de seguridad que pueden causar los productos peligrosos. Estas leyes pueden provocar la prohibición del producto y su retirada del mercado. Bastantes empresas son conscientes de que las reclamaciones legales en su contra podrían ser muy costosas y arruinar su reputación de marca. Por esta razón emplean buenos abogados, para ganar cualquiera de los casos en su contra o llegan a acuerdos extrajudiciales con condiciones de no divulgación.

De esta manera el verdadero costo de la mala ingeniería de diseño se oculta algunas veces a la opinión pública, a los gobiernos y al mercado en general.

Pero se debe tener en cuenta que los costos de aplicar correctamente un buen diseño de CEM y de seguridad funcional son menores que los potenciales costos legales de ignorarla. Estas técnicas de buen diseño contribuyen además a la mejora de la funcionalidad y la calidad del producto y en consecuencia a tener una mejor introducción en el mercado. Los métodos de buen diseño de CEM y seguridad funcional se pueden utilizar para reducir los riesgos en las aplicaciones críticas de alta fiabilidad y de metrología legal, así como en la mejora general de los resultados económicos y de cuota de mercado del producto fabricado.

Cuando una empresa desea controlar mejor sus procesos de conformidad con la CEM y la seguridad es necesario asumir una larga curva de aprendizaje. El riesgo de no mejorar este aspecto es tener un futuro con niveles inaceptables de incidentes con riesgos económicos y pérdidas inaceptables para el fabricante, sus clientes y sus usuarios, como se muestra en la figura 1. Estas mejoras

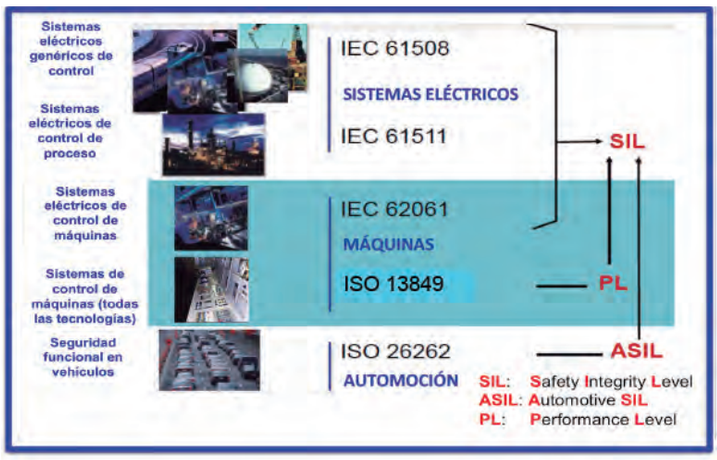

Figura 4 : Los niveles SIL y los niveles PL y sus normas de aplicación en sistemas eléctricos, control de proceso, máquinas y automoción

deberían ser vistas claramente como una metodología para el incremento de la rentabilidad y la reducción de los riesgos económicos a medio y largo plazo. Los responsables técnicos también pueden utilizar estas mejoras como un método para reducir su responsabilidad personal (responsabilidad civil o incluso de homicidio a causa de accidentes de seguridad). También puede ayudar a los consultores de seguridad funcional (por ejemplo, los que están cualificados para evaluar la norma IEC 61508 o sus normas "hijas" tales como la IEC 61511 o la IEC 62061, mejorando sus habilidades necesarias para evaluar la CEM para la seguridad funcional. La figura 5 muestra un cuadro resumen de las normas de CEM y de seguridad funcional. Destacar que a norma IEC 61000-1-2 es la norma IEC "básica" de la CEM para la seguridad funcional.

Para evitar confusiones con tantos términos diferentes utilizados en electrónica (por ejemplo: dispositivo, aparato, sistema, equipo, sistema de seguridad, instalación,…) se ha acuñado una nueva sigla: EFS - definida como: "Cualquier Entidad que emplea las tecnologías eléctricas y / o electrónicas que provee una o más Funciones que tienen un impacto directo en la Seguridad". La intención de esta sigla es la de cubrir toda la gama de posibilidades de diseño, realización y fabricación de un equipo, producto, aparato, máquina o sistema. Una EFS no es nunca un componente, parte, elemento, subsistema o subconjunto de la entidad que proporciona la función de seguridad. La figura 6 muestra los nueve pasos básicos de verificación para ayudar a la gestión de los proyectos, el diseño y la evaluación de la conformidad con la CEM y la seguridad funcional.

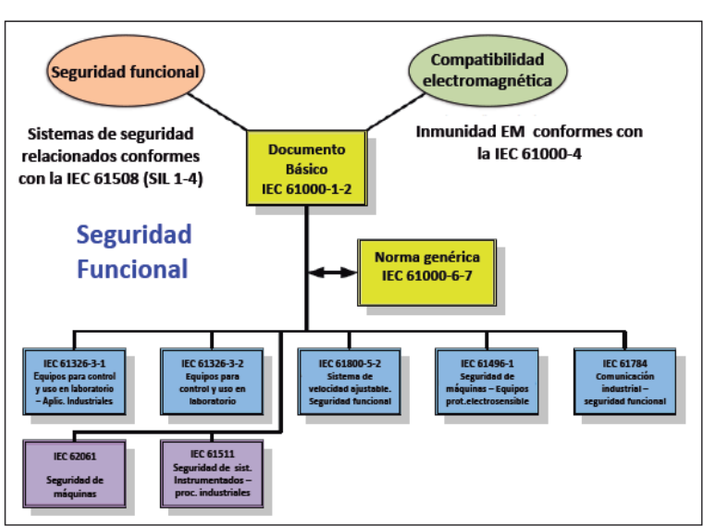

Figura 5 : Resumen de normas aplicables para la seguridad funcional y la CEM

Fallos afectando a la inmunidad

La inmunidad al entorno electromagnético (EM) normal en el área de trabajo del sistema puede verse afectada negativamente por los fallos. Por ejemplo : juntas conductoras dañadas con mala conductividad o no existentes, circuitos abiertos o en corto, fijaciones o uniones sueltas o faltantes en recintos o blindajes de cables, fallos de protección contra sobretensiones, conexiones eléctricas intermitentes, fallos en filtros, componentes incorrectos fuera de la tolerancia, corrosión en uniones de metales diferentes, condiciones eléctricas intermitentes, etc.

Las pruebas de seguridad normal simulan todos los fallos razonablemente previsibles para comprobar si la protección que ha sido diseñada (generalmente como resultado del análisis AMFE (Análisis Modal de Fallos y sus Efectos), el análisis del árbol de fallos (FTA: Fault Tree Analisys), o similar opera como se ha diseñado. Pero las pruebas de inmunidad de CEM normalmente sólo se realizan con los prototipos perfectos de los productos o sistemas, justo antes del inicio de la producción. Este método no es suficiente por sí solo para aceptar las pruebas de CEM como un medio correcto para demostrar que las EMI no pueden causar riesgos excesivos de seguridad funcional.

No es raro que los componentes de automoción o de máquinas fabricados en serie fallen en sus ensayos de CEM de control de calidad regular. A veces, los componentes se montan de forma incorrecta y aunque su funcionalidad es correcta, su inmunidad electromagnética se ve comprometida. Entonces se corrige el error en el componente, se repite la prueba y se pasa positivamente. No hay nada incorrecto en el diseño en cuanto a pasar sus pruebas de CEM, pero se deben reforzar las medidas en el diseño para proporcionar un sistema a prueba de fallos, para que el error de montaje sea razonablemente previsible. Además, a veces, si no se toman medidas para mejorar el proceso de producción, las características de CEM de los vehículos, máquinas o sistemas entregados a los clientes realmente se desconocen. Es necesario tener en cuenta la CEM en el

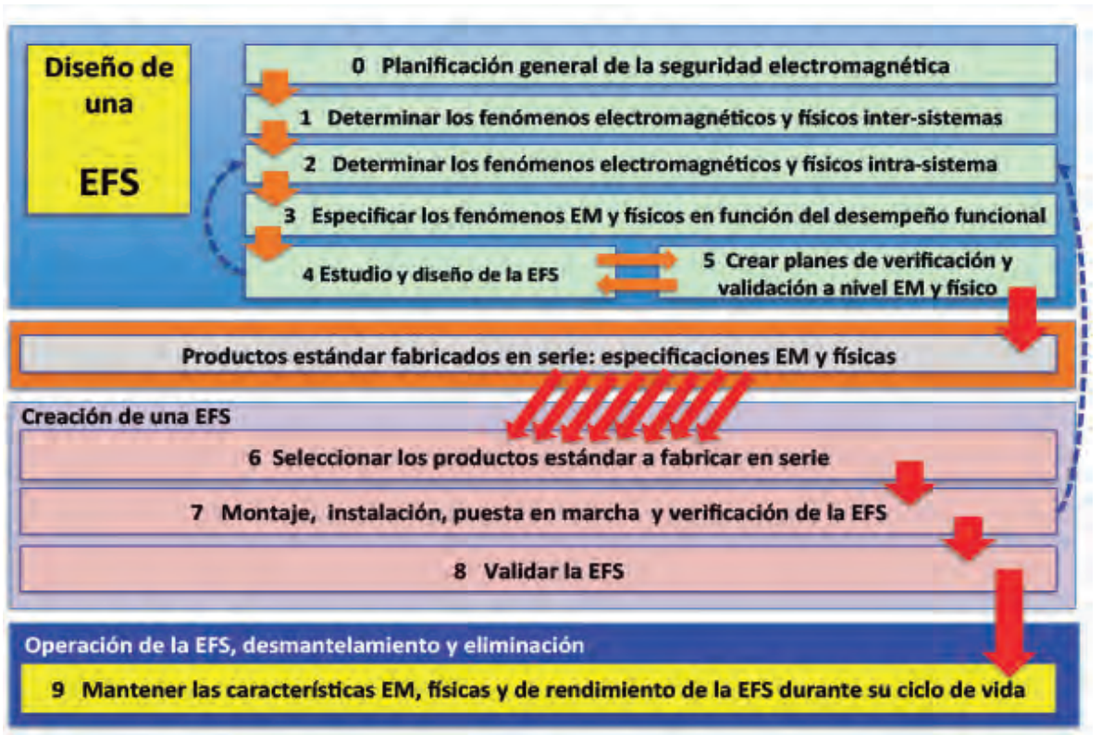

Figura 6: Los pasos básicos de verificación para ayudar a la gestión de los proyectos, el diseño y la evaluación de la conformidad

control de calidad de la producción, tal como se exige en las directivas de CEM.

Los ensayos de inmunidad

La mayoría de las normas de ensayos de inmunidad radiada especifican usar cámaras anecoicas de pruebas porque ayudan a realizar pruebas más fáciles de repetir. Su entorno EM interno es diferente a los entornos EM usuales en la vida real, por lo que sus resultados pueden diferir considerablemente de lo que va a suceder en la vida real. Algunos fabricantes y la mayoría de los directores de laboratorios de ensayos de CEM suponen que aumentar los niveles de ensayo más allá de lo que va a ocurrir en la vida real del producto proporciona un "margen de seguridad" suficiente (cuidado con este término en este contexto). Por supuesto, incrementando los niveles de exigencia se mejora la confianza en que estos niveles aplicados en el ensayo son realmente iguales o superiores a los niveles de prueba especificados para el entorno EM real, como se muestra en la figura 7.

Además, si se supone que las medidas de mitigación EM, tales como los blindajes y los filtros se degradarán en unos dB a lo largo de la vida útil del equipo, es razonable añadir esos dB al nivel exigido en los ensayos. Pero, ¿qué pasa si un filtro de 60dB sufre un fallo catastrófico, o el operador deja la puerta abierta de un armario apantallado y por ello probamos el equipo con 60dB más en los niveles de inmunidad para preverlo? Por ejemplo, en lugar de realizar los ensayos de inmunidad con 3 V/m, ¿podemos añadir 60dB más para permitir ver los efectos de la degradación del blindaje o del filtro y hacemos la prueba con 3.000 V/m ? ¿Y si también queremos cambiar el ajuste del nivel de ensayo aumentándolo por cuatro desviaciones estándar para alcanzar el 99,99% de confianza (figura 7) de que hemos probado igual o por encima del nivel especificado?, ¿No deberíamos entonces probar a 10.000 V/m ? Estos niveles de radiación son difíciles y caros de conseguir debido a la gran potencia de RF necesaria. No es muy fácil económicamente llegar a estos valores.

También se debe considerar la incertidumbre de medición en las cámaras de ensayo. Usando cámaras de reverberación se pueden realizar pruebas más realistas, y por ello se utilizan para ensayar equipos críticos en aviónica y automoción.

Para facilitar las pruebas, con bajos costos y alta repetitividad, los ensayos estándar de inmunidad usan una modulación de onda sinusoidal de 1kHz. Pero algunos fabricantes utilizan la modulación de impulsos para simular los efectos de los teléfonos móviles digitales y los radares en sus productos. Algunas normas militares usan ondas cuadradas de 1kHz. Sin embargo, los entornos EM de la vida real contienen perturbaciones EM con una amplia gama de diferentes tipos de modulación y frecuencias con las que la inmunidad se puede degradar de manera significativa (20 dB o más) cuando la modulación de la EMI se corresponde con las frecuencias o las formas de onda utilizadas en los procesos internos del equipo o resuenan internamente con sus circuitos, cables, transductores o cargas.

Un elemento del equipo sometido a un campo EM radiado recoge tensiones de RF en todos sus cables, con diferencias de fase entre ellos debido a sus diferentes rutas, capacidades parásitas, etc, Normalmente, en los ensayos de inmunidad, sólo se aplican tensiones de RF en un cable a la vez. Inyectado energía de RF en todos los conductores de un equipo

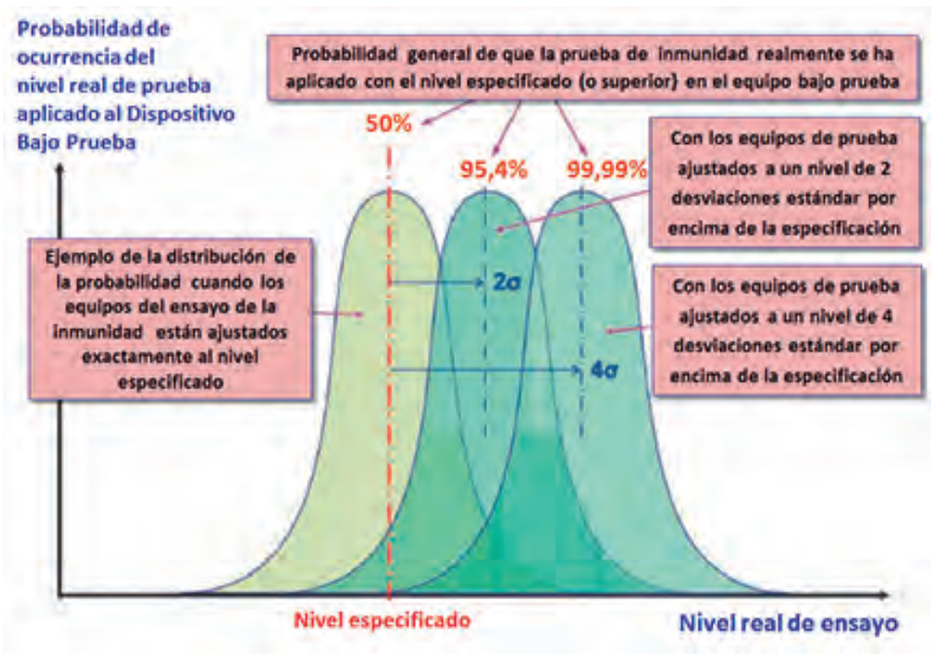

Figura 7: Usando una "incertidumbre expandida" se mejora la confianza del ensayo cuando se prueban sistemas lineales con pruebas de inmunidad conducida y radiada.

a un mismo tiempo, pero con cambios de fase para coincidir con lo que se espera que suceda en la vida real, la inmunidad puede ser significativamente peor que aplicando el ensayo normal probando cada cable por separado.

Perturbaciones electromagnéticas simultáneas

Las pruebas de inmunidad se aplican con un número limitado de tipos de perturbación EM, siempre un tipo de perturbación a la vez. Pero en la vida real, el funcionamiento del equipo a menudo está expuesto a EMI simultáneas. Por ejemplo: dos o más campos de RF a diferentes frecuencias, o un campo radiado más un transitorio conducido o una descarga electrostática, etc. Un equipo que pasa sus ensayos de inmunidad de forma individual puede ser mucho más susceptible a los niveles inferiores de las mismas perturbaciones cuando éstas se aplican de forma simultánea, como ocurre en la vida real.

En el mundo de la CEM, a menudo se argumenta que las perturbaciones simultáneas son demasiado poco probables, pero es bastante obvio que, por ejemplo, en el suministro de la red eléctrica, las formas de onda distorsionadas se producen con frecuencia todo el tiempo. Si esta distorsión da lugar a huecos de tensión o micro-cortes (como ocurre a menudo), entonces el condensador de almacenamiento en el lado no regulado de la fuente de alimentación de CC no se cargará al nivel suficiente, como sería normal, y la susceptibilidad del equipo a los fallos de tensión de red será diferente a lo que se tiene cuando se prueba con una alimentación nominal correcta y limpia. También es bastante obvio que en algunas zonas pueden haber intensidades de campo muy altas debido a transmisores de radio o TV. Incluso gran parte de algunas ciudades están expuestas a campos de más de 3 V/m en múltiples frecuencias de difusión a la vez. En estas zonas los transitorios y las ESD continúan con normalidad, por supuesto, lo que significa que la exposición a uno o más campos de RF, al mismo tiempo que los transitorios y las ESD es una situación razonablemente previsible.

Todo ello a la vez puede causar más problemas que por separado. Los transitorios pueden ser tal vez muy poco frecuentes y pueden ser ignorados en las aplicaciones normales pero, por ejemplo, cuando se considera un sistema de seguridad que se produce en volúmenes muy altos, incluso una muy pequeña posibilidad puede suceder a diario, por lo que es razonablemente previsible y debe ser tenida en cuenta.

Las perturbaciones simultáneas con diferentes frecuencias pueden causar EMI a través de la intermodulación (IM) que, como la demodulación, se produce de forma natural en los dispositivos no lineales como los semiconductores de los CI, (diodos y transistores). La figura 8 muestra un sencillo ejemplo de dos campos de RF a diferentes frecuencias, que pueden causar EMI debido: a la interferencia directa de cada frecuencia de forma independiente, la demodulación de las envolventes de amplitud de una u otra frecuencia, o de ambas frecuencias a la vez y por la intermodulación, por la que se crean nuevas frecuencias. Imaginemos que realizamos las pruebas normales de inmunidad radiada en el rango de frecuencias de 150 kHz a 6 GHz, y descubrimos que nuestro producto es muy susceptible entre 20 MHz y 200 MHz. Para evitarlo agregamos o modificamos el blindaje y el filtrado para que sean más efectivos en el rango de frecuencias susceptibles y con estas mejoras el equipo pasa la prueba. Podemos felicitarnos por el buen resultado y procedemos a realizar la siguiente prueba. No nos molestamos en mejorar la mitigación de problemas de inmunidad en el rango de 200MHz a 6GHz, porque no es necesario para pasar la prueba.

¿Por qué perder el tiempo, y añadir costes innecesarios ? Pero en la vida real, podrían entrar EMIs simultáneas en la gama de frecuencias de 200MHz a 6GHz y , de hecho, entrarán en el equipo, donde se intermodularán y, con una baja probabilidad, pero de forma razonablemente previsible, podrán crear EMIs internas en el rango de 20 MHz a 200 MHz, causando EMIs allí donde estábamos tan convencidos de haberlas eliminado. Esto muestra que realizando una prueba normal es difícil descubrir este problema, no importa lo alto que sea el nivel del ensayo.

Efectos físicos y climáticos

Por razones de seguridad es importante mantener un buen nivel de rendimiento EM a lo largo todo el ciclo de vida previsto del equipo, a pesar de los efectos previsibles de los entornos físicos y climáticos, incluyendo todos los efectos siguientes.

A nivel mecánico, por ejemplo, las fuerzas estáticas (flexión, torsión), golpes, vibraciones, etc. A nivel climático cabe tener en cuenta como afecta la temperatura, la humedad, la presión atmosférica, en sus extremos y los efectos de los ciclos de cambio. A nivel químico, la oxidación, la corrosión galvánica, el polvo conductor, la condensación, las gotas, el aerosol, la inmersión, la formación de hielo, etc. A nivel biológico, el crecimiento de moho, la destrucción causada por roedores, etc. A nivel operativo, el desgaste en el curso de la vida del producto como, la fricción, el rozamiento, la limpieza repetitiva, la acumulación de grasa, etc. Y por último el envejecimiento.

Los efectos previsibles varían desde los efectos inmediatos (por ejemplo, al abrir la puerta de un armario apantallado) a los efectos a largo plazo (por ejemplo, la corrosión de una articulación de un blindaje o la unión eléctrica a tierra de un filtro). Se puede llegar a tener una degradación de 20dB en la atenuación de un filtro causada por una combinación de la temperatura ambiente, la tensión de alimentación y la corriente de carga, todo ello dentro de las especificaciones del filtro, en comparación con los resultados de la pruebas normales de inmunidad. Algunos fabricantes realizan "Pruebas de vida altamente acelerada" (conocido como HALT ("Highly-Accelerated Life Testing") para comprobar que la funcionalidad se mantiene a lo largo del ciclo de vida esperado. Pero las unidades "pre-envejecidas" resultantes no se prueban de nuevo para ver si sus características EM se han degradado demasiado. En algunos equipos críticos, también después de la simulación de la exposición a su vida útil física y climática, sería bueno ejecutar de nuevo las pruebas de CEM para comprobar que el equipo sigue cumpliendo las especificaciones.

La calidad del diseño electromagnético

Es muy común para los fabricantes probar sus productos con ensayos de CEM, iterando sus diseños hasta que superan los ensayos. Aparte de ser un muy mal uso de los recursos y tener excesivos gastos extras, este método de prueba y error no puede revelar si la conformidad se logra mediante un buen diseño EM, o por alguna otra razón que no se puede controlar de manera adecuada durante la fabricación en serie a lo largo toda la vida útil de la producción. Por ejemplo, si el diseño EM de un producto no tiene en cuenta las tolerancias de los componentes, los cambios de tecnología en los circuitos integrados (CI), las variaciones en el montaje (por ejemplo, el posicionado de los mazos de cables, puesta a tierra, etc), la sustitución de componentes obsoletos, las correcciones de errores de firmware, etc, entonces las previsibles variaciones en la fabricación en serie podrían degradar sus características EM y agravar los riesgos de seguridad. El hecho de que uno o dos prototipos de un producto pasen sus pruebas de CEM no significa nada en absoluto para las características EM del resto de la producción suministrada, a menos que en su diseño se haya considerado las cuestiones de variabilidad explicadas anteriormente.

Por supuesto, se trata de un tema general para cualquier integrador de sistemas, incluso si se comprueba que los ensayos de CEM se realizaron correctamente y que realmente fueron aprobados, en las unidades que se tiene previsto comprar y montar en un sistema crítico. ¿Cómo se puede estar seguro de que las unidades suministradas pasarían las mismas pruebas ?

Los errores de montaje

Una buena técnica de seguridad siempre requiere algunas pruebas básicas en el control final de la línea de producción de cada unidad fabricada, para asegurarse de que los errores de montaje no la han hecho más insegura. Pero los ensayos estándar de CEM no incluyen los requisitos que obliguen a los fabricantes a llevar a cabo continuos controles de rutina sobre las características de CEM durante la fabricación en serie. No es raro que los elementos de los equipos que funcionan correctamente fallen en las pruebas de CEM debido a un mal montaje. Aunque la mayoría de los fabricantes emplean rigurosas pruebas de fin de línea, incluyendo pruebas en el propio circuito que pueden descubrir montajes incorrectos que afectan a la funcionalidad, casi nunca tienen el objetivo de descubrir montajes incorrectos que pueden afectar a las características de CEM, que luego pueden afectar a los riesgos de seguridad.

Conforme a las Directivas de la UE y otros países, la empresa que coloca el equipo terminado en el mercado, es la responsable de la totalidad de su seguridad y de su CEM. En caso de incumplimiento, la empresa no puede esperar que los investigadores oficiales sigan la cadena de suministro y evitar ser procesada. Se supone que los integradores de sistemas son profesionales, y como resultado son plenamente conscientes de cuestiones como las que se acaban de exponer.

Los efectos sistemáticos

La suposición general es que si todos los productos incorporados en un sistema complejo, como una máquina, han pasado bien sus prue-

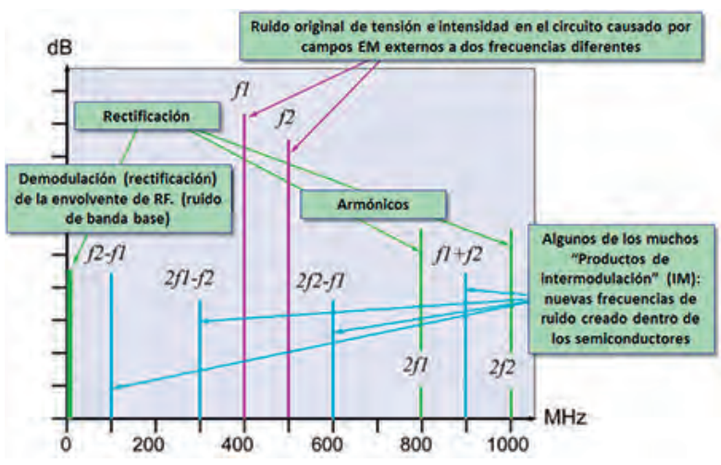

Figura 8: Ejemplo de demodulación e intermodulación (IM)

bas de inmunidad y de emisiones individualmente, a continuación, los sistemas integrados usando estos productos serán también conformes a la directiva de CEM. Este es el concepto CE + CE = CE que trata de una práctica común, pero incorrecta, en el sector de la gran maquinaria y las ingenierías integradoras de grandes sistemas complejos. Se basa en la idea de que si se compra un número de componentes o aparatos destinados a un sistema, todos ellos con el marcado CE, el sistema completo formado por estos componentes no necesita ningún trabajo adicional para poder tener el marcado CE. Así se podría declarar compatible con todas las directivas pertinentes de seguridad, baja tensión y compatibilidad electromagnética y podría automáticamente aplicar el marcado CE a la máquina completa. Pero, lo más seguro es que si se realizan las pruebas de CEM, no sea así y la máquina completa no cumpla y no pueda aplicarse correctamente el marcado CE. El concepto CE+CE=CE está completamente equivocado y legalmente no es aceptado. Degradaciones de rendimiento EM que son perfectamente aceptables cuando un elemento del equipo ha pasado las pruebas de CEM, o no son medidas durante la prueba, podrían tener implicaciones importantes para la seguridad funcional de los sistemas que los utilizan.

Así, es claro que CE + CE ≠ CE y es necesario asegurar la conformidad de CEM y de seguridad en el sistema completo. Un buen ejemplo es una unidad de fuente de alimentación de 3,3V utilizada para alimentar una unidad de control usando un microprocesador. Cuando la fuente se somete a la norma IEC 61000-4-4 (ráfaga transitoria rápida) la salida de la fuente de alimentación será inestable, es decir, tenderá cero voltios durante unos pocos cientos de milisegundos y luego se recuperará automáticamente. Así, la fuente cumple con el Criterio de Desempeño B, que es todo lo que se requiere. Cuando la unidad de control se prueba según la IEC 61000-4-4, nada sale mal. Pero, al poner las dos unidades juntas para controlar un robot y aplicar el mismo criterio al sistema completo, la unidad de control se bloqueará y le tomará decenas de segundos reiniciarse, mientras que el sistema que estaba controlando se volverá loco y quizá hará estragos a su alrededor, afectando incluso a algún operario a su alcance. El máximo nivel de prueba no es necesariamente el peor caso. Los dispositivos electrónicos son todos no-lineales y los circuitos y su firmware pueden ser muy complejos, por lo que los productos a veces pueden fallar cuando se prueban con las perturbaciones EM de bajo nivel, de una manera diferente, o incluso pasar correctamente cuando se prueban con los niveles máximos especificados. Sin embargo, muchas pruebas de inmunidad EM exponen al equipo al más alto nivel especificado, para ahorrar tiempo de prueba y costos. Los niveles de perturbación inferiores suelen ser mucho más probables en la vida real, por lo que podrían ser mucho más significativos para la seguridad funcional.

Conclusiones

Alcanzar la confianza suficiente en la utilización de la seguridad funcional usando sólo pruebas de CEM, requeriría afrontar demasiados puntos de análisis, como hemos visto, requiriendo un plan de pruebas que nadie podría permitirse, en coste o en tiempo. Por ello tenemos que ser más eficientes para alcanzar la seguridad funcional con tiempos y gastos más razonables. Las pruebas de CEM nunca pueden ser suficientes (por sí solas) para demostrar que los riesgos funcionales de seguridad son lo bastante bajos o que la reducción del riesgo será suficientemente alta a lo largo del ciclo de vida de un equipo, teniendo en mente sus entornos físicos y climáticos (incluyendo desgaste y envejecimiento). El número de variables es demasiado grande. Los planes de prueba se deben elaborar para que proporcionen la necesaria confianza de diseño. Para combinar la CEM y la seguridad funcional se requiere seguir el enfoque que se ha adoptado en todos los demás aspectos de la ingeniería de seguridad, incluyendo el software: aplicar una buena ingeniería con técnicas probadas como la gestión de riesgos, utilizando una amplia gama de métodos de verificación y validación. La verificación y validación implica realizar pruebas CEM, pero deberán ser cuidadosamente adaptadas a cada proyecto, para proporcionar la confianza suficiente en el diseño de la seguridad y durante la producción. Tener en cuenta la CEM en la seguridad funcional significa que tenemos que aplicar los métodos de la Gestión de Riesgos, como los de la IEC 61508, también para la CEM. Este es exactamente el enfoque de la IEC 61000-1-2.

Conviene trabajar en equipo un experto en seguridad con un experto en CEM para realizar un buen diseño para la seguridad funcional.

REFERENCIAS

- *Joan Pere López Varaguas, "Compatibilidad Electromagnétcia y Seguridad Funcional en Sistemas Electrónicos", Marcombo, 2010*
- *Alfons de Victoria, "Aspectes tècnics de seguretat de màquines", Curs de Formació Contínua Enginyers Industrials de Catalunya, 2014*
- *Francesc Daura, Marcado CE + marcado CE ≠ marcado CE: concepto aplicado a máquinas, sistemas complejos o instalaciones fijas, Revista Española de Electrónica, Noviembre 2013*
- *The IET, The Institution of Engineering and Technology: "Electromagnetic Compatibility for Functional Safety", 2008 "Overview of techniques and measures related to EMC and Functional Safety", 2013. http://www.theiet.org/factfiles/emc/index.cfm*
- *Keith Armstrong, "Cost-effective Risk Management of CEM without special CEM design expertise or testing", IEEE 2013 CEM Symposium*
- *Keith Armstrong, "Why increasing immunity test levels is not sufficient for high-reliability and critical equipment", August 2009, IEEE*
- *Keith Armstrong, "Why EMC immunity Testing is inadequate for Functional Safety", 2004 IEEE*
- *ernd Jaekel, Current status of standardization related to electromagnetic compatibility and functional safety, Siemens AG, Sector Industry, 2012*
- *Normas: IEC 61508, IEC TS 61000-1-2, IEC 62061, IEC 62511 , ISO 13849, ISO 26262*