Seguridad Funcional Aplicada a los Sistemas de Seguridad en Túneles

D. Fernando Martín Jiménez
D. Joseán Morales Arostegui
IKUSI, Ángel Iglesias, S.A.

1. Introducción

Desde 1999, la seguridad en túneles de carretera ha sido objeto de creciente interés como consecuencia del dramático accidente del túnel de Mont Blanc y Tauern. Numerosas iniciativas tuvieron lugar a nivel nacional y europeo, fruto de las cuales son las regulaciones presentes.

Adicionalmente, dentro de la propia Asociación Mundial de Carretera (PIARC) existen Comités de expertos dedicados al análisis de la operación de túneles de carreteras, cuya finalidad es el estudio y discusión de aquellos aspectos relacionados con la seguridad de dichos túneles, identificando, desarrollando y diseminando las mejores prácticas de gestión de la seguridad en túneles. Una de las tareas de dicho grupo es la mejora de las verificaciones de seguridad, diseños y procedimientos que permitan garantizar los niveles necesarios de seguridad.

En estos Comités, hay grupos de trabajo que han realizado diferentes estudios e informes descriptivos de las diferentes prácticas de seguridad en varios países a nivel mundial. Uno de los objetivos de dichos estudios es el de evaluar la posibilidad de definir un marco global que tome en cuenta todos los aspectos relevantes relacionados con la seguridad funcional de un modo integrado.

La regulación actual requiere la realización de evaluaciones de riesgos, basados en análisis de riesgos probabilísticos o determinísticos basados en escenarios, o una combinación de ambos. Sin embargo, no parece tener en cuenta la naturaleza y arquitectura de los propios elementos y sistemas (eléctricos, electrónicos, hidráulicos, neumáticos, etc.) encargados de garantizar la seguridad.

Es común en este tipo de infraestructuras el empleo de componentes eléctricos/electrónicos para la realización de funciones de seguridad, por lo que parece beneficioso analizar con detenimiento las prácticas exigidas a este tipo de equipamiento en otros de sectores o aplicaciones, si ello permite obtener un mayor nivel de seguridad.

El objetivo de este documento es realizar una breve presentación de los conceptos básicos asociados a la seguridad funcional, entendida esta como la garantía de que los sistemas eléctrico/electrónico/electrónico programables (E/E/PE) operen correctamente en respuesta a sus entradas y que por tanto sean altamente confiables, es decir, no basta con disponer del sistema de seguridad sino además de garantizar, dentro del riesgo asumible, que este disponible cuando se necesite.

Para este objetivo nos hemos basado en la norma IEC 61508 y su trasposición a la legislación nacional UNE-EN 61508 por los motivos que más adelante se explicarán.

A continuación se presentará, de un modo resumido, el ciclo de vida de seguridad asociado a sistemas E/E/PE empleados para realizar funciones de seguridad, según propone la norma anteriormente citada.

Finalmente describiremos muy brevemente lo que entendemos que implicaría su aplicación en el entorno de túneles viarios, identificando los sistemas candidatos a requerir funciones de seguridad.

2. Situación de Partida

Durante muchos años, se han empleado sistemas formados por componentes eléctricos y/o electrónicos para realizar funciones de seguridad en la mayor parte de las industrias o sectores de aplicación. Se trata de sistemas, cuya falla podría tener un impacto en la seguridad de las personas, el ambiente y/o la propiedad.

Los sistemas basados en computadores (también denominados sistemas de electrónica programable) se han empleado habitualmente para realizar funciones

no seguras pero actualmente su uso para este tipo de funciones está totalmente generalizado.

De cara a garantizar la explotación efectiva y segura de la tecnología de sistemas basados en computador, es esencial disponer de un conjunto de directrices referentes a los aspectos de seguridad para la toma de decisiones.

Existen un conjunto de estándares y normativas genéricas de seguridad, entre las que destaca la IEC 61508, que proporciona una guía para todas las actividades relacionadas con el ciclo de vida de la seguridad para aquellos sistemas compuestos por componentes eléctricos y/o electrónicos y/o electrónicos programables (sistemas E/E/PE) empleados para realizar funciones de seguridad.

Existe una gran variedad de aplicaciones de sistemas E/E/PE en múltiples industrias y con diferentes niveles de complejidad, peligrosidad y riesgo. La definición específica de las medidas de seguridad dependerá de múltiples factores específicos a dichas industrias o sectores de aplicación.

El estándar IEC 61508 provee un marco que permite la definición de estas medidas de seguridad en estándares específicos por industria o sector de aplicación. Entre otros, podemos citar las siguientes normas:

- IEC61511 aplicable al sector de procesos (químicas, petroquímicas, alimentación)
- IEC62061 aplicable al sector de maquinaria
- IEC61513 aplicable al sector nuclear

La normativa genérica suele ser empleada en caso de no existir una norma específica en dicha industria o sector de aplicación. Esta norma es de aplicación voluntaria, sin embargo es considerada “buena práctica” y es mencionada dentro del ámbito legal y jurídico en ciertos países.
En el sector de las infraestructuras viarias no se ha definido ninguna normativa específica en lo referente a la seguridad funcional hasta la fecha por lo que no existe una metodología suficientemente sistemática y unificada que prescriba las actividades necesarias para asegurar la seguridad funcional de los sistemas E/E/PE empleados para realizar funciones de seguridad.

No obstante, en el entorno de los túneles, estamos tratando con auténticos Sistemas Instrumentados de Seguridad (SIS) que afectan a la seguridad de las personas y de la propia infraestructura y como tales deben ser tratados.

3. Seguridad Funcional Genérica

El estándar internacional IEC61508 describe todas las fases del ciclo de vida de seguridad (diseño inicial, diseño, implementación, instalación, puesta en marcha, operación, mantenimiento y desmantelamiento) en lo referente a sistemas E/E/PE empleados para realizar funciones de seguridad.

Este estándar proporciona una metodología para el establecimiento de especificaciones de requisitos de seguridad con el fin de alcanzar el nivel de seguridad requerido para los sistemas E/E/PE. Para ello, define los niveles de integridad de seguridad (SIL) que especifican los niveles objetivo de seguridad que deben alcanzar los sistemas E/E/PE empleados para realizar funciones de seguridad.

Asimismo, define unos valores mínimos para las medidas probabilísticas de fallo que deben ser satisfechos por los sistemas E/E/PE empleados para realizar funciones de seguridad.

Por otra parte, el estándar IEC61508 también especifica el nivel de información a ser documentada y las actividades de gestión y técnicas a ser llevadas a cabo durante las diferentes fases del ciclo de vida de seguridad tanto a nivel global como de sistemas E/E/PE e incluso los responsables de cada una de las tareas, departamentos y organizaciones implicados.

De cara a realizar de un modo sistemático todas las actividades necesarias para conseguir el nivel de integridad de seguridad requerido para los sistemas E/E/PE, el estándar adopta un ciclo de vida de seguridad global como marco técnico. La Figura 1 presenta el ciclo de vida de seguridad global.

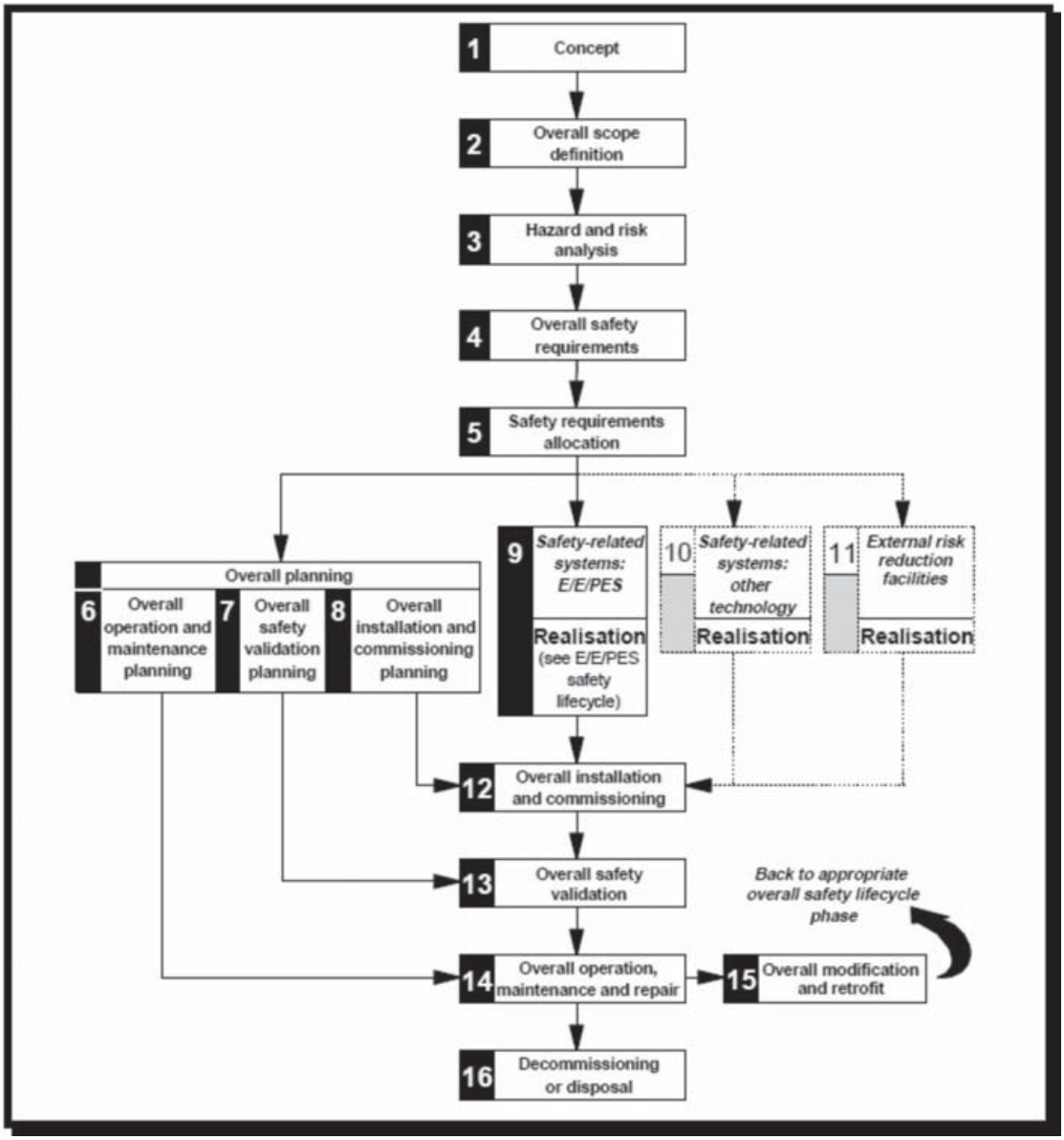

Figura 1: Ciclo de vida de la seguridad global

El ciclo de vida de seguridad genérico que se describe en el estándar tiene 16 fases que pueden ser agrupadas del siguiente modo:

- Fases 1-5 aborda el análisis de los sistemas
- Fases 6-13 aborda la implementación
- Fases 14-16 trata la operación

La parte del ciclo de vida de seguridad específico de los sistemas E/E/PE y del software asociado a los controladores programables se trata de modo específico, según se muestra en la Figura 2 y en la Figura 3.

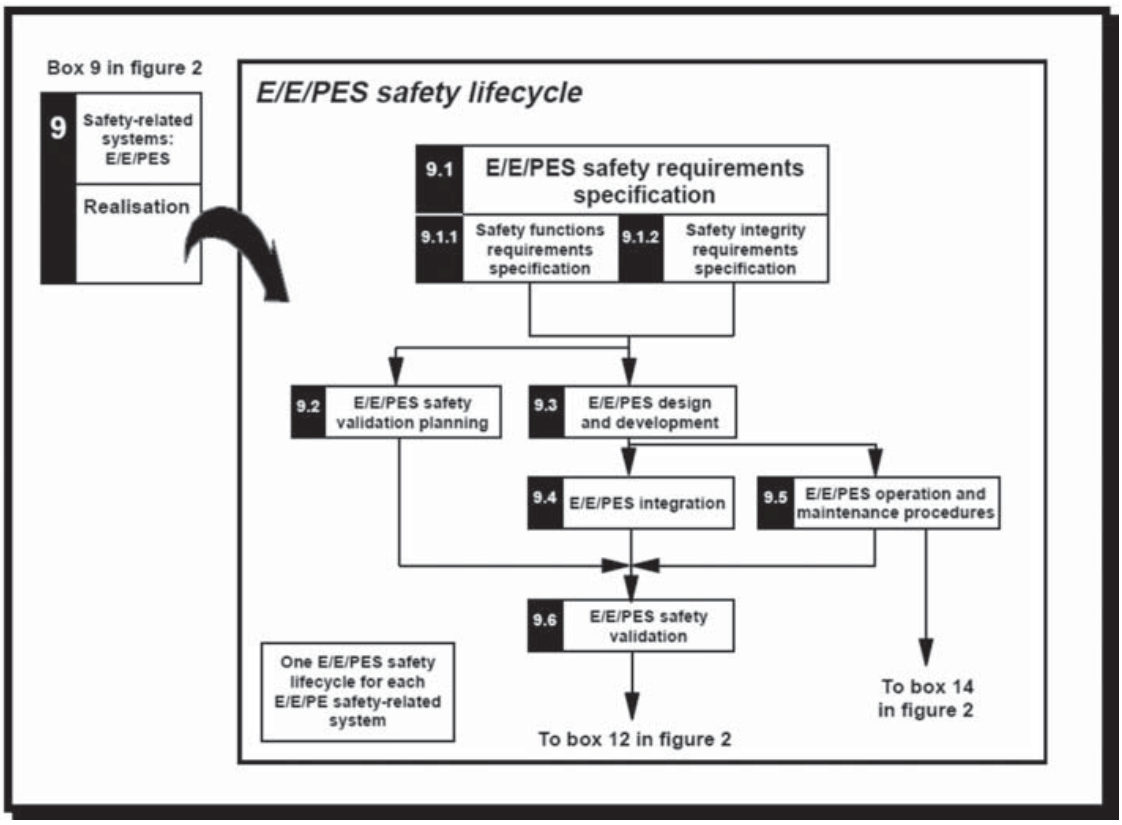

Figura 2: Ciclo de vida de seguridad específico de los sistemas E/E/PE (1)

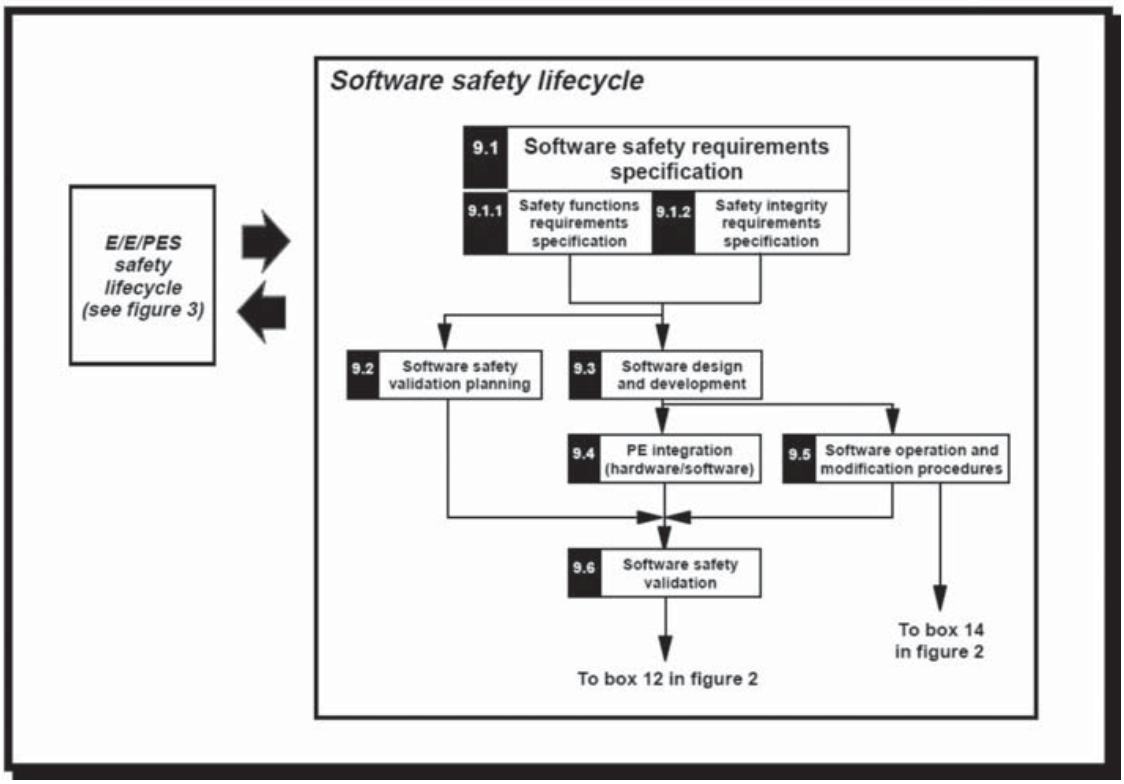

Figura 3: Ciclo de vida de seguridad específico de los sistemas E/E/PE (2)

Un concepto clave es el de función de seguridad, entendida como una función a ser implementada en un Sistema E/E/PE, cuyo cometido es llevar a, o mantener en, un estado seguro al equipo bajo control con respecto a un evento peligroso específico.

En muchas ocasiones caemos en el error de confundir o no diferenciar la redundancia y la disponibilidad del controlador y los dispositivos de captura con la seguridad de la propia función a sistema.

Una vez determinada la función de seguridad dentro de uno de los sistemas de seguridad considerados, esta abarca desde el elemento sensor hasta el dispositivo actuador pasando por el controlador y las comunicaciones afectadas dentro de las posibilidades de la infraestructura.

Figura 4: Actores en la función de seguridad

Otro concepto clave es del riesgo, obtenido como una función de la probabilidad/frecuencia de un evento peligroso y la severidad de la consecuencia asociada.

En función del riesgo, para cada evento peligroso se especifica la función de seguridad necesaria para garantizar la seguridad funcional requerida y la reducción de riesgo necesaria.

A cada función de seguridad se le asociará un requisito de integridad de seguridad, que se traduce en la especificación de un nivel de integridad de seguridad (SIL) para cada función de seguridad de un sistema E/E/PE.

Se trata de niveles discretos, uno de cuatro posibles, donde el nivel de integridad de la seguridad SIL4 es el más alto nivel y el nivel de integridad de la seguridad SIL1 es el más bajo. Como características principales, podemos citar:

- Es una propiedad de la función de seguridad completa.
- Cada valor corresponde a un rango seleccionado de probabilidad de fallas de la función de seguridad.

- Es una medida cualitativa de la seguridad.
- Cuanto más alto el nivel SIL, más estrictos son los requerimientos técnicos y administrativos.

SIL	PFD	Fallo máx. aceptado del SIS
SIL 1	$\geq 10^{-2}$ a $< 10^{-1}$	un fallo peligroso en 10 años
SIL 2	$\geq 10^{-3}$ a $< 10^{-2}$	un fallo peligroso en 100 años
SIL 3	$\geq 10^{-4}$ a $< 10^{-3}$	un fallo peligroso en 1000 años
SIL 4	$\geq 10^{-5}$ a $< 10^{-4}$	un fallo peligroso en 10000 años

Figura 5: Niveles SIL según la probabilidad de fallo ante demanda

SIL	PFH (por hora)	Fallo máx. aceptado del SIS
SIL 1	$\geq 10^{-6}$ a $< 10^{-5}$	un fallo peligroso en 100.000 horas
SIL 2	$\geq 10^{-7}$ a $< 10^{-6}$	un fallo peligroso en 1.000.000 horas
SIL 3	$\geq 10^{-8}$ a $< 10^{-7}$	un fallo peligroso en 10.000.000 horas
SIL 4	$\geq 10^{-9}$ a $< 10^{-8}$	un fallo peligroso en 100.000.000 horas

Figura 6: Niveles SIL según la probabilidad de fallo por hora

4. Seguridad Funcional Aplicada a Túneles de Carretera

Como se comentaba inicialmente, existe abundante regulación asociada con la seguridad en túneles en todos sus aspectos (documental, gestión, operación, mantenimiento, etc.…).

Si bien la normativa IEC61508 también trata estos aspectos, no está clara la aportación que puede traer la aplicación de esta norma en aspectos ya regulados de modo sectorial. Sí parece que es en las fases más técnicas (especificación de requisitos, diseño y desarrollo, integración) donde esta norma puede aportar una metodología de gran valor. Dichos aspectos se tratan con detalle en las diversas partes de la norma.

A falta de realizar un análisis de mayor detalle en Comités de expertos, parece evidente que al menos los siguientes sistemas constan de alguna función de seguridad:

- Sistemas de detección de incendios
- Sistemas de ventilación
- Sistemas de cierre de barreras

Estos tres sistemas están compuestos por sistemas E/E/PE, a nivel de sensores, sistemas lógicos y actuadores, por lo que parece razonable pensar en la aplicación de criterios de seguridad funcional a la hora de la concepción del diseño.

Si bien todos ellos cuentan con sensores y actuadores, los sistemas lógicos que recogen los datos de dichos sensores y controlan los actuadores pueden formar parte de arquitecturas muy diferentes.

Adicionalmente, aparece otro elemento de gran importancia que es la red de comunicaciones así como el protocolo en si mismo que transporta los datos necesarios entre elementos.

Por otro lado, si consideramos la función de seguridad a nivel local evitando dependencias de controles remotos, no sólo debemos considerar el hardware que conforma la función de seguridad sino también el software del controlador programables locales el cual debe estar dotado de unas características especiales. Esto no significa la pérdida de control funcional desde Centro sino la capacidad del sistema local de actuar con seguridad en situaciones de riesgo o error en el sistema.

Existen diversas tecnologías, soluciones y modelos de seguridad pero, independientemente de las arquitecturas y tecnologías usadas hasta la fecha, la mayor aportación derivada de la aplicación de un estándar que tenga en cuenta los aspectos descritos, vendrá dada por el hecho de ayudar a sistematizar las tareas a realizar durante la realización de la solución con el fin de garantizar que se cumplen los niveles de integridad de seguridad deseados.

Como ejemplo, la adopción de normativa IEC61508 conllevaría el estudio detallado desde el punto de vista de la seguridad funcional de los elementos y procedimientos citados a lo largo del documento.

Sin pretender entrar a detalle en todo el conjunto de tareas a realizar que la normativa describe, al menos se debería contemplar lo siguiente:

- Asignación de funciones de seguridad a los diferentes elementos
- Establecimiento de requisitos para las funciones de seguridad

- Establecimiento de requisitos a nivel de integridad de seguridad (determinación de nivel SIL requerido)
- Planificación de los procedimientos de validación de la seguridad en funciones de seguridad
- Diseño y desarrollo de sistemas E/E/PE (esta fase es probablemente la que mayor impacto puede tener en cuanto al aseguramiento de la calidad, con las siguientes tareas a realizar)
  - o definición de restricciones de arquitectura
  - o establecimiento de requisitos a nivel de probabilidad de fallas peligrosas aleatorias a nivel de hardware
  - o establecimiento de requisitos para evitar fallas aleatorias de hardware
  - o establecimiento de requisitos para control de fallas sistemáticas
  - o a nivel de integridad de seguridad de hardware, selección de la arquitectura y técnicas que garantizan el cumplimiento de las restricciones de arquitectura y que las probabilidades de fallo de las funciones de seguridad cumplen con los objetivos deseados (técnicas definidas en Anexo A.2 del fascículo IEC61508-2)
  - o a nivel de integridad de seguridad sistemática, selección de caracterísi cas, técnicas y medidas que controlan y evitan la falla sistemática (técnicas definidas en Anexo A.3 del fascículo IEC61508-2)
  - o Establecimiento de requisitos sobre el comportamiento del sistema en caso de falla.
  - o Establecimiento de requisitos para la implantación del sistema E/E/PE.
  - o Establecimiento de requisitos para las comunicaciones de datos.
- Desarrollo de procedimientos de integración y testeo de los sistemas E/E/PE
- Desarrollo de procedimientos que garanticen que la seguridad funcional requerida se mantiene durante las fases de operación y mantenimiento.
- Validación de cumplimiento de los niveles de seguridad requeridos.

5. Conclusiones

Existe abundante normativa sectorial tanto a nivel europeo, como nacional, que viene siendo aplicada con éxito a lo largo de los últimos años.

Por otro lado, existe normativa genérica empleada en entornos en los cuales un evento peligroso puede provocar daños humanos, materiales o ambientales, muy centrada en los sistemas eléctricos y/o electrónicos y/o electrónico programables y que puede completar determinadas áreas no tratadas en detalle por las normativas sectoriales.

Parece razonable pensar que el estudio en detalle de dichas normativa, su contraste con la normativa genérica y la identificación de puntos complementarios puede ayudar a extender el conjunto de buenas prácticas seguidas hasta la fecha, redundando en un beneficio para todos los actores implicados en el sector del transporte por carretera.

También parece claro que en caso de aplicación de estándares de este tipo, sería necesaria una revisión de la arquitectura del sistema de control en su conjunto. Obviamente esta revisión requeriría de un profundo análisis en el Comité de expertos correspondiente donde se estudiara la funcionalidad degradada, los controladores locales y la capacidad de adaptación a la seguridad, las comunicaciones, etc.