Agencia Ferroviaria Europea	
Colección de ejemplos de evaluaciones de riesgos y de posibles herramientas de apoyo al Reglamento MCS	
Referencia en la Agencia Ferroviaria Europea:	ERA/GUI/02-2008/SAF
Versión en la Agencia Ferroviaria Europea:	1.1
Fecha:	06/01/2009

Documento elaborado por:	Agencia Ferroviaria Europea Boulevard Harpignies, 160 BP 20392 F-59307 Valenciennes Cedex Francia
Tipo de documento:	Guía
Estatus del documento:	Público

	Nombre	Cargo
Publicado por	Marcel VERSLYPE	Director Ejecutivo
Revisado por	Anders LUNDSTRÖM Thierry BREYNE	Jefe de la Unidad de Seguridad Jefe del Sector de Evaluación de la Seguridad
Escrito por (Autor)	Dragan JOVICIC	Unidad de Seguridad – Oficial de Proyecto

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

INFORMACIÓN SOBRE EL DOCUMENTO

Registro de modificaciones

Cuadro 1: Estatus del documento.

Fecha de la versión	Autor(es)	Número de sección	Descripción de la modificación
Título y estructura del antiguo documento: *"Orientaciones para el uso de la Recomendación sobre el primer paquete de MCS"*			
Versión 0.1 de las orientaciones 15/02/2007	Dragan JOVICIC	Todas	Primera versión de las "orientaciones de uso" asociada a la versión 1.0 de las "recomendaciones del primer paquete de MCS". Ésta es, asimismo, la primera versión del documento transmitido al grupo de trabajo de MCS para revisión formal.
Versión 0.2 de las orientaciones 07/06/2007	Dragan JOVICIC	Todas	Reorganización del documento para que se ajuste a la estructura de la versión 4.0 de la recomendación de MCS. Actualización con respecto al Proceso de revisión formal por el grupo de trabajo de MCS sobre la versión 1.0 de la recomendación.
		Todas	Actualización del documento con información adicional recopilada durante reuniones internas de la Agencia Ferroviaria Europea, así como con las solicitudes del equipo de trabajo y del grupo de trabajo de MCS para desarrollar nuevos apartados.
		Figura 1	Modificación de la figura que representa el "marco de gestión del riesgo para el primer paquete de Métodos Comunes de Seguridad" de acuerdo con los comentarios de la revisión y la terminología ISO.
Versión 0.3 de las orientaciones 20/07/2007	Dragan JOVICIC	Apéndices	Reorganización de apéndices y creación de nuevos apéndices. Nuevo apéndice que reúne todos los diagramas que ilustran y facilitan la lectura y comprensión de la Guía.
		Todas las secciones	Documento actualizado con el fin de: • desarrollar en la mayor medida posible las "x "secciones existentes; • desarrollar con mayor detalle lo que se entiende por "demostración del cumplimiento de los requisitos de seguridad por parte del sistema"; • crear un vínculo con el ciclo en V de CENELEC (es decir, la Figura 8 y la Figura 10 de EN 50 126); • desarrollar con mayor detalle la necesidad de colaboración y coordinación entre los diferentes agentes del sector ferroviario cuyas actividades puedan afectar en la seguridad del sistema ferroviario; • aportar aclaraciones acerca de las evidencias esperadas(por ejemplo, registro de peligros y análisis de seguridad) que demuestren a los organismos de evaluación la correcta aplicación del proceso de evaluación del riesgo del MCS; Documento actualizado asimismo de conformidad con una primera revisión interna de la Agencia.
Versión 0.4 de las orientaciones 16/11/2007	Dragan JOVICIC	Todas las secciones	Documento actualizado después del Proceso de revisión formal de conformidad con los comentarios recibidos sobre la versión 0.3 de los siguientes miembros del grupo de trabajo de MCS u organizaciones y acordado con los mismos durante llamadas telefónicas: • Autoridades nacionales de seguridad belga, española, finlandesa, noruega, francesa y danesa; • SIEMENS (miembro de UNIFE); • Administrador de la infraestructura noruego (Jernbaneverket – miembro de EIM).

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

Cuadro 1: Estatus del documento.

Fecha de la versión	Autor(es)	Número de sección	Descripción de la modificación
Versión 0.5 de las orientaciones 27/02/2008	Dragan JOVICIC	Todas las secciones	Documento actualizado de conformidad con los comentarios recibidos sobre la versión 0.3 de los siguientes miembros del grupo de trabajo de MCS u organizaciones, y acordado con los mismos durante llamadas telefónicas: • CER • Autoridad nacional de seguridad holandesa
		Todas las secciones	Documento actualizado de conformidad con la versión firmada de la recomendación de MCS. Documento actualizado de conformidad con los comentarios de la revisión interna de la Agencia formulados por Christophe CASSIR y Marcus ANDERSSON
		Todas las secciones Apéndices	Renumeración completa del párrafo del documento con respecto a la recomendación Inclusión de ejemplos de aplicación de la recomendación de MCS.
Título y estructura del nuevo documento: *"Recopilación de ejemplos de evaluaciones de riesgos y de posibles herramientas de apoyo al Reglamento MCS"*			
Versión 0.1 de la Guía 23/05/2008	Dragan JOVICIC	Todas	Primera versión del documento resultante de la división de la versión 0.5 de las "orientaciones de uso" en dos documentos complementarios.
Versión 0.2 de la Guía 03/09/2008	Dragan JOVICIC	Todas	Actualización del documento de conformidad con: • el Reglamento MCS de la Comisión Europea **Error! Reference source not found.**; • comentarios del taller de 1 de julio de 2008 con miembros del Comité de Interoperabilidad y Seguridad ferroviaria (RISC); • los comentarios de los miembros del grupo de trabajo de MCS (Autoridades nacionales de seguridad noruega, finlandesa, británica y francesa, CER, EIM, Jens BRABAND [UNIFE] y Stéphane ROMEI [UNIFE])
Versión 1.0 de la Guía 10/12/2008	Dragan JOVICIC	Todas	Actualización del documento de conformidad con el Reglamento MCS de la Comisión Europea sobre la evaluación del riesgo **Error! Reference source not found.** aprobado por el Comité de Interoperabilidad y Seguridad ferroviaria (RISC) durante su reunión plenaria de 25 de noviembre de 2008.
Versión 1.1 de la Guía 06/01/2009	Dragan JOVICIC	Todas	Actualización del documento de conformidad con los comentarios sobre el Reglamento MCS formulados por los servicios jurídico y lingüístico de la Comisión Europea.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

Índice

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

Lista de figuras

Lista de cuadros

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

0. INTRODUCCIÓN

0.1. Ámbito de aplicación

0.1.1. El objetivo del presente documento es ofrecer más precisiones acerca del "Reglamento de la Comisión relativo a la adopción de un método común de seguridad para la evaluación y valoración del riesgo con arreglo a lo dispuesto en el artículo 6 (3) (a) de la Directiva 2004/49/CE del Parlamento Europeo y del Consejo" {Ref. 3}. El Reglamento se denominará en el presente documento "Reglamento MCS".

0.1.2. Este documento no es jurídicamente vinculante y su contenido no debe interpretarse como la única manera de cumplir los requisitos del MCS. La finalidad del presente documento es complementar la guía para la aplicación del Reglamento MCS {Ref. 4} sobre cómo podría usarse y aplicarse el proceso del Reglamento MCS. Ofrece información práctica adicional, sin dictar con carácter obligatorio procedimientos que han de seguirse y sin establecer ninguna práctica jurídicamente vinculante . Esta información puede ser útil para todos los agentes[1] cuyas actividades puedan afectar en la seguridad de los sistemas ferroviarios que deben, directa o indirectamente, aplicar el MCS. El documento presenta ejemplos de evaluaciones de riesgos y posibles herramientas que apoyan la aplicación del MCS. Estos ejemplos se ofrecen únicamente a modo de asesoramiento y asistencia. Los agentes podrán usar métodos alternativos o podrán seguir empleando sus propios métodos y herramientas existentes para cumplir los requisitos del MCS, si consideran que responden mejor a los mismos.
Asimismo, los ejemplos y la información adicional que se ofrecen en este documento no son exhaustivos y no cubren todas las situaciones posibles en las que se proponen cambios significativos, por lo que el documento sólo puede considerarse como meramente informativo.

0.1.3. Este documento informativo deberá interpretarse únicamente como una ayuda adicional para la aplicación del Reglamento MCS. Cuando se utilice, este documento debe interpretarse en relación con el Reglamento MCS {Ref. 3} y la guía asociada {Ref. 4} para facilitar en mayor medida la aplicación del MCS, pero no sustituye al Reglamento MCS.

0.1.4. Este documento ha sido preparado por la Agencia Ferroviaria Europea con el apoyo de expertos de la asociación ferroviaria y del grupo de trabajo de MCS del órgano nacional de seguridad . Representa un conjunto desarrollado de ideas e información recabadas por la Agencia durante reuniones internas y reuniones con el grupo de trabajo MCS y equipos de trabajo de MCS. Cuando sea necesario, la Agencia Ferroviaria Europea revisará y actualizará el documento para que refleje los progresos realizados en relación con las normas europeas, los cambios introducidos en el Reglamento MCS sobre evaluación del riesgo y los posibles resultados obtenidos de la experiencia sobre el uso del Reglamento MCS. Dado que no es posible presentar un calendario para este proceso de revisión en el momento en que se redacta el presente documento, el lector deberá recurrir a la Agencia Ferroviaria Europea para obtener información acerca de la última edición disponible del documento.

---

(1) *Los agentes en cuestión son las entidades contratantes que se definen en la letra r) del artículo 2 de la Directiva 2008/57/CE sobre la interoperabilidad del sistema ferroviario dentro de la Comunidad, o los fabricantes, todos ellos definidos en el Reglamento como el "proponente", o sus proveedores y prestadores de servicios.*

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

0.2. Fuera del ámbito de aplicación

0.2.1. El presente documento no ofrece orientaciones sobre el modo de organizar, explotar o diseñar (y fabricar) un sistema ferroviario o partes del mismo. Tampoco define los acuerdos y disposiciones contractuales que pueden existir entre algunos agentes para la aplicación del proceso de gestión del riesgo. Las disposiciones contractuales específicas del proyecto no entran en el ámbito de aplicación del Reglamento MCS, al igual que la guía asociada y el presente documento.

0.2.2. Aunque estén fuera del ámbito de aplicación de este documento, las disposiciones que se acuerden entre los agentes afectados podrán anotarse en los contratos que corresponda al inicio del proyecto, sin perjuicio de las disposiciones del Reglamento MCS. Esto podría incluir, por ejemplo:

(a) los costes inherentes a la gestión de los riesgos relacionados con la seguridad en las interfaces entre los agentes;
(b) los costes inherentes a transferencias de peligros y medidas de seguridad asociadas entre los agentes que no se conozcan al inicio del proyecto;
(c) el modo de gestionar los conflictos que pudieran surgir durante el proyecto;
(d) etc.

En caso de que surjan desacuerdos o de que se produzca un conflicto entre el proponente y sus subcontratistas durante el desarrollo del proyecto, podrá hacerse referencia a los contratos que corresponda para ayudar a solucionar cualquier conflicto.

0.3. Principio para este documento

0.3.1. Si bien puede parecer que este documento es independiente a efectos de interpretación, no sustituye al Reglamento MCS {Ref. 3}**Error! Reference source not found.**. Para facilitar la consulta, en este documento se reproduce cada uno de los artículos del Reglamento MCS. En su caso, el artículo que corresponda se explica de antemano en la guía para la aplicación del Reglamento MCS {Ref. 4}. A continuación, se ofrece información adicional en los párrafos siguientes para ayudar a entender mejor el Reglamento MCS, en la medida en que se considere necesario.

*0.3.2. The articles and their underlying paragraphs from the CSM Regulation are copied in a text box in the present document using the "Bookman Old Style" Italic Font, the same as the present text. That formatting enables to easily distinguish the original text of the CSM Regulation {Ref. 3}**Error! Reference source not found.** from the additional explanations provided in this document. The text from the guide for the application of the CSM Regulation {Ref. 4} is not copied in the present document.*

0.3.3. La estructura del presente documento se ha trazado sobre la base de la estructura del Reglamento MCS y la guía asociada con el fin de ayudar al lector.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

0.4. Descripción del documento

0.4.1. Este documento se divide en las siguientes partes:

Capítulo 0, en el que se define el ámbito de aplicación del documento y se presenta la lista de documentos de referencia;
Anejo I y Anejo II, en los que se ofrece información adicional sobre las secciones correspondientes del Reglamento MCS {Ref. 3} y de la guía asociada {Ref. 4};
Nuevos apéndices, en los que se desarrollan en mayor detalle algunos aspectos específicos y se ofrecen ejemplos.

0.5. Documentos de referencia

Cuadro 2: Cuadro de documentos de referencia.

{Ref. Nº}	Título	Referencia	Versión
{Ref. 1}	Directiva 2004/49/CE del Parlamento Europeo y del Consejo, de 29 de abril de 2004, sobre la seguridad de los ferrocarriles comunitarios y por la que se modifican la Directiva 95/18/CE del Consejo sobre concesión de licencias a las empresas ferroviarias y la Directiva 2001/14/CE relativa a la adjudicación de la capacidad de infraestructura ferroviaria, aplicación de cánones por su utilización y certificación de la seguridad (Directiva de seguridad ferroviaria)	2004/49/CE DO L 164 de 30.4.2004, p. 44, corregida por DO L 220 de 21.6.2004, p. 16.	-
{Ref. 2}	Directiva 2008/57/CE del Parlamento Europeo y del Consejo, de 17 de junio de 2008, sobre la interoperabilidad del sistema ferroviario dentro de la Comunidad	2008/57/CE DO L 191 de 18.07.08, p.1	-
{Ref. 3}	Reglamento de la Comisión (CE) nº…/ de [...] relativo a la adopción de un método común de seguridad para la evaluación y valoración del riesgo con arreglo a lo dispuesto en el artículo 6 (3) (a) de la Directiva 2004/49/CE del Parlamento Europeo y del Consejo	xxxx/yy/CE	votada por el RISC el 25/11/2008
{Ref. 4}	Guía para la aplicación del Reglamento de la comisión sobre la adopción de un método común de seguridad para la evaluación y valoración del riesgo a que se refiere la letra a) del apartado 3 del artículo 6 de la Directiva de seguridad ferroviaria	ERA/GUI/01-2008/SAF	1.0
{Ref. 5}	Directiva 2008/57/CE del Parlamento Europeo y del Consejo, de 17 de junio de 2008, sobre la interoperabilidad del sistema ferroviario dentro de la Comunidad	2008/57/CE DO L 191 de 18.07.08, p.1	-
{Ref. 6}	Sistema de gestión de la seguridad - Criterios de evaluación de las empresas ferroviarias y los administradores de la infraestructura	Criterios de evaluación de los SGS Certificados y Autorizaciones de Seguridad de la Parte A	31/05/2007
{Ref. 7}	Aplicaciones ferroviarias–Sistemas de comunicación, señalización y procesamiento. Sistemas electrónicos de seguridad para la señalización	EN 50129	Febrero de 2003
{Ref. 8}	Aplicaciones ferroviarias–-Especificación y demostración de la, fiabilidad, disponibilidad, mantenebilidad y seguridad (RAMS). Parte 1:La propia norma	EN 50126-1	Septiembre de 2006
{Ref. 9}	Aplicaciones ferroviarias– Especificación y demostración de la fiabilidad, disponibilidad, mantenebilidad y seguridad (RAMS). Parte 2: Guía de aplicación de EN 50126-1 a efectos de seguridad	EN 50126-2 (Directriz)	Proyecto final (agosto de 2006)

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

Cuadro 2: Cuadro de documentos de referencia.

{Ref. Nº}	Título	Referencia	Versión
{Ref. 10}	Directriz general para el cálculo del riesgo inherente en el transporte de mercancías peligrosas por ferrocarril	Directriz de la OTIF aprobada por el Comité de expertos del RID	24 de noviembre de 2005
{Ref. 11}	Criterio de aceptación del riesgo para sistemas técnicos	Nota 01/08	1.1 (25/01/2008)
{Ref. 12}	Unidad de Seguridad de la Agencia Ferroviaria Europea: Estudio de viabilidad – "Distribución de objetivos de seguridad (a subsistemas de la ETI) y consolidación de la ETI desde un punto de vista de la seguridad" WP1.1 - Evaluación de la viabilidad de distribuir objetivos comunes de seguridad	WP1.1	1.0
{Ref. 13}	Aplicaciones ferroviarias– Sistema de clasificación de vehículos ferroviarios. EN 0015380 Parte 4: Grupo de funciones	EN 0015380 Parte 4	

0.6. Definiciones, términos y abreviaturas normalizados

0.6.1. Las definiciones, los términos y las abreviaturas generales utilizadas en el presente documento pueden encontrarse en un diccionario estándar.

0.6.2. Las definiciones, términos y abreviaturas nuevos que aparecen en esta guía se definen en las secciones que figuran más abajo.

0.7. Definiciones específicas

0.7.1. Véase el Artículo 3.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

0.8. Términos y abreviaturas específicos

0.8.1. En esta sección se definen los nuevos términos y abreviaturas específicos que se utilizan con frecuencia en el presente documento.

Cuadro 3: Cuadro de términos.

Término	Definición
Agencia	la Agencia Ferroviaria Europea
guía	la "guía para la aplicación del Reglamento de la Comisión nº…/ de [...] relativo a la adopción de un método común de seguridad para la evaluación y valoración del riesgo con arreglo a lo dispuesto en el artículo 6, apartado 3, letra a) de la Directiva 2004/49/CE del Parlamento Europeo y del Consejo
Reglamento MCS	el "Reglamento de la Comisión nº…/ de [...] relativo a la adopción de un método común de seguridad para la evaluación y valoración del riesgo con arreglo a lo dispuesto en el artículo 6, apartado 3, letra a) de la Directiva 2004/49/CE del Parlamento Europeo y del Consejo" {Ref. 3}

Cuadro 4: Cuadro de abreviaturas.

Abreviatura	Significado
CCS	Control Command and Signalling (Mando de control y señalización)
CE	Comisión Europea
ERA	European Railway Agency (Agencia Ferroviaria Europea)
ETI	Especificaciones técnicas de interoperabilidad
IM	Infrastructure Manager(s) (Administrador/es de la infraestructura)
ISA	Independent Safety Asesor (Evaluador independiente de seguridad)
MCS	Método(s) común(es) de seguridad
MS	Member State (Estado miembro)
NOBO	Notified Body (Organismo notificado)
NSA	National Safety Authority (Autoridad de seguridad nacional)
OCS	Objetivos comunes de seguridad
OTIF	Organización Intergubernamental para los Transportes Internacionales por Ferrocarril
QMP	Quality Management Process (Proceso de gestión de la calidad)
QMS	Quality Management System (Sistema de gestión de la calidad)
RISC	Railway Interoperability and Safety Committee (Comité sobre interoperabilidad y seguridad del ferrocarril)
RU	Railway Undertaking(s) (Empresa/s ferroviarias)
SGS	Sistema de gestión de la seguridad
SMP	Safety Management Process (Proceso de gestión de la calidad)
SRT	Safety in Railway Tunnels (Seguridad en los túneles ferroviarios)
TBC	To be completed (a completar)

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

EXPLICACIÓN DE LOS ARTÍCULOS DEL REGLAMENTO MCS

Artículo 1. Objeto

Artículo 1 (1)

This Regulation establishes a common safety method on risk evaluation and assessment (CSM) as referred to in Article 6(3)(a) of Directive 2004/49/EC.

[G 1] No se considera necesario ofrecer una explicación más detallada.

Artículo 1 (2)

The purpose of the CSM on risk evaluation and assessment is to maintain or to improve the level of safety on the Community's railways, when and where necessary and reasonably practicable. The CSM shall facilitate the access to the market for rail transport services through harmonisation of:

(a) the risk management processes used to assess the safety levels and the compliance with safety requirements;
(b) the exchange of safety-relevant information between different actors within the rail sector in order to manage safety across the different interfaces which may exist within this sector;
(c) the evidence resulting from the application of a risk management process.

[G 1] No se considera necesario ofrecer una explicación más detallada.

Artículo 2. Ámbito de aplicación

Artículo 2 (1)

The CSM on risk evaluation and assessment shall apply to any change of the railway system in a Member State, as referred to in point (2) (d) of Annex III to Directive 2004/49/EC, which is considered to be significant within the meaning of Article 4 of this Regulation. Those changes may be of a technical, operational or organisational nature. As regards organisational changes, only those changes which could impact the operating conditions shall be considered.

[G 1] El MCS se aplica a todo el sistema ferroviario, y comprende la evaluación de los siguientes cambios en los sistemas ferroviarios, si de la evaluación se desprende que son significativos con arreglo a la aplicación del Artículo 4:

(a) construcción de nuevas líneas o cambios de líneas existentes,
(b) introducción de sistemas técnicos nuevos y/o modificados;

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(c) cambios operativos (tales como normas operativas y procedimientos de mantenimiento nuevos o modificados);
(d) cambios dentro de las organizaciones de empresas ferroviarias y/o de administradores de la infraestructura.

En el MCS, el término “sistema” se refiere a todos los aspectos de un sistema, incluidos, entre otros, su desarrollo, explotación, mantenimiento, etc., hasta su desmantelamiento o retirada.

[G 2] El MCS cubre los cambios significativos de:

(a) sistemas “pequeños y sencillos” que podrían estar compuestos por pocos subsistemas o elementos técnicos, y,
(b) sistemas “grandes y más complejos” (que pueden incluir estaciones y túneles).

Artículo 2 (2)

Where the significant changes concern structural sub-systems to which Directive 2008/57/EC applies, the CSM on risk evaluation and assessment shall apply:

(a) if a risk assessment is required by the relevant technical specification for interoperability (TSI). In this case the TSI shall, where appropriate, specify which parts of the CSM apply;

(b) to ensure safe integration of the structural subsystems to which the TSIs apply into an existing system, by virtue of Article 15(1) of Directive 2008/57/EC.

However, application of the CSM in the case referred to in point (b) of the first subparagraph must not lead to requirements contradictory to those laid down in the relevant TSIs which are mandatory.

Nevertheless if the application of the CSM leads to a requirement that is contradictory to that laid down in the relevant TSI, the proposer shall inform the Member State concerned which may decide to ask for a revision of the TSI in accordance with Article 6(2) or Article 7 of Directive 2008/57/EC or a derogation in accordance with Article 9 of that Directive.

[G 1] Por ejemplo, de conformidad con la Directiva de seguridad ferroviaria {Ref. 1} y la Directiva de interoperabilidad ferroviaria {Ref. 2}, un nuevo tipo de material rodante para una línea de alta velocidad deberá ser compatible con la ETI “Material rodante de alta velocidad”. Aunque la ETI cubre la mayor parte del sistema objeto de evaluación, no incluye la cuestión clave de los factores humanos relacionada con el puesto de conducción. Por lo tanto, para garantizar que se identifiquen y controlen adecuadamente todos los peligros razonablemente previsibles relacionados con cuestiones relativas al factor humano (es decir, con las interfaces entre el maquinista, el material rodante y el resto del sistema ferroviario), se utilizará el proceso del MCS.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

Artículo 2 (3)

This Regulation shall not apply to:

(a) metros, trams and other light rail systems;
(b) networks that are functionally separate from the rest of the railway system and intended only for the operation of local, urban or suburban passenger services, as well as railway undertakings operating solely on these networks;
(c) privately owned railway infrastructure that exists solely for use by the infrastructure owner for its own freight operations;
(d) heritage vehicles that run on national networks providing that they comply with national safety rules and regulations with a view to ensuring safe circulation of such vehicles;
(e) heritage, museum and tourist railways that operate on their own network, including workshops, vehicles and staff.

[G 1] No se considera necesario ofrecer una explicación más detallada.

Artículo 2 (4)

This Regulation shall not apply to systems and changes, which, on the date of entry into force of this Regulation, are projects at an advanced stage of development within the meaning of Article 2 (t) of Directive 2008/57/EC.

[G 1] No se considera necesario ofrecer una explicación más detallada.

Artículo 3. Definiciones

For the purpose of this Regulation the definitions in Article 3 of Directive 2004/49/EC shall apply.

The following definitions shall also apply:

(1) 'risk' means the rate of occurrence of accidents and incidents resulting in harm (caused by a hazard) and the degree of severity of that harm (EN 50126-2);

(2) 'risk analysis' means systematic use of all available information to identify hazards and to estimate the risk (ISO/IEC 73);

(3) 'risk evaluation' means a procedure based on the risk analysis to determine whether the acceptable risk has been achieved (ISO/IEC 73);

(4) 'risk assessment' means the overall process comprising a risk analysis and a risk evaluation (ISO/IEC 73);

(5) 'safety' means freedom from unacceptable risk of harm (EN 50126-1);

(6) 'risk management' means the systematic application of management policies, procedures and practices to the tasks of analysing, evaluating and controlling risks (ISO/IEC 73);

(7) 'interfaces' means all points of interaction during a system or subsystem life cycle, including operation and maintenance where different actors of the rail sector will work together in order to manage the risks;

(8) 'actors' means all parties which are, directly or through contractual arrangements, involved in the application of this Regulation pursuant to Article 5 (2);

(9) 'safety requirements' means the safety characteristics (qualitative or quantitative) of a system and its operation (including operational rules) necessary in order to meet legal or company safety targets;

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(10) 'safety measures' means a set of actions either reducing the rate of occurrence of a hazard or mitigating its consequences in order to achieve and/or maintain an acceptable level of risk;

(11) 'proposer' means the railway undertakings or the infrastructure managers in the framework of the risk control measures they have to implement in accordance with Article 4 of Directive 2004/49/EC, the contracting entities or the manufacturers when they invite a notified body to apply the "EC" verification procedure in accordance with Article 18(1) of Directive 2008/57/EC or the applicant of an authorisation for placing in service of vehicles;

(12) 'safety assessment report' means the document containing the conclusions of the assessment performed by an assessment body on the system under assessment;

(13) 'hazard' means a condition that could lead to an accident (EN 50126-2);

(14) 'assessment body' means the independent and competent person, organisation or entity which undertakes investigation to arrive at a judgment, based on evidence, of the suitability of a system to fulfil its safety requirements;

(15) 'risk acceptance criteria' means the terms of reference by which the acceptability of a specific risk is assessed; these criteria are used to determine that the level of a risk is sufficiently low that it is not necessary to take any immediate action to reduce it further;

(16) 'hazard record' means the document in which identified hazards, their related measures, their origin and the reference to the organisation which has to manage them are recorded and referenced;

(17) 'hazard identification' means the process of finding, listing and characterising hazards (ISO/IEC Guide 73);

(18) 'risk acceptance principle' means the rules used in order to arrive at the conclusion whether or not the risk related to one or more specific hazards is acceptable;

(19) 'code of practice' means a written set of rules that, when correctly applied, can be used to control one or more specific hazards;

(20) 'reference system' means a system proven in use to have an acceptable safety level and against which the acceptability of the risks from a system under assessment can be evaluated by comparison;

(21) 'risk estimation' means the process used to produce a measure of the level of risks being analysed, consisting of the following steps: estimation of frequency, consequence analysis and their integration (ISO/IEC 73);

(22) 'technical system' means a product or an assembly of products including the design, implementation and support documentation; the development of a technical system starts with its requirements specification and ends with its acceptance; although the design of relevant interfaces with human behaviour is considered, human operators and their actions are not included in a technical system; the maintenance process is described in the maintenance manuals but is not itself part of the technical system;

(23) 'catastrophic consequence' means fatalities and/or multiple severe injuries and/or major damages to the environment resulting from an accident (Table 3 from EN 50126);

(24) 'safety acceptance' means status given to the change by the proposer based on the safety assessment report provided by the assessment body;

(25) 'system' means any part of the railway system which is subject to a change;

(26) 'notified national rule' means any national rule notified by Member States under Council Directive 96/48/EC(4), Directive 2001/16/EC of the European Parliament and the Council(5) and Directives2004/49/EC and 2008/57/EC.

(4) DO L 235, 17.9.1996, p. 6.

(5) DO L 110, 20.4.2001, p. 1.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

[G 1] No se considera necesario ofrecer una explicación más detallada.

Artículo 4. Cambios significativos

Artículo 4 (1)

If there is no notified national rule for defining whether a change is significant or not in a Member State, the proposer shall consider the potential impact of the change in question on the safety of the railway system.

When the proposed change has no impact on safety, the risk management process described in Article 5 does not need to be applied.

[G 1] Si no existe una norma nacional notificada, la decisión es responsabilidad del proponente. La importancia del cambio se basa en la opinión de expertos. Por ejemplo, si el cambio previsto en un sistema existente es complejo, puede considerarse significativo si existe un alto riesgo de que afecte en funciones existentes(6) del sistema, aunque el cambio en sí no esté necesariamente relacionado con la seguridad.

Artículo 4 (2)

When the proposed change has an impact on safety, the proposer shall decide, by expert judgement, the significance of the change based on the following criteria:

(a) failure consequence: credible worst-case scenario in the event of failure of the system under assessment, taking into account the existence of safety barriers outside the system;

(b) novelty used in implementing the change: this concerns both what is innovative in the railway sector, and what is new just for the organisation implementing the change;

(c) complexity of the change;

(d) monitoring: the inability to monitor the implemented change throughout the system life-cycle and take appropriate interventions;

(e) reversibility: the inability to revert to the system before the change;

(f) additionality: assessment of the significance of the change taking into account all recent safety-related modifications to the system under assessment and which were not judged as significant.

The proposer shall keep adequate documentation to justify his decision.

[G 1] **Ejemplo de pequeños cambios:** tras el desmantelamiento del sistema, el aumento una única vez de la velocidad máxima de la línea en 5 km/h podría no ser significativo. No obstante, si continúa aumentándose la velocidad máxima de la línea en intervalos de 5 km/h, la suma de los cambios sucesivos (considerados por separado como cambios no significativos) podría llegar a ser un cambio significativo con respecto a los requisitos de seguridad del sistema inicial.

(6) *Dado que las funciones de un sistema no son siempre independientes, los cambios introducidos en algunas funciones también pueden afectar en otras funciones del sistema, aunque pudiera parecer que no se ven directamente afectadas por los cambios.*

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

[G 2] Para determinar si una serie de cambios sucesivos (no significativos) es significativa, cuando se consideran en su conjunto, deben evaluarse todos los peligros y riesgos asociados vinculados a todos los cambios. La serie de cambios en cuestión puede considerarse no significativa si el riesgo resultante es ampliamente aceptable.

[G 3] La labor de la Agencia en materia de cambios significativos ha demostrado que:

(a) no es posible identificar umbrales o normas armonizados a partir de los cuales, en relación con un cambio dado, pueda adoptarse la decisión sobre la importancia del cambio, y;
(b) no es posible proporcionar una lista exhaustiva de cambios significativos;
(c) la decisión no puede ser válida para todos los proponentes y todas las condiciones técnicas, operativas, organizativas y ambientales

Así pues, resulta fundamental ceder la responsabilidad de la decisión a los proponentes, quienes, con arreglo al apartado 3 del artículo 4 de la Directiva de seguridad ferroviaria {Ref. 1}, son los responsables de la explotación segura del sistema y del control de los riesgos asociados con la parte del sistema que les compete.

[G 4] Para ayudar al proponente, en la sección C.2 del Apéndice C se ofrece un ejemplo de "valoración y uso de criterios".

[G 5] No deberá aplicarse el MCS si no se considera que un cambio relacionado con la seguridad es significativo. Pero esto no quiere decir que no haya que hacer nada. El proponente efectúa unos tipos de análisis (preliminares) de riesgos para decidir si el cambio es significativo. Es necesario documentar estos análisis de riesgos, así como cualesquier justificación y argumento, para que la Autoridad nacional de seguridad pueda llevar a cabo auditorías. La valoración de la importancia de un cambio, y la decisión de que un cambio no es significativo, no deberán ser objeto de una evaluación independiente por un organismo de evaluación.

Artículo 5. Proceso de gestión del riesgo

Artículo 5 (1)

The risk management process described in the Annex I shall apply:

(a) for a significant change as specified in Article 4, including the placing in service of structural sub-systems as referred to in Article 2(2)(b);
(b) where a TSI as referred to in Article 2(2)(a) refers to this Regulation in order to prescribe the risk management process described in Annex I.

[G 1] No se considera necesario ofrecer una explicación más detallada.

Artículo 5 (2)

The risk management process described in Annex I shall be applied by the proposer.

[G 1] No se considera necesario ofrecer una explicación más detallada.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

Artículo 5 (3)

The proposer shall ensure that risks introduced by suppliers and service providers, including their subcontractors, are managed. To this end, the proposer may request that suppliers and service providers, including their subcontractors, participate in the risk management process described in Annex I.

[G 1] No se considera necesario ofrecer una explicación más detallada.

Artículo 6. Evaluación independiente

Artículo 6 (1)

An independent assessment of the correct application of the risk management process described in Annex I and of the results of this application shall be carried out by a body which shall meet the criteria listed in Annex II. Where the assessment body is not already identified by Community or national legislation, the proposer shall appoint its own assessment body which may be another organisation or an internal department.

[G 1] El nivel de independencia que debe tener el organismo de evaluación depende del nivel de seguridad requerido para el sistema objeto de evaluación. En espera de la armonización de esta cuestión, las mejores prácticas a este respecto pueden encontrarse en la cláusula 8 de la norma IEC61508-1:2001 o en la sección 5.3.9. de la norma EN 50 129 {Ref. 7}. El grado de independencia depende de la gravedad de la consecuencia del peligro asociado con el equipo y de su novedad. En la sección 9.7.2 de las normas EN 50 126-2 y EN 50129 se define el nivel de independencia requerido para sistemas de señalización. En principio, esto podría aplicarse a otros sistemas.

[G 2] La Agencia todavía trabaja en la definición de las funciones y responsabilidades de los diferentes organismos de evaluación (la autoridad nacional de seguridad, el organismo notificado y el evaluador independiente de la seguridad) así como de las interfaces necesarias entre los mismos. Con ello se determinará cuál (de ser posible) de entre esos organismos de evaluación se encargará de qué y cómo lo hará. Al final, ello permitirá definir el modo de:

(a) comprobar, basándose en evidencias, que los procesos de gestión y evaluación del riesgo cubiertos por el MCS se aplican correctamente, y;
(b) apoyar al proponente en su decisión de aceptar el cambio significativo dentro del sistema objeto de evaluación.

Artículo 6 (2)

Duplication of work between the conformity assessment of the safety management system as required by Directive 2004/49/EC, the conformity assessment carried out by a notified body or a national body as required by Directive 2008/57/EC and any independent safety assessment carried out by the assessment body in accordance with this Regulation, shall be avoided.

[G 1] El trabajo de la Agencia en relación con la definición de las funciones y responsabilidades de los organismos de evaluación aportará información adicional.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

Artículo 6 (3)

The safety authority may act as the assessment body where the significant changes concern the following cases:

(a) where a vehicle needs an authorisation for placing in service, as referred to in Articles 22(2) and 24(2) of Directive 2008/57/EC;

(b) where a vehicle needs an additional authorisation for placing in service, as referred to in Articles 23(5) and 25(4) of Directive 2008/57/EC;

(c) where the safety certificate has to be updated due to an alteration of the type or extent of the operation, as referred to in Article 10(5) of Directive 2004/49/EC;

(d) where the safety certificate has to be revised due to substantial changes to the safety regulatory framework, as referred to in Article 10(5) of Directive 2004/49/EC;

(e) where the safety authorisation has to be updated due to substantial changes to the infrastructure, signalling or energy supply, or to the principles of its operation and maintenance, as referred to in Article 11(2) of Directive 2004/49/EC;

(f) where the safety authorisation has to be revised due to substantial changes to the safety regulatory framework, as referred to in Article 11(2) of Directive 2004/49/EC.

[G 1] No se considera necesario ofrecer una explicación más detallada.

Artículo 6 (4)

Where the significant changes concern a structural subsystem that needs an authorisation for placing in service as referred to in Article 15(1) or Article 20 of Directive 2008/57/EC, the safety authority may act as the assessment body unless the proposer already gave that task to a notified body in accordance with Article 18(2) of that Directive.

[G 1] No se considera necesario ofrecer una explicación más detallada.

Artículo 7. Informes de evaluación de la seguridad

Artículo 7 (1)

The assessment body shall provide the proposer with a safety assessment report.

[G 1] No se considera necesario ofrecer una explicación más detallada.

Artículo 7 (2)

In the case referred to in point (a) of Article 5(1), the safety assessment report shall be taken into account by the national safety authority in its decision to authorise the placing in service of subsystems and vehicles.

[G 1] No se considera necesario ofrecer una explicación más detallada.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

Artículo 7 (3)

In the case referred to in point (b) of Article 5(1), the independent assessment shall be part of the task of the notified body, unless otherwise prescribed by the TSI.
If the independent assessment is not part of the task of the notified body, the safety assessment report shall be taken into account by the notified body in charge of delivering the conformity certificate or by the contracting entity in charge of drawing up the EC declaration of verification.

[G 1] No se considera necesario ofrecer una explicación más detallada.

Artículo 7 (4)

When a system or part of a system has already been accepted following the risk management process specified in this Regulation, the resulting safety assessment report shall not be called into question by any other assessment body in charge of performing a new assessment for the same system. The recognition shall be conditional on demonstration that the system will be used under the same functional, operational and environmental conditions as the already accepted system, and that equivalent risk acceptance criteria have been applied.

[G 1] Este principio del reconocimiento mutuo ya ha sido aceptado por las normas CENELEC: véanse la sección 5.5.2 de la norma EN 50 129 y la sección 5.9 de la norma EN 50 126-2. En las normas CENELEC, los proponentes o evaluadores independientes de la seguridad aplican el principio de la aceptación cruzada o del reconocimiento mutuo a productos genéricos o aplicaciones genéricas[7], siempre que la evaluación de la seguridad y la demostración de la seguridad se efectúen de conformidad con los requisitos de las normas CENELEC.

[G 2] El reconocimiento mutuo también deberá aplicarse para la aceptación de sistemas nuevos o modificados si la evaluación del riesgo de los mismos y la demostración del cumplimiento de los requisitos de seguridad por parte del sistema se efectúan con arreglo a las disposiciones del Reglamento MCS {Ref. 3}

Artículo 8. Gestión del control del riesgo/auditorías internas y externas

Artículo 8 (1)

The railway undertakings and infrastructure managers shall include audits of application of the CSM on risk evaluation and assessment in their recurrent auditing scheme of the safety management system as referred to in Article 9 of Directive 2004/49/EC.

[G 1] No se considera necesario ofrecer una explicación más detallada.

---

[7] *Véase el apartado [G 5] de la sección 1.1.5 y las notas a pie de página (9) y (10) en la página 30, así como el Figura 3, del presente documento para obtener una explicación más detallada de los términos "producto genérico y aplicación genérica" y los principios inherentes.*

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

Artículo 8 (2)

Within the framework of the tasks defined in Article 16(2)(e) of Directive 2004/49/EC, the national safety authority shall monitor the application of the CSM on risk evaluation and assessment.

[G 1] No se considera necesario ofrecer una explicación más detallada.

Artículo 9. Información y progresos técnicos

Artículo 9 (1)

Each infrastructure manager and each railway undertaking shall, in its annual safety report referred to in Article 9(4) of Directive 2004/49/EC, report briefly on its experience with the application of the CSM on risk evaluation and assessment. The report shall also include a synthesis of the decisions related to the level of significance of the changes.

[G 1] No se considera necesario ofrecer una explicación más detallada.

Artículo 9 (2)

Each national safety authority shall, in its annual safety report referred to in Article 18 of Directive 2004/49/EC, report on the experience of the proposers with the application of the CSM on risk evaluation and assessment, and, where appropriate, its own experience.

[G 1] No se considera necesario ofrecer una explicación más detallada.

Artículo 9 (3)

The European Railway Agency shall monitor and collect feedback on the application of the CSM on risk evaluation and assessment and, where applicable, shall make recommendations to the Commission with a view to improving it.

[G 1] No se considera necesario ofrecer una explicación más detallada.

Artículo 9 (4)

The European Railway Agency shall submit to the Commission by 31 December 2011 at the latest, a report which shall include:

(a) an analysis of the experience with the application of the CSM on risk evaluation and assessment, including cases where the CSM has been applied by proposers on a voluntary basis before the relevant date of application provided for in Article 10;
(b) an analysis of the experience of the proposers concerning the decisions related to the level of significance of the changes;
(c) an analysis of the cases where codes of practice have been used as described in section

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

2.3.8 of Annex I;

(d) an analysis of overall effectiveness of the CSM on risk evaluation and assessment.

The safety authorities shall assist the Agency by identifying cases of application of the CSM on risk evaluation and assessment.

[G 1] No se considera necesario ofrecer una explicación más detallada.

Artículo 10. Entrada en vigor

Artículo 10 (1)

This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.

[G 1] No se considera necesario ofrecer una explicación más detallada.

Artículo 10 (2)

This Regulation shall apply from 1 July 2012.

However, it shall apply from 19 July 2010:

(a) to all significant technical changes affecting vehicles as defined in Article 2 (c) of Directive 2008/57/EC;

(b) to all significant changes concerning structural sub-systems, where required by Article 15(1) of Directive 2008/57/EC or by a TSI.

[G 1] No se considera necesario ofrecer una explicación más detallada.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

ANEXO I – EXPLICACIÓN DEL PROCESO PREVISTO EN EL REGLAMENTO MCS

1. PRINCIPIOS GENERALES APLICABLES AL PROCESO DE GESTIÓN DEL RIESGO

1.1. Principios y obligaciones generales

1.1.1. The risk management process covered by this Regulation shall start from a definition of the system under assessment and comprise the following activities:

(a) the risk assessment process, which shall identify the hazards, the risks, the associated safety measures and the resulting safety requirements to be fulfilled by the system under assessment;
(b) demonstration of the compliance of the system with the identified safety requirements and;
(c) management of all identified hazards and the associated safety measures.

This risk management process is iterative and is depicted in the diagram of the Appendix (of the CSM Regulation)*. The process ends when the compliance of the system with all safety requirements necessary to accept the risks linked to the identified hazards is demonstrated.*

[G 1] El marco de gestión del riesgo del MCS y el proceso de evaluación del riesgo asociado se ilustran en la Figura 1. Cuando se considere necesario, cada recuadro o actividad de esta figura se describe en mayor detalle en una sección específica del presente documento.

[G 2] CENELEC aconseja que los procesos de gestión del riesgo y evaluación del riesgo se describan en un plan de seguridad. Con todo, si no resulta apropiado para el proyecto, la descripción asociada puede incluirse en cualquier otro documento pertinente. Véase la sección 1.1.6.

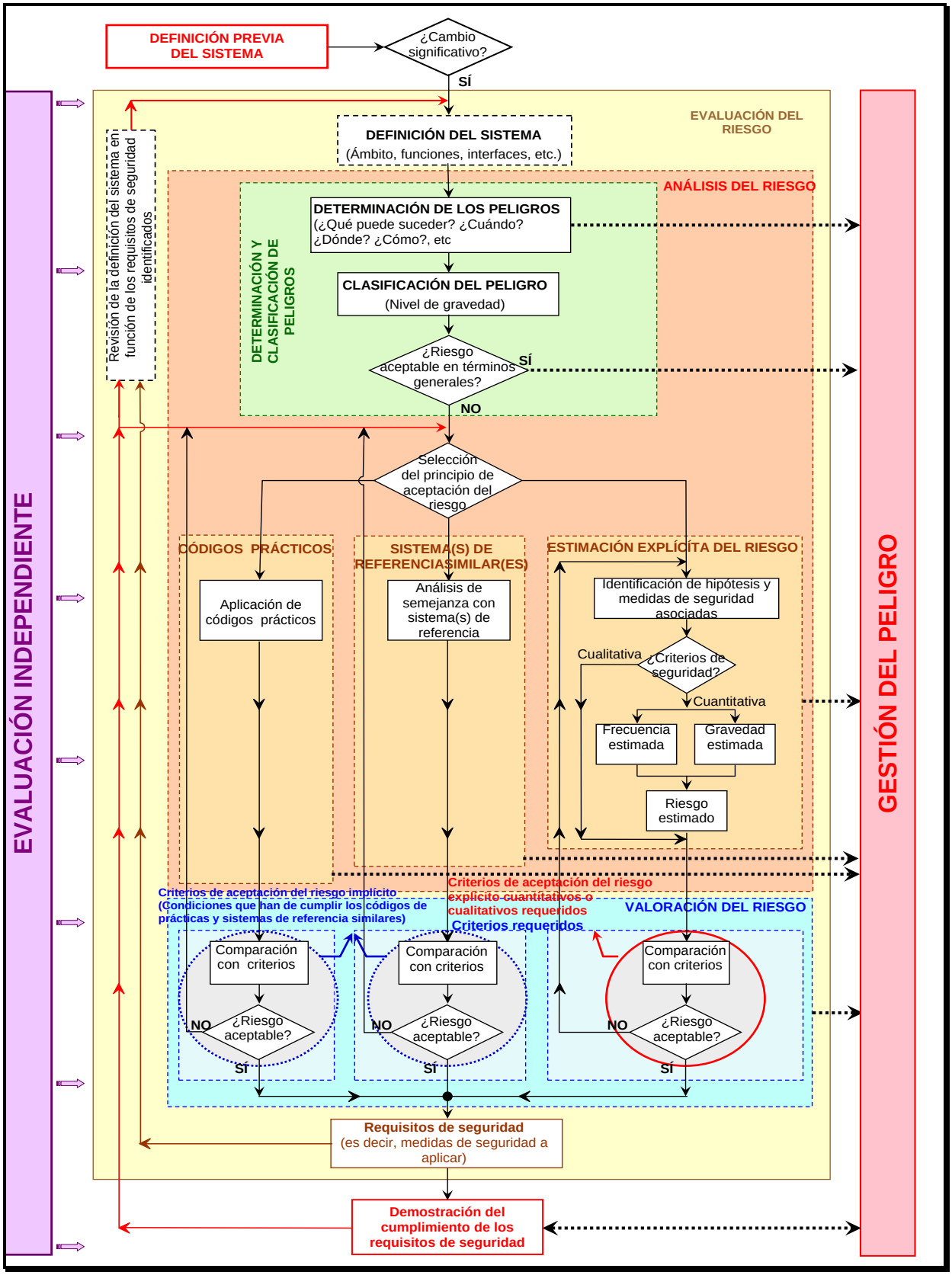
European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

[G 3] El proceso de evaluación del riesgo se inicia con una definición preliminar del sistema. Durante el desarrollo del proyecto, la definición preliminar del sistema se actualiza progresivamente y se sustituye por la definición del sistema. Si no hubiera definición preliminar del sistema, se emplearía la definición oficial del sistema para realizar la evaluación del riesgo, en cuyo caso, convendría que todas los agentes afectados por el cambio significativo se reunieran al inicio del proyecto con el fin de:

(a) acordar los principios generales del sistema, las funciones del sistema, etc. En principio, estos aspectos podrían describirse en una definición preliminar del sistema;
(b) acordar la organización del proyecto;
(c) acordar el reparto de las funciones y responsabilidades entre los diferentes agentes ya afectados, incluidos la autoridad nacional de seguridad, el organismo notificado y el evaluador independiente de la seguridad, cuando proceda.

Este tipo de coordinación, por ejemplo, durante la definición preliminar del sistema, ofrece al proponente, a los subcontratistas, a la autoridad nacional de seguridad, al organismo notificado y al evaluador independiente de la seguridad, si procede, la oportunidad de acordar en una fase temprana los códigos prácticos o sistemas de referencia cuyo empleo es aceptable en el marco del proyecto

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu



European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

Figura 1: Marco de gestión del riesgo en el Reglamento MCS {Ref. 3}.

1.1.2. This iterative risk management process:

(a) shall include appropriate quality assurance activities and be carried out by competent staff;
(b) shall be independently assessed by one or more assessment bodies.

[G 1] El sistema de gestión de la seguridad de la empresa ferroviaria y del administrador de la infraestructura establece los procesos y procedimientos que:

(a) controlan que el sistema siga siendo seguro durante todo su ciclo vital (es decir, durante su explotación y mantenimiento);
(b) garantizan un desmantelamiento o una sustitución segura del sistema en cuestión.

Este proceso no forma parte del MCS de evaluación del riesgo.

[G 2] Para aplicar el MCS, es necesario que todas las partes afectadas sean competentes (es decir, que posean las cualificaciones, los conocimientos y la experiencia adecuados). Existe una necesidad constante para gestionar la competencia en el seno de la organización de las partes del sector ferroviario:

(a) por lo que respecta a los administradores de la infraestructura y las empresas ferroviarias, esta necesidad queda cubierta por su sistema de gestión de la seguridad en virtud de la letra e) del apartado 2 del Anexo III de la Directiva de seguridad ferroviaria {Ref. 1};
(b) por lo que respecta a las otros agentes cuyas actividades podrían inafectar a la seguridad del sistema ferroviario, aunque el sistema de gestión de la seguridad no sea obligatorio, en general, al menos en el nivel del proyecto (véase el apartado [G 1] de la sección 5.1), cuentan con un proceso de gestión de la calidad y/o un proceso de gestión de la seguridad que cubre este requisito.

[G 3] Las secciones de la norma CENELEC EN 50 126-1 {Ref. 8} que se exponen a continuación sirven de orientación en materia de competencia:

(a) en virtud de la letra b) de la sección 5.3.5.: *"todo el personal que tenga responsabilidades en el marco del proceso de gestión"* del riesgo debe ser *"competente para desempeñar dichas responsabilidades"*;
(b) letra d) de la sección 5.3.5.: los requisitos relativos a la gestión del riesgo y la evaluación del riesgo deben *"ponerse en práctica en el marco de procesos de negocio apoyados por un sistema de gestión de la calidad que cumpla los requisitos de la norma EN ISO 9001, EN ISO 9002 o EN ISO 9003 adecuados al sistema objeto de"* evaluación. En la sección 5.2. de la norma EN 50 129 {Ref. 7} se ofrece un ejemplo de aspectos controlados por el sistema de gestión de la calidad.

Éstos incluyen las actividades adecuadas de aseguramiento de la calidad, así como la competencia y formación del personal o de las personas, requeridas para apoyar el proceso cubierto por el MCS.

[G 4] Con frecuencia, un organismo de evaluación realiza un seguimiento del proceso de evaluación del riesgo desde el mismo comienzo del proyecto; sin embargo, salvo que así lo exija la legislación nacional de un Estado miembro, tal implicación temprana del organismo de evaluación no es obligatoria, aunque sí aconsejable. El dictamen del organismo de evaluación independiente podría ser útil antes de pasar de una fase de la evaluación del

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

riesgo a la siguiente. Véase el Artículo 6 para obtener más detalles sobre la evaluación independiente.

1.1.3. The proposer in charge of the risk management process required by this Regulation shall maintain a hazard record according to section 4.

[G 1] No se considera necesario ofrecer una explicación más detallada.

1.1.4. The actors who already have in place methods or tools for risk assessment may continue to apply them as far as they are compatible with the provisions of this Regulation and subject to the following conditions:

(a) the risk assessment methods or tools are described in a safety management system which has been accepted by a national safety authority in accordance with Article 10(2)(a) or Article 11(1)(a) of Directive 2004/49/EC, or;

(b) the risk assessment methods or tools are required by a TSI or comply with publicly available recognised standards specified in notified national rules.

[G 1] La Figura 2 representa la relación existente entre el MCS y los “sistemas de gestión de la seguridad y procesos de evaluación del riesgo”.

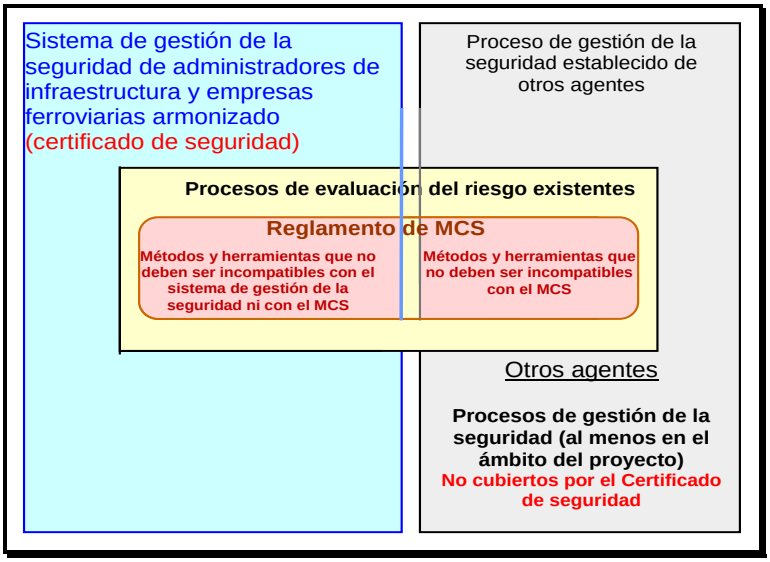


Figura 2: Sistema de gestión de la seguridad y MCS armonizados.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

1.1.5. Without prejudice to civil liability in accordance with the legal requirements of the Member States, the risk assessment process shall fall within the responsibility of the proposer. In particular the proposer shall decide, with agreement of the actors concerned, who will be in charge of fulfilling the safety requirements resulting from the risk assessment. This decision shall depend on the type of safety measures selected to control the risks to an acceptable level. The demonstration of compliance with the safety requirements shall be conducted according to section 3.

[G 1] Si el proponente es un administrador de la infraestructura o una empresa ferroviaria, a veces podría ser necesario hacer partícipes a otros agentes en el proceso [8] (véase la sección 1.2.1). En algunos casos, el administrador de la infraestructura o la empresa ferroviaria puede subcontratar, parcialmente o en su totalidad, las actividades de evaluación del riesgo. Las funciones y responsabilidades para cada agente suelen acordarse entre los agentes afectados en una fase temprana del proyecto.

[G 2] Es importante señalar que, en cualquier caso, el proponente sigue siendo responsable de la aplicación del MCS, de la aceptación del riesgo y, por tanto, de la seguridad del sistema. Dicha responsabilidad incluirá garantizar que:

(a) exista plena cooperación entre los agentes afectados, de modo que se facilite toda la información necesaria, y;
(b) quede claro quién debe cumplir los requisitos particulares del MCS (por ejemplo, efectuar el análisis de riesgos o gestionar el registro de peligros).

En caso de desacuerdo entre los agentes acerca de los requisitos de seguridad que deben cumplir, se podría consultar para el dictamen a la Autoridad nacional de seguridad. No obstante, la responsabilidad de encontrar una solución sigue recayendo en el proponente y no puede transferirse a la Autoridad nacional de seguridad: véase, asimismo, la sección 0.2.2.

[G 3] Si se subcontrata la tarea, el subcontratista no tendrá la obligación de tener su propia organización de seguridad en caso de que éste no sea un administrador de la infraestructura o una empresa ferroviaria, o especialmente si la estructura o tamaño del subcontratista es reducido o si su contribución al sistema global es limitada. La responsabilidad de la gestión del riesgo, incluidas las actividades de evaluación del riesgo y gestión del peligro, puede recaer en la organización de nivel superior (es decir, en el cliente del subcontratista). No obstante, el subcontratista siempre es responsable de facilitar la información adecuada relacionada con sus actividades, necesaria para constituir la documentación relativa a la gestión del riesgo para la organización de nivel superior.
Las organizaciones que cooperen también pueden acordar la creación de una organización de seguridad común, por ejemplo, para optimizar los costes. En ese caso, una sola organización gestionará las actividades de seguridad de todas las organizaciones implicadas. La responsabilidad de la fidelidad de la información (es decir, los peligros, los riesgos y las medidas de seguridad), así como de la gestión de la aplicación de las medidas de seguridad, recae en la organización encargada de controlar los peligros asociados a estas medidas de seguridad.

(8) *Ello es conforme con lo establecido en el Apéndice A.4 de la norma CENELEC 50 129 {Ref. 7}.*

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

[G 4] Normalmente, el proponente establecería los "niveles de seguridad" y "requisitos de seguridad" asignados a los agentes afectados en el proyecto y a los diferentes subsistemas y equipos de dichos agentes:

(a) en los contratos entre el proponente y los agentes correspondientes (subcontratistas);
(b) en un plan de seguridad, o cualquier otro documento pertinente que tenga la misma finalidad, en el que se describan la organización del proyecto general y las responsabilidades de cada agente, incluidas las del propio proponente: véase la sección 1.1.6;
(c) en el registro o los registros de peligros del proponente: véase la sección 4.1.1.

Esta asignación de "niveles de seguridad" y "requisitos de seguridad" del sistema a los subsistemas y equipos subyacentes, y, por lo tanto, a los agentes correspondientes, incluido el propio proponente, puede mejorarse o ampliarse durante la "fase de demostración del cumplimiento de los requisitos de seguridad por parte del sistema": véase la Figura 1. En comparación con el ciclo en V de CENELEC (véanse la sección 2.1.1 y la Figura 5 en la página 35), esta actividad corresponde a la Fase 5, que se ocupa de la "distribución de requisitos del sistema" a los diferentes subsistemas y componentes.

[G 5] El Artículo 1.Artículo 5 (2) permite que otros agentes distintos de la empresa ferroviaria o del administrador de la infraestructura asuman la responsabilidad general del cumplimiento del MCS en función de sus respectivas necesidades. Por lo que respecta a los productos genéricos o las aplicaciones genéricas(9), por ejemplo, el fabricante puede realizar la evaluación del riesgo basándose en una "definición genérica del sistema" para especificar los niveles de seguridad y los requisitos de seguridad que deberán cumplir los productos genéricos y las aplicaciones genéricas.

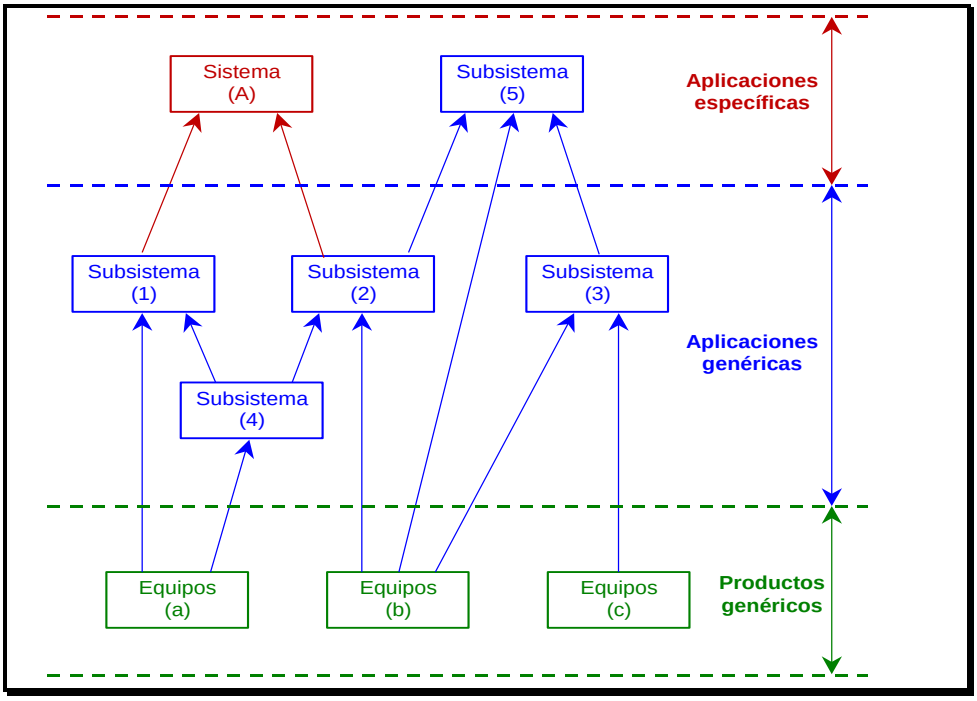


Figura 3: Ejemplos de relaciones de dependencia entre casos de seguridad (extraídos de la Figura 9 de la norma EN 50 129).

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

[G 6] CENELEC aconseja que el fabricante facilite las evidencias documentales de la evaluación del riesgo, en casos de seguridad, y en registros de peligros de un producto genérico (y de una aplicación genérica[9], respectivamente). Estos casos de seguridad y registros de peligros recogen todos los supuestos[10] e identifican "restricciones de uso" (es decir, condiciones de aplicación relacionadas con la seguridad) que son aplicables a los productos genéricos de que se trate (y a la aplicación genérica, respectivamente). Por lo tanto, en los casos en que se utilice un producto genérico o una aplicación genérica en el funcionamiento de una aplicación específica, es necesario demostrar, en cada aplicación, el cumplimiento de todos los supuestos[9] y las "restricciones de uso" (o condiciones de aplicación relacionadas con la seguridad).

1.1.6. The first step of the risk management process shall be to identify in a document, to be drawn up by the proposer, the different actors' tasks, as well as their risk management activities. The proposer shall coordinate close collaboration between the different actors involved, according to their respective tasks, in order to manage the hazards and their associated safety measures.

---

(9) *Los términos "aplicación genérica" y "casos de seguridad de un producto genérico" empleados por CENELEC se reutilizan en los casos en que puedan contemplarse tres categorías diferentes de casos de seguridad (véase Figura 3):*

- *(a)* ***Caso de seguridad de un producto genérico*** *(independiente de la aplicación). Un producto genérico puede reutilizarse para diferentes aplicaciones independientes;*
- *(b)* ***Caso de seguridad de una aplicación genérica*** *(para una clase de aplicación). Una aplicación genérica puede reutilizarse para una clase o un tipo de aplicación con funciones comunes;*
- *(c)* ***Caso de seguridad de una aplicación específica*** *(para una aplicación específica). Se utiliza una aplicación específica para una sola instalación en particular.*

Para obtener más información acerca de su interdependencia, véanse la sección 9.4. y la Figura 9.1 de la Directriz CENELEC 50 126-2 {Ref. 9}.

(10) *Estos supuestos y restricciones de uso determinan los límites y la validez de las "evaluaciones de la seguridad" y los "análisis de la seguridad" asociados a los casos de seguridad de un producto genérico y una aplicación genérica de que se trate. Si la aplicación específica de que se trate no los cumple, es necesario actualizar o sustituir las "evaluaciones de la seguridad" y los "análisis de la seguridad" que correspondan (por ejemplo, análisis causales) por otros nuevos.*

> *Ello se ajusta al siguiente principio general de la seguridad: "En los casos en que el proyecto de un (sub)sistema específico se base en aplicaciones genéricas y productos genéricos, deberá demostrarse que el (sub)sistema específico cumple todos los supuestos y restricciones de uso (denominados condiciones de aplicación relacionadas con la seguridad en CENELEC) que se exportan en los casos de seguridad de un productos genérico o una aplicación genérica que correspondan (véase Figura 3)"*

Si, para una aplicación específica, no es posible cumplir algunos supuestos y restricciones de uso a nivel de un subsistema (por ejemplo, en caso de requisitos de seguridad operativos), pueden transferirse los supuestos y restricciones de uso que correspondan a un nivel superior (es decir, normalmente al nivel del sistema). A continuación, estos supuestos y restricciones de uso se identifican claramente en el "caso de seguridad de una aplicación específica" del subsistema de que se trate. Esto es fundamental para garantizar, en esos ejemplos de dependencia, que las condiciones de aplicación relacionadas con la seguridad de cada caso de seguridad se cumplan en el caso de seguridad de nivel superior, o bien se incluyan en las condiciones de aplicación relacionadas con la seguridad del caso de seguridad de más alto nivel (es decir, el caso de seguridad del sistema).

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

[G 1] Con frecuencia, salvo que se acuerde otra cosa en los contratos al inicio del proyecto, cada proyecto incluye un documento en el que se describen las actividades de gestión del riesgo. El documento en cuestión se actualiza y revisa en caso de que se produzcan modificaciones significativas en el sistema original.

[G 2] En dicho documento se establecen la estructura organizativa, las responsabilidades asignadas al personal, los procesos, los procedimientos y las actividades que, conjuntamente, garantizan el cumplimiento de los niveles de seguridad y los requisitos de seguridad especificados por parte del sistema objeto de evaluación. Este documento debe cumplir el MCS, dado que sirve de apoyo y ofrece orientaciones al organismo de evaluación. Las normas CENELEC aconsejan que este tipo de información se incluya en un plan de seguridad o en otro documento que dedique una parte a esas cuestiones.

[G 3] En el plan de seguridad del proponente, en particular, o en cualquier otro documento pertinente, se presenta la organización general del proyecto y se describe la manera en que se distribuyen las funciones y responsabilidades entre los agentes afectados. Para obtener información detallada, puede hacerse referencia a los planes de seguridad u organizaciones de seguridad de las diferentes partes involucradas. Normalmente, la distribución de responsabilidades entre las diferentes partes se debate y acuerda durante la definición preliminar del sistema (es decir, al inicio del proyecto), en su caso.

[G 4] El plan de seguridad es un documento vivo que se actualiza cuando proceda durante la vida del proyecto.

[G 5] Puede obtenerse más información en la norma EN 50 126-1 {Ref. 8} y su Directriz 50 126-2 asociada {Ref. 9} acerca del contenido de un plan de seguridad.

1.1.7. Evaluation of the correct application of the risk management process described in this Regulation falls within the responsibility of the assessment body.

[G 1] No se considera necesario ofrecer una explicación más detallada.

1.2. Gestión de las interfaces

1.2.1. For each interface relevant to the system under assessment and without prejudice to specifications of interfaces defined in relevant TSIs, the rail-sector actors concerned shall cooperate in order to identify and manage jointly the hazards and related safety measures that need to be handled at these interfaces. The management of shared risks at the interfaces shall be co-ordinated by the proposer.

[G 1] Por ejemplo, si por razones operativas una empresa ferroviaria necesita que un administrador de la infraestructura realice determinados cambios en la infraestructura, en virtud de los requisitos de la letra g) del apartado 2 del Anexo III de la Directiva de seguridad ferroviaria {Ref. 1}, la empresa ferroviaria también controlará esas actividades para garantizar la correcta realización de los cambios previstos. No obstante, el liderazgo de la empresa ferroviaria no elimina la responsabilidad del administrador de la infraestructura en cuestión de informar a las otras empresas ferroviarias si éstas también se ven afectadas por el correspondiente cambio de la infraestructura. Puede que el administrador de la

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

infraestructura tenga incluso que llevar a cabo una evaluación del riesgo, de conformidad con el MCS, si el cambio en cuestión es significativo desde su punto de vista.

[G 2] Las transferencias de responsabilidades entre las diferentes agentes son posibles y, en algunas circunstancias, incluso necesarias. No obstante, cuando en un sistema intervienen diversos agentes, a menudo se designa a uno de ellos el responsable del sistema global. Siempre existen relaciones de dependencia entre subsistemas y operaciones que requieren esfuerzos especiales para identificarlas. Así pues, es necesario que alguien asuma la responsabilidad general de los análisis de la seguridad y obtenga, asimismo, pleno acceso a toda la documentación pertinente. Evidentemente, el proponente que pretenda introducir el cambio significativo es, en términos generales, responsable de que la evaluación del riesgo sea sistemática y completa.

[G 3] Los principales criterios que deben acordarse para la gestión de una interfaz entre las partes implicadas son:

(a) el liderazgo, que a menudo garantiza el proponente que pretende introducir el cambio significativo;
(b) los datos requeridos;
(c) los métodos para la determinación del peligro y la evaluación del riesgo;
(d) los participantes que se requieren con la competencia necesaria (es decir, una combinación de conocimientos, cualificaciones y experiencia práctica – véase, asimismo, la definición de “competencia del personal” en la letra b) del apartado [G 2] del artículo 3 de {Ref. 4});
(e) los resultados previstos.

Estos criterios se describen en los planes de seguridad (o en cualquier otro documento pertinente) de las empresas que se ocupan de las interfaces en cuestión.

[G 4] En la sección C.3. del Apéndice C se ofrecen ejemplos de interfaces, así como un ejemplo de la aplicación de esos criterios principales respecto a la gestión de la interfaz entre un fabricante de tren y un administrador de la infraestructura o una empresa ferroviaria.

[G 5] En la gestión de la interfaz también deben tenerse en cuenta los riesgos que podrían aparecer en las interfaces con la interacción humana(utilizados durante las operaciones de explotación y mantenimiento) para el diseño de esas interfaces.

1.2.2. When, in order to fulfil a safety requirement, an actor identifies the need for a safety measure that it cannot implement itself, it shall, after agreement with another actor, transfer the management of the related hazard to the latter using the process described in section 4.

[G 1] El proceso de transferencia de peligros y medidas de seguridad asociadas entre los agentes también es aplicable a niveles inferiores del ciclo en V de CENELEC, como se muestra en la Figura 1 de la página 35. Por ejemplo, puede aplicarse, en la medida de lo necesario, para intercambiar esa información entre un agente y sus subcontratistas, La diferencia con el mismo proceso a nivel del sistema reside en que el proponente no debe estar informado de todas las transferencias de peligros y medidas de seguridad asociadas a nivel del subsistema. Sólo se mantiene informado al proponente cuando los peligros transferidos y las medidas de seguridad asociadas están relacionados con interfaces de alto nivel (es decir, cuando afectan a una interfaz con el proponente).

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

1.2.3. For the system under assessment, any actor who discovers that a safety measure is non-compliant or inadequate is responsible for notifying it to the proposer, who shall in turn inform the actor implementing the safety measure.

[G 1] El sistema de gestión de la seguridad de la empresa ferroviaria y el administrador de la infraestructura cubre las disposiciones y procedimientos que permiten garantizar la correcta gestión de los incumplimientos o insuficiencias de las medidas de seguridad. Por lo tanto, estas disposiciones y procedimientos no forman parte del MCS.

[G 2] Asimismo, las disposiciones y procedimientos(11) que deberán establecer otros agentes(12) para garantizar que los incumplimientos e insuficiencias de las medidas de seguridad se gestionen correctamente y, de ser necesario, que las medidas de seguridad se transfieran a todos los agentes, que sean acordadas al inicio del proyecto y se detallen en su plan de seguridad: véase la sección 0.2. Fuera del ámbito de aplicación

1.2.4. The actor implementing the safety measure shall then inform all the actors affected by the problem either within the system under assessment or, as far as known by the actor, within other existing systems using the same safety measure.

[G 1] Ello permitirá, por tanto, gestionar el posible incumplimiento o la posible insuficiencia de la medida de seguridad dentro del sistema objeto de evaluación o dentro de sistemas similares que utilicen la misma medida.

1.2.5. When agreement cannot be found between two or more actors it is the responsibility of the proposer to find an adequate solution.

[G 1] No se considera necesario ofrecer una explicación más detallada.

1.2.6. When a requirement in a notified national rule cannot be fulfilled by an actor, the proposer shall seek advice from the relevant competent authority.

[G 1] No se considera necesario ofrecer una explicación más detallada.

1.2.7. Independently from the definition of the system under assessment, the proposer is responsible for ensuring that the risk management covers the system itself and the integration into the railway system as a whole.

[G 1] No se considera necesario ofrecer una explicación más detallada.

---

(11) En principio, estas disposiciones y procedimientos quedan cubiertos por el proceso de gestión de la calidad y/o gestión de la seguridad de estas partes, que se establecen como mínimo a nivel del proyecto (véase, asimismo, Figura 2).

(12) El término "otros agentes" designa a todas los agentes afectados distintos de los administradores de la infraestructura y las empresas ferroviarias.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

2. DESCRIPCIÓN DEL PROCESO DE EVALUACIÓN DEL RIESGO

2.1. Descripción general – Correspondencia entre el proceso de evaluación del riesgo del MCS y el ciclo en V de CENELEC

2.1.1. The risk assessment process is the overall iterative process that comprises:

(a) the system definition;
(b) the risk analysis including the hazard identification;
(c) the risk evaluation.

The risk assessment process shall interact with the hazard management according to section 4.1.

[G 1] El proceso de gestión del riesgo cubierto por el MCS puede representarse dentro de un ciclo en V que comienza con la definición (preliminar) del sistema y que finaliza con la aceptación del sistema: véase la Figura 4. Este ciclo en V simplificado puede reflejarse, entonces, en el ciclo en V clásico de la Figura 10 de la norma EN 50 126-1 {Ref. 8}. Para mostrar la correspondencia del proceso de gestión del riesgo del MCS de la Figura 1, en la Figura 5 se recuerda el ciclo en V de CENELEC de la Figura 10:

(a) la "definición preliminar del sistema" del MCS de la Figura 1 corresponde a la Fase 1 del ciclo en V de CENELEC, es decir, a la definición del "concepto" de sistema (véase el RECUADRO 1 de la Figura 5);
(b) la "evaluación del riesgo" del MCS de la Figura 1 incluye las siguientes fases del ciclo en V de CENELEC (véase el RECUADRO 2 de la Figura 5):

- Fase 2 de la Figura 5: "definición del sistema y condiciones de aplicación";
- Fase 3 de la Figura 5: "análisis de riesgos";
- Fase 3 de la Figura 5: "requisitos del sistema";
- Fase 5 de la Figura 5: "distribución de requisitos del sistema" hasta los diferentes subsistemas y componentes.

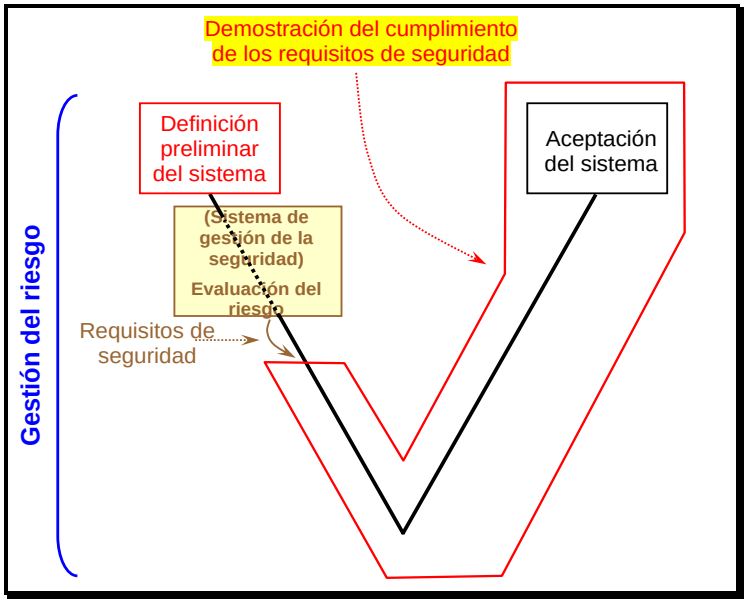


Figura 4: Ciclo en V simplificado de la Figura 10 de la norma EN 50 126.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

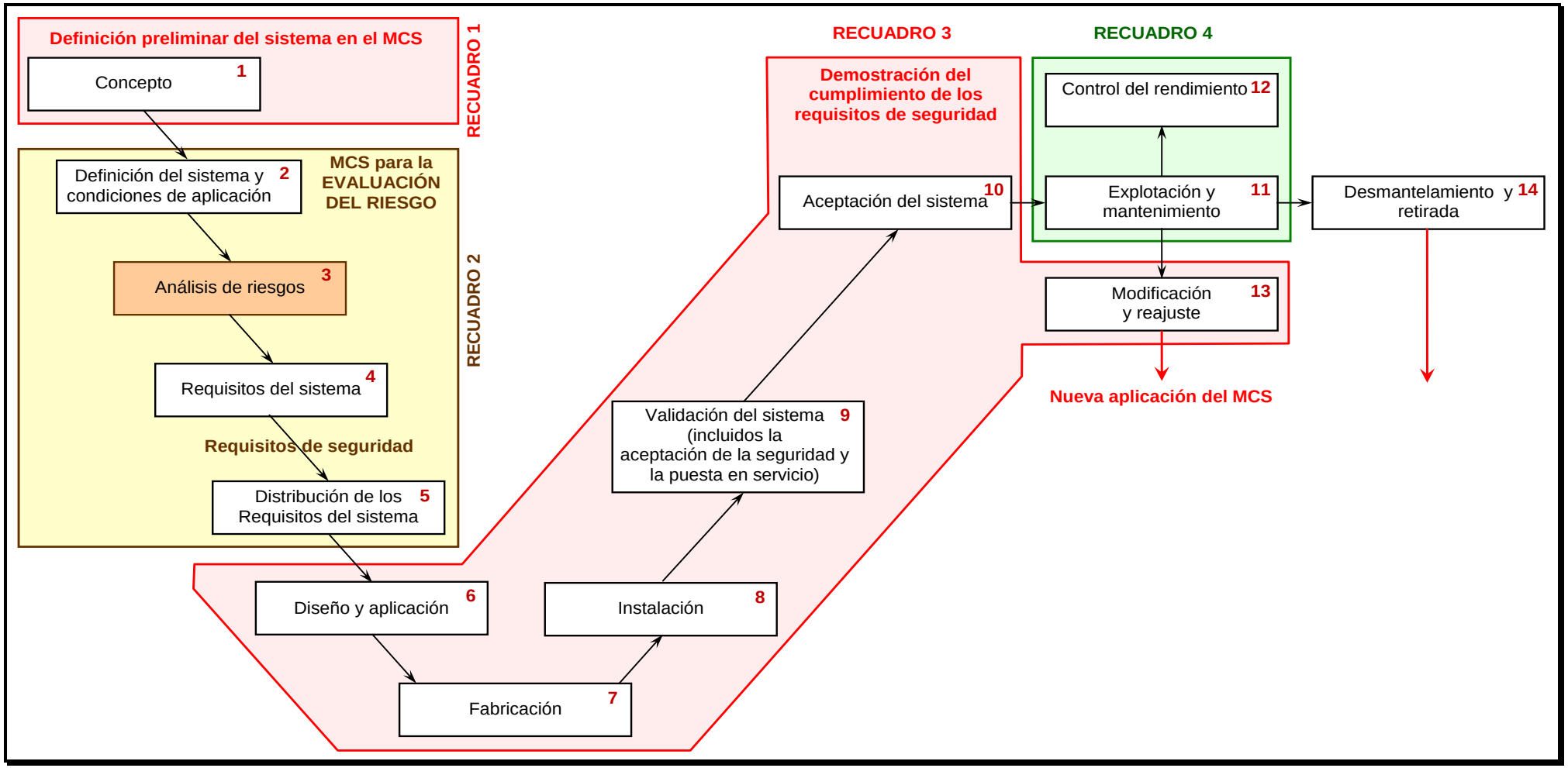


Figura 5: Figura 10 del ciclo en V de la norma EN 50 126 (ciclo vital del sistema de CENELEC).

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

[G 2] Los resultados del proceso de evaluación del riesgo del MCS son (después de iteraciones – véase la Figura 1):

(a) la "definición del sistema" actualizada con los "requisitos de seguridad" resultantes de las actividades de "análisis de riesgos" y "valoración del riesgo" (véase la sección 2.1.6);
(b) la "distribución de los requisitos del sistema" hasta los diferentes subsistemas y componentes (Fase 5 de la Figura 5);
(c) el "registro de peligros", en el que se registran:

(1) todos los peligros identificados y las medidas de seguridad asociadas;
(2) los requisitos de seguridad resultantes;
(3) los supuestos que se han tenido en cuenta para el sistema que determinan los límites y la validez de la evaluación del riesgo (véase la letra (g) de la sección 2.1.2);

(d) y, en general, todas las evidencias resultantes de la aplicación del MCS: véase la sección 5;

Estos resultados de la evaluación del riesgo del MCS corresponden a los resultados relacionados con la seguridad de la Fase 4 del ciclo en V de CENELEC, es decir, a la especificación de requisito del sistema de la Figura 5.

[G 3] La definición del sistema actualizada con los resultados de la evaluación del riesgo y el registro de peligros constituye la información básica con la que se diseña y acepta el sistema. La "demostración de que el sistema cumple los requisitos de seguridad" del MCS corresponde a las siguientes fases del ciclo en V de CENELEC (véase el RECUADRO 3 de la Figura 5):

(a) Fase 6 de la Figura 5: "diseño y aplicación";
(b) Fase 7 de la Figura 5: "fabricación";
(c) Fase 8 de la Figura 5: "instalación";
(d) Fase 9 de la Figura 5: "validación del sistema (incluidos la aceptación de la seguridad y puesta en servicio");
(e) Fase 10 de la Figura 5: "aceptación del sistema".

[G 4] La demostración del cumplimiento de los requisitos de seguridad por parte del sistema depende de si el cambio significativo es de carácter técnico, operativo u organizativo. Así pues, los diferentes pasos del ciclo en V de CENELEC de la Figura 5 puede que no sean adecuados para todos los cambios significativos de esa clase. El ciclo en V de la Figura 5 debe considerarse y utilizarse teniendo debidamente en cuenta lo que se ajusta a cada aplicación concreta (por ejemplo, para los cambios operativos y organizativos, no hay fase de fabricación).

[G 5] Esto significa que la "demostración de que el sistema cumple los requisitos de seguridad" del MCS no incluye únicamente las actividades de "verificación y validación" mediante evidencias o simulaciones. En la práctica, abarca las fases "6 a 10" (véase la lista enumerada anteriormente y la Figura 5) del ciclo en V de CENELEC. Éstas incluyen las actividades de diseño, fabricación, instalación, verificación y validación, así como las actividades RAMS asociadas y la aceptación del sistema.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

[G 6] Durante la “demostración de que el sistema cumple los requisitos de seguridad”, el principio general consiste en realizar una evaluación del riesgo que se centre únicamente en las funciones e interfaces del sistema relacionadas con la seguridad. Esto quiere decir que, en caso de que deban realizarse actividades de evaluación del riesgo y la seguridad con arreglo a una de las fases del ciclo en V de CENELEC de la Figura 5, dicha evaluación debe centrarse en:

(a) las funciones e interfaces relacionadas con la seguridad;
(b) los subsistemas y/o componentes implicados en la consecución de las funciones y/o interfaces relacionadas con la seguridad evaluadas durante las actividades de evaluación del riesgo de nivel superior.

[G 7] De la comparación con el clásico ciclo en V de CENELEC de la Figura 5 se desprende que:

(a) el MCS abarca las fases “1 a 10” y “13” de este ciclo en V. Éstas incluyen el conjunto de actividades necesarias para la aceptación del sistema objeto de evaluación;

(b) el MCS no abarca las fases “11”, “12” ni “14” del ciclo vital del sistema:

(1) las fases “11” y “12” están relacionadas con “la explotación y el mantenimiento” y “el control del rendimiento” del sistema, respectivamente, tras su aceptación sobre la base del MCS. Estas dos fases están cubiertas por el sistema de gestión de la seguridad de la empresa ferroviaria y el administrador de la infraestructura – (Véase el RECUADRO 4 de la Figura 5). No obstante, si durante la explotación, el mantenimiento o el control del rendimiento del sistema resulta necesario modificar y adaptar el sistema (Fase 13 de la Figura 5), mientras que ya está en funcionamiento, el MCS vuelve a aplicarse a los nuevos cambios requeridos de conformidad con el Artículo 2. Por lo tanto, si el cambio es significativo:

(i) los procesos de gestión del riesgo y evaluación del riesgo del MCS se aplican a estos nuevos cambios;
(ii) se requiere una aceptación de estos cambios con arreglo al Artículo 6;

(2) “el desmantelamiento y la retirada” de un sistema en funcionamiento (Fase 14) también podría considerarse como un cambio significativo, y, por lo tanto, podría aplicarse una vez más el MCS con arreglo al Artículo 2 para la fase 14 de la Figura 5

Para obtener más información acerca del ámbito de aplicación de cada fase o actividad del ciclo en V de CENELEC que se recuerda en la Figura 5, véase la sección 6 de la norma EN 50 126-1 {Ref. 8}.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

2.1.2. The system definition should address at least the following issues:

(a) system objective, e.g. intended purpose;
(b) system functions and elements, where relevant (including e.g. human, technical and operational elements);
(c) system boundary including other interacting systems;
(d) physical (i.e. interacting systems) and functional (i.e. functional input and output) interfaces;
(e) system environment (e.g. energy and thermal flow, shocks, vibrations, electromagnetic interference, operational use);
(f) existing safety measures and, after iterations, definition of the safety requirements identified by the risk assessment process;
(g) assumptions which shall determine the limits for the risk assessment.

[G 1] No se considera necesario ofrecer una explicación más detallada.

2.1.3. A hazard identification shall be carried out on the defined system, according to section 2.2.

[G 1] No se considera necesario ofrecer una explicación más detallada.

2.1.4. The risk acceptability of the system under assessment shall be evaluated by using one or more of the following risk acceptance principles:

(h) the application of codes of practice (section 2.3);
(i) a comparison with similar systems (section 2.4);
(j) an explicit risk estimation (section 2.5).

In accordance with the general principle referred to in section 1.1.5, the assessment body shall refrain from imposing the risk acceptance principle to be used by the proposer.

[G 1] En general, el proponente decidirá qué principio de aceptación del riesgo resulta más adecuado para controlar los peligros identificados basándose en los requisitos específicos del proyecto, así como en su experiencia con los tres principios.

[G 2] No siempre es posible evaluar la aceptabilidad del riesgo a nivel del sistema utilizando sólo uno de los tres principios de aceptación del riesgo. La aceptación del riesgo a menudo se basará en una combinación de estos principios. Si a un cambio significativo deben aplicarse varios principios de aceptación del riesgo para controlar el riesgo asociado, es necesario dividir el peligro en cuestión en subpeligros, de manera que los distintos subpeligros sean adecuadamente controlados mediante un solo principio de aceptación del riesgo.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

[G 3] La decisión de controlar un peligro mediante un principio de aceptación del riesgo debe tener en cuenta el peligro y las causas del peligro previamente identificado durante la fase de determinación del peligro. Así pues, si dos causas diferentes e independientes están asociadas al mismo peligro, es necesario subdividir el peligro en dos subpeligros diferentes. A continuación, cada subpeligro será controlado mediante un único principio de aceptación del riesgo. Los dos subpeligros deben registrarse y gestionarse en el registro de peligros. Por ejemplo, si el peligro se debe a un error de diseño, puede gestionarse aplicando un código práctico, mientras que si el peligro se debe a un error de mantenimiento, puede que un código práctico no sea suficiente; en ese caso, es necesario aplicar otro principio de aceptación del riesgo.

[G 4] La reducción del riesgo a un nivel aceptable puede requerir varias iteraciones entre las fases de análisis y valoración de riesgos, hasta que se identifiquen medidas de seguridad adecuadas.

[G 5] Se reconoce que el riesgo residual presente que ha resurgido de la experiencia sobre el terreno es aceptable para los sistemas existentes y para los sistemas basados en la aplicación de códigos prácticos. El riesgo resultante de la estimación explícita del riesgo se basa en la opinión de expertos y en diferentes supuestos contemplados por el experto durante los análisis, o en bases de datos relacionadas con experiencias de accidentes o de explotación. Por lo tanto, el riesgo residual de la estimación explícita del riesgo no puede confirmarse inmediatamente a partir de la experiencia sobre el terreno. Tal demostración exige tiempo para dirigir, controlar y obtener una experiencia representativa para el sistema o los sistemas de que se trate. En general, la aplicación de códigos prácticos y la comparación con sistemas de referencia similares presentan la ventaja de evitar la excesiva especificación de requisitos de seguridad innecesariamente estrictos que pueden derivarse de supuestos (de seguridad) excesivamente moderados contemplados en estimaciones explícitas del riesgo. No obstante, podría ocurrir que algunos requisitos de seguridad de códigos prácticos o sistemas de referencia similares no se realicen para el sistema objeto de evaluación. En ese caso, la aplicación de la estimación explícita del riesgo presentaría la ventaja de evitar un diseño excesivo innecesario del sistema objeto de evaluación y permitiría ofrecer un diseño más rentable que no se ha probado anteriormente.

[G 6] Si los peligros identificados y el riesgo o los riesgos asociado(s) del sistema objeto de evaluación no pueden controlarse aplicando códigos prácticos o sistemas de referencia similares, se realizará una estimación explícita del riesgo basada en análisis cuantitativos y cualitativos de sucesos peligrosos. Esta situación surge cuando el sistema objeto de evaluación es nuevo en su totalidad (o su diseño es innovador) o cuando el sistema se desvía de un código práctico o un sistema de referencia. A continuación, en la estimación explícita del riesgo se evaluará si el riesgo es aceptable (es decir, no es necesario efectuar más análisis) o si es preciso adoptar medidas de seguridad adicionales para reducir el riesgo en mayor medida.

[G 7] Asimismo, en la sección 8. de la Directriz EN 50 126-2 {Ref. 9} pueden encontrarse orientaciones para la reducción del riesgo y la aceptación del riesgo.

[G 8] El organismo de evaluación debe evaluar el principio de aceptación del riesgo utilizado y su aplicación.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

2.1.5. The proposer shall demonstrate in the risk evaluation that the selected risk acceptance principle is adequately applied. The proposer shall also check that the selected risk acceptance principles are used consistently.

[G 1] Por ejemplo, si para el programa informático de un componente se especifica como requisito de seguridad la aplicación del proceso de desarrollo del nivel de integridad de la seguridad SIL 4 de la norma EN 50 128, la demostración deberá probar que se cumple el proceso recomendado por la norma. Esto incluye, por ejemplo, demostrar que:

(a) se cumplen los requisitos relativos a la independencia en la organización del diseño, verificación y validación del programa informático;
(b) se aplican los métodos correctos de la norma EN 50 128 para el nivel de integridad de la seguridad SIL 4;
(c) etc.

[G 2] Por ejemplo, si se va a utilizar un código práctico específico para fabricar electroválvulas de freno de emergencia, la demostración deberá probar que se cumplen todos los requisitos del código práctico durante el proceso de fabricación.

2.1.6. The application of these risk acceptance principles shall identify possible safety measures which make the risk(s) of the system under assessment acceptable. Among these safety measures, the ones selected to control the risk(s) shall become the safety requirements to be fulfilled by the system. Compliance with these safety requirements shall be demonstrated in accordance with section 3.

[G 1] Pueden identificarse dos tipos de medidas de seguridad:

(a) “medidas de seguridad preventivas”, que previenen la aparición de peligros o sus causas, y;
(b) “medidas de seguridad de mitigación”, que evitan que los peligros se conviertan en accidentes o reducen las consecuencias de accidentes una vez que se han producido (medidas de protección).

En términos generales, en beneficio de la operabilidad, la prevención de causas es más eficaz.

[G 2] El proponente considerará como idóneas las medidas de seguridad que ofrezcan el mejor equilibrio entre el coste para reducir el riesgo y el nivel del riesgo residual. Las medidas de seguridad elegidas se convierten en los requisitos de seguridad para el sistema objeto de evaluación.

[G 3] Es importante comprobar que las medidas de seguridad seleccionadas para controlar un peligro no son incompatibles con otros peligros. Como se ilustra en la Figura 6, pueden darse los dos casos siguientes, por ejemplo[13]:

(a) CASO 1: si la misma medida de seguridad (medida A en la Figura 6) puede controlar diferentes peligros sin crear conflictos entre ellos, y si está justificadas desde el punto de vista económico, podría seleccionarse como “requisito de seguridad” asociado sólo

(13) *Cabe señalar que en la guía no se enumeran todas las situaciones en las que las medidas de seguridad podrían ser incompatibles con otros peligros identificados. Sólo se ofrecen algunos ejemplos ilustrativos.*

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

la medida de seguridad en cuestión. El número total de requisitos de seguridad que han de cumplirse es inferior al que supone la aplicación de las medidas B y C;

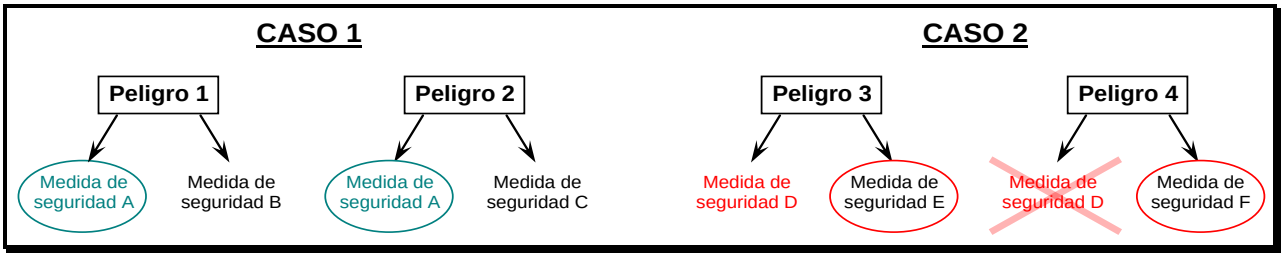


Figura 6: Selección de medidas de seguridad adecuadas para controlar riesgos.

(b) CASO 2: recíprocamente, si una medida de seguridad puede controlar un riesgo pero crea un conflicto con otro peligro (medida D en la Figura 6), no puede seleccionarse como "requisito de seguridad". Deben utilizarse las otras medidas de seguridad para el peligro considerado (medidas E y F en la Figura 6):

(1) Un ejemplo típico del Sistema de Control y Mando es el uso de la localización del tren en la vía, ya sea para controlar la aplicación del freno o para autorizar la aceleración del tren. El uso del tren delantero como localización del tren (y, del tren posterior, respectivamente) no es seguro en todas las situaciones:

(i) cuando el sistema de control y mando ETCS tiene que aplicar de modo seguro los frenos de emergencia, utiliza el EXTREMO FRONTAL MÁXIMO SEGURO para garantizar que el tren delantero se detenga realmente antes de alcanzar el Punto de Peligro;

(ii) recíprocamente, cuando el tren tiene autorización para acelerar, por ejemplo, después de una limitación de velocidad, el sistema de control y mando ETCS utiliza el EXTREMO TRASERO MÍNIMO SEGURO;

(2) Otro ejemplo lo constituye una medida de seguridad que podría aplicarse para detener un tren en casi todas las circunstancias para que se encuentre en estado de seguridad de funcionamiento, salvo en el caso de un túnel o un puente. En este último caso, no se adoptará la medida D del CASO 2 de la Figura 6.

2.1.7. The iterative risk assessment process can be considered as completed when it is demonstrated that all safety requirements are fulfilled and no additional reasonably foreseeable hazards have to be considered.

[G 1] Dependiendo, por ejemplo, de las opciones técnicas que se elijan para el diseño de un sistema, sus subsistemas y equipos, podrían identificarse nuevos peligros durante la "demostración del cumplimiento de los requisitos de seguridad" (por ejemplo, el uso de determinadas pinturas podría generar gases tóxicos en caso de incendio). Estos nuevos peligros y los riesgos asociados deben considerarse como nueva información básica para un nuevo bucle en el proceso iterativo de evaluación del riesgo. En el Apéndice A.4.3. de la norma EN 50 129 se ofrecen otros ejemplos en los que podrían introducirse nuevos peligros que deben ser objeto de control.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

2.2. Determinación de los peligros

2.2.1. The proposer shall systematically identify, using wide-ranging expertise from a competent team, all reasonably foreseeable hazards for the whole system under assessment, its functions where appropriate and its interfaces.

All identified hazards shall be registered in the hazard record according to section 4.

[G 1] Los peligros se describen, en la medida de lo posible, con el mismo grado de detalle. Puede ocurrir que durante los análisis preliminares del peligro se identifiquen peligros con diferentes grados de detalle (por ejemplo, porque durante el análisis HAZOP se reúnen personas con experiencia diversa).
El grado de detalle depende, asimismo, del principio de aceptación del riesgo que se seleccione para controlar el peligro o los peligros identificados. Por ejemplo, si un código práctico o un sistema de referencia similar controlan un peligro en su totalidad, no será necesario identificar el peligro en mayor detalle.

[G 2] Todos los peligros identificados durante el proceso de evaluación del riesgo (incluidos los asociados con riesgos ampliamente aceptables), las medidas de seguridad asociadas y los riesgos asociados deben registrarse en el registro de peligros.

[G 3] En función de la naturaleza del sistema que se vaya a analizar, pueden usarse diferentes métodos para la determinación del peligro.

(c) puede usarse la determinación empírica del peligro aprovechando la experiencia pasada (por ejemplo, el uso de listas de comprobación o listas de peligros genéricos);
(d) puede usarse la determinación creativa del peligro para nuevos ámbitos de preocupación (pronóstico anticipatorio, por ejemplo, estudios estructurados de “WHAT-IF” como FMEA o HAZOP).

[G 4] Los métodos empíricos y creativos para la determinación del peligro pueden combinarse para complementarse mutuamente, lo que garantiza la exhaustividad de la lista de peligros potenciales y medidas de seguridad, cuando proceda.

[G 5] Como paso preliminar, la determinación del peligro podría comenzar con la creación de un equipo creativo integrado por expertos con diferentes competencias que cubran todos los aspectos relevantes del cambio significativo. Cuando el grupo de expertos lo estime necesario, pueden usarse métodos empíricos para analizar una función o un modo operativo específico.

[G 6] Los métodos utilizados para la determinación del peligro dependen de la definición del sistema. En el Apéndice B se ofrecen algunos ejemplos.

[G 7] En los Anexos A.2 y E de la Directriz EN 50 126-2 {Ref. 9} puede encontrarse más información sobre las técnicas y los métodos de determinación del peligro.

[G 8] En la sección C.17. Ejemplo de una lista de peligros genéricos para la explotación ferroviaria del Apéndice C se ofrece un ejemplo de una lista de peligros genéricos.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

2.2.2. To focus the risk assessment efforts upon the most important risks, the hazards shall be classified according to the estimated risk arising from them. Based on expert judgement, hazards associated with a broadly acceptable risk need not be analysed further but shall be registered in the hazard record. Their classification shall be justified in order to allow independent assessment by an assessment body.

[G 1] Para facilitar el proceso de evaluación del riesgo, los peligros significativos pueden volver a agruparse en diferentes categorías. Por ejemplo, los peligros significativos pueden clasificarse en función de la gravedad del riesgo prevista y de su frecuencia de aparición. Las normas CENELEC brindan orientaciones para un ejercicio de estas características: véase la sección A.2. Clasificación del peligro del Apéndice APÉNDICE A: .

[G 2] El análisis y la valoración del riesgo que se describen en la sección 2.1.4 se aplican con carácter prioritario a los peligros clasificados en la categoría más alta.

2.2.3. As a criterion, risks resulting from hazards may be classified as broadly acceptable when the risk is so small that it is not reasonable to implement any additional safety measure. The expert judgement shall take into account that the contribution of all the broadly acceptable risks does not exceed a defined proportion of the overall risk.

[G 1] Por ejemplo, un riesgo asociado a un peligro puede considerarse ampliamente aceptable:

(a) si el riesgo es inferior a un porcentaje establecido (por ejemplo, x%) del Máximo Riesgo Tolerable para este tipo de peligro. El valor de x% podría basarse en las mejores prácticas y la experiencia con diversos enfoques de análisis de riesgos, por ejemplo, la proporción entre las clasificaciones de riesgo ampliamente aceptable y riesgo intolerable en curvas FN o en matrices de riesgo. Ello puede representarse como se muestra en la Figura 7;

(b) o si la pérdida asociada al riesgo es tan pequeña que no resulta razonable aplicar contramedida de seguridad alguna.

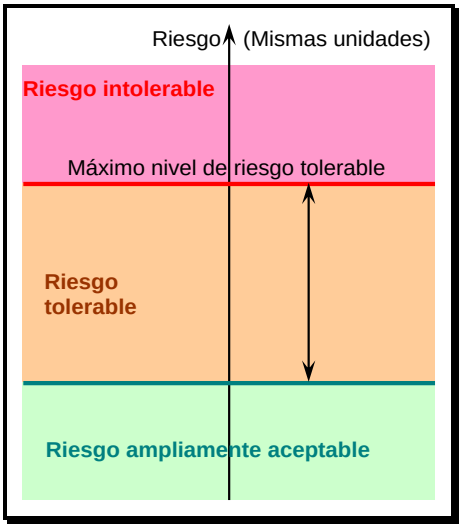


Figura 7: Riesgos ampliamente aceptables

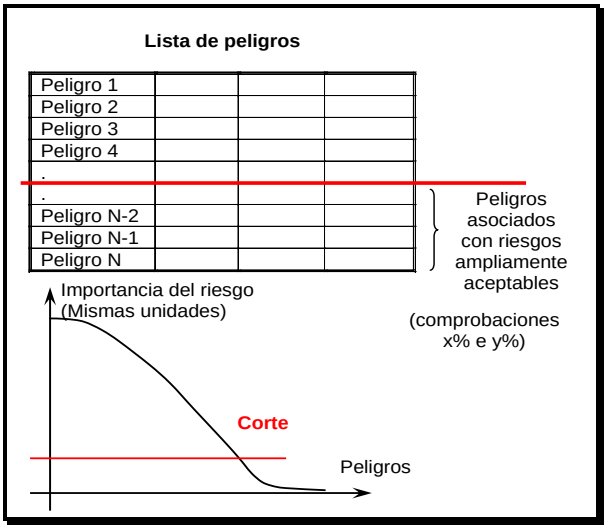


Figura 8: Eliminación de peligros asociados a un riesgo ampliamente aceptable.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

[G 2] Por otra parte, si se identifican peligros con diferentes grados de detalle (es decir, peligros de alto nivel, por un lado, y subpeligros detallados, por otro), deben tomarse precauciones a fin de evitar que se clasifiquen erróneamente como peligros asociados con un riesgo o riesgos ampliamente aceptables. La contribución de todos los peligros asociados con riesgos ampliamente aceptables no puede superar un porcentaje establecido (por ejemplo, y%) del riesgo general en el nivel del sistema. Es necesario realizar esta comprobación para evitar que la lógica expuesta quede vacía de fundamento al subdividir los peligros en muchos subpeligros de bajo nivel. De hecho, si un peligro se expresa como varios subpeligros diferentes "más pequeños", cada uno de éstos puede clasificarse fácilmente como asociado a un riesgo ampliamente aceptable si se evalúan independientemente pero asociarse con un riesgo significativo cuando se evalúen conjuntamente (es decir, como un peligro de alto nivel). El valor del porcentaje (por ejemplo, y%) depende de los criterios de aceptación del riesgo aplicables en el nivel del sistema. Puede basarse en la experiencia de la explotación de sistemas de referencia similares y estimarse a partir de la misma.

[G 3] Las dos comprobaciones anteriormente referidas (es decir, x % e y %) permiten centrar la evaluación del riesgo en los peligros más importantes, así como asegurar el control de cualquier riesgo significativo (véase la Figura 8).
Sin perjuicio de los requisitos legales de un Estado miembro, el proponente es responsable de definir, basándose en la opinión de expertos, los valores de x % e y % y someterlos a la evaluación independiente por parte de un organismo de evaluación. Un ejemplo de órdenes de magnitud puede ser x = 1% e y = 10%, si la opinión de expertos lo considera aceptable.

[G 4] La sección 2.2.2 exige que la clasificación en la categoría de "riesgo(s) ampliamente aceptable(s)" se someta a la evaluación independiente a través de un organismo de evaluación.

2.2.4. During the hazard identification, safety measures may be identified. They shall be registered in the hazard record according to section 4.

[G 1] El objetivo principal de esta actividad es identificar los peligros relacionados con el cambio. Si ya se han identificado medidas de seguridad, deben registrarse en el registro de peligros. La naturaleza de las medidas depende del cambio; pueden ser medidas de procedimiento, técnicas, operativas u organizativas.

2.2.5. The hazard identification only needs to be carried out at a level of detail necessary to identify where safety measures are expected to control the risks in accordance with one of the risk acceptance principles mentioned in point 2.1.4. Iteration may thus be necessary between the risk analysis and the risk evaluation phases until a sufficient level of detail is reached for the identification of hazards.

[G 1] Aun cuando se controle un riesgo a un nivel aceptable, el proponente podrá decidir si es necesario identificar el peligro en mayor detalle. Una de las razones de tal decisión podría ser la probabilidad de encontrar medidas de seguridad de control de riesgo más rentables si se realiza una determinación del peligro más detallada.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

2.2.6. Whenever a code of practices or a reference system is used to control the risk, the hazard identification can be limited to:

(c) The verification of the relevance of the code of practices or of the reference system.
(d) The identification of the deviations from the code of practices or from the reference system.

[G 1] No se considera necesario ofrecer una explicación más detallada.

2.3. Uso de códigos prácticos y valoración del riesgo

2.3.1. The proposer, with the support of other involved actors and based on the requirements listed in point 2.3.2, shall analyse whether one or several hazards are appropriately covered by the application of relevant codes of practice.

[G 1] No se considera necesario ofrecer una explicación más detallada.

2.3.2. The codes of practice shall satisfy at least the following requirements:

(e) be widely acknowledged in the railway domain. If this is not the case, the codes of practice will have to be justified and be acceptable to the assessment body;
(f) be relevant for the control of the considered hazards in the system under assessment;
(g) be publicly available for all actors who want to use them.

[G 1] No se considera necesario ofrecer una explicación más detallada.

2.3.3. Where compliance with TSIs is required by Directive 2008/57/EC and the relevant TSI does not impose the risk management process established by this Regulation, the TSIs may be considered as codes of practice for controlling hazards, provided requirement (c) of point 2.3.2 is fulfilled.

[G 1] No se considera necesario ofrecer una explicación más detallada.

2.3.4. National rules notified in accordance with Article 8 of Directive 2004/49/EC and Article 17(3) of Directive 2008/57/EC may be considered as codes of practice provided the requirements of point 2.3.2 are fulfilled.

[G 1] No se considera necesario ofrecer una explicación más detallada.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

2.3.5. If one or more hazards are controlled by codes of practice fulfilling the requirements of point 2.3.2, then the risks associated with these hazards shall be considered as acceptable. This means that:

(h) these risks need not be analysed further;
(i) the use of the codes of practice shall be registered in the hazard record as safety requirements for the relevant hazards.

[G 1] No se considera necesario ofrecer una explicación más detallada.

2.3.6. Where an alternative approach is not fully compliant with a code of practice, the proposer shall demonstrate that the alternative approach taken leads to at least the same level of safety.

[G 1] No se considera necesario ofrecer una explicación más detallada.

2.3.7. If the risk for a particular hazard cannot be made acceptable by the application of codes of practice, additional safety measures shall be identified applying one of the two other risk acceptance principles.

[G 1] No se considera necesario ofrecer una explicación más detallada.

2.3.8. When all hazards are controlled by codes of practice, the risk management process may be limited to:

(j) The hazard identification in accordance with section 2.2.6;
(k) The registration of the use of the codes of practice in the hazard record in accordance with section 2.3.5;
(l) The documentation of the application of the risk management process in accordance with section 5;
(m) An independent assessment in accordance with Article 6.

[G 1] No se considera necesario ofrecer una explicación más detallada.

2.4. Uso de un sistema de referencia y valoración del riesgo

2.4.1. The proposer, with the support of other involved actors, shall analyse whether one or more hazards are covered by a similar system that could be taken as a reference system.

[G 1] En la sección 8 de la guía EN 50 126-2 {Ref. 9} puede encontrarse más información sobre estos principios.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

2.4.2. A reference system shall satisfy at least the following requirements:

(n) it has already been proven in-use to have an acceptable safety level and would still qualify for acceptance in the Member State where the change is to be introduced;
(o) it has similar functions and interfaces as the system under assessment;
(p) it is used under similar operational conditions as the system under assessment;
(q) it is used under similar environmental conditions as the system under assessment.

[G 1] Por ejemplo, un antiguo sistema de control y mando del que se demuestre durante su uso que presenta un nivel de seguridad aceptable podría sustituirse por otro sistema con tecnología más reciente y mejores resultados en materia de seguridad. Así pues, resulta pertinente comprobar cada vez que se aplique un sistema de referencia si éste sigue reuniendo los requisitos necesarios para su aceptación.

[G 2] Por ejemplo, dado que algunos aspectos de la seguridad de los túneles o la seguridad del transporte de mercancías peligrosas podrían ser específicos y podrían depender de condiciones de funcionamiento y ambientales, es necesario comprobar para cada proyecto que el sistema se utilizará en las mismas condiciones.

2.4.3. If a reference system fulfils the requirements listed in point 2.4.2, then for the system under assessment:

(r) the risks associated with the hazards covered by the reference system shall be considered as acceptable;
(s) the safety requirements for the hazards covered by the reference system may be derived from the safety analyses or from an evaluation of safety records of the reference system;
(t) these safety requirements shall be registered in the hazard record as safety requirements for the relevant hazards.

[G 1] No se considera necesario ofrecer una explicación más detallada.

2.4.4. If the system under assessment deviates from the reference system, the risk evaluation shall demonstrate that the system under assessment reaches at least the same safety level as the reference system. The risks associated with the hazards covered by the reference system shall, in that case, be considered as acceptable.

[G 1] En la sección 8.1.3. de la Directriz EN 50 126-2 {Ref. 9} puede encontrarse más información sobre análisis de similitud.

2.4.5. If the same safety level as the reference system cannot be demonstrated, additional safety measures shall be identified for the deviations, applying one of the two other risk acceptance principles.

[G 1] No se considera necesario ofrecer una explicación más detallada.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

2.5. Estimación explícita y valoración del riesgo

2.5.1. When the hazards are not covered by one of the two risk acceptance principles described in sections 2.3 and 2.4, the demonstration of the risk acceptability shall be performed by explicit risk estimation and evaluation. Risks resulting from these hazards shall be estimated either quantitatively or qualitatively, taking existing safety measures into account.

[G 1] No se considera necesario ofrecer una explicación más detallada.

2.5.2. The acceptability of the estimated risks shall be evaluated using risk acceptance criteria either derived from or based on legal requirements stated in Community legislation or in notified national rules. Depending on the risk acceptance criteria, the acceptability of the risk may be evaluated either individually for each associated hazard or globally for the combination of all hazards considered in the explicit risk estimation.

If the estimated risk is not acceptable, additional safety measures shall be identified and implemented in order to reduce the risk to an acceptable level.

[G 1] Para evaluar si los riesgos derivados del sistema objeto de evaluación son aceptables o no, es necesario aplicar criterios de aceptación del riesgo (véanse los recuadros "valoración del riesgo" de la Figura 1). Los criterios de aceptación del riesgo pueden ser implícitos o explícitos:

(a) criterios de aceptación del riesgo implícitos: con arreglo a las secciones 2.3.5 y 2.4.3, los riesgos cubiertos por la aplicación de códigos prácticos y por la comparación con sistemas de referencia se consideran implícitamente aceptables siempre que, respectivamente, (véanse los puntos delimitados por círculos de la Figura 1):

(1) se reúnan las condiciones de aplicación de códigos prácticos de la sección 2.3.2;
(2) se reúnan las condiciones de uso de un sistema de referencia de la sección 2.4.2;

(b) criterios de aceptación del riesgo explícitos: para evaluar si los riesgos controlados mediante la aplicación de una estimación explícita del riesgo son aceptables o no, es necesario aplicar criterios de aceptación del riesgo explícitos (véanse las líneas delimitadas por círculos de la Figura 1 para el tercer principio). Éstos pueden definirse en diferentes niveles de un sistema ferroviario. Pueden considerarse como una "pirámide de criterios" (véase la Figura 9) que va desde los criterios de aceptación del riesgo de alto nivel (expresado, por ejemplo, como riesgo para la sociedad en su conjunto o como riesgo individual), hasta los subsistemas y componentes (para cubrir sistemas técnicos), e incluye las acciones humanas durante las actividades de explotación y mantenimiento del sistema y los subsistemas. Aunque los criterios de aceptación del riesgo contribuyen a la seguridad del sistema, y, por tanto, están vinculados a objetivos comunes de seguridad y valores de referencia nacionales, resulta muy difícil establecer un modelo matemático entre ellos: para obtener más detalles al respecto, véase {Ref. 12}.
El nivel en el que se definen los criterios de aceptación del riesgo explícitos debe corresponderse con la importancia y complejidad del cambio significativo. Por ejemplo, no es necesario evaluar el riesgo del sistema ferroviario en general cuando se modifique un tipo de eje en materiales rodantes. La definición de los criterios de aceptación del riesgo puede centrarse en la seguridad del material rodante. Recíprocamente, los cambios o adiciones de gran envergadura realizados en un sistema ferroviario existente no deben evaluarse exclusivamente basándose en la

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

seguridad de funciones o cambios específicos añadidos. Asimismo, conviene verificar en el nivel del sistema ferroviario que el cambio es aceptable en su conjunto.

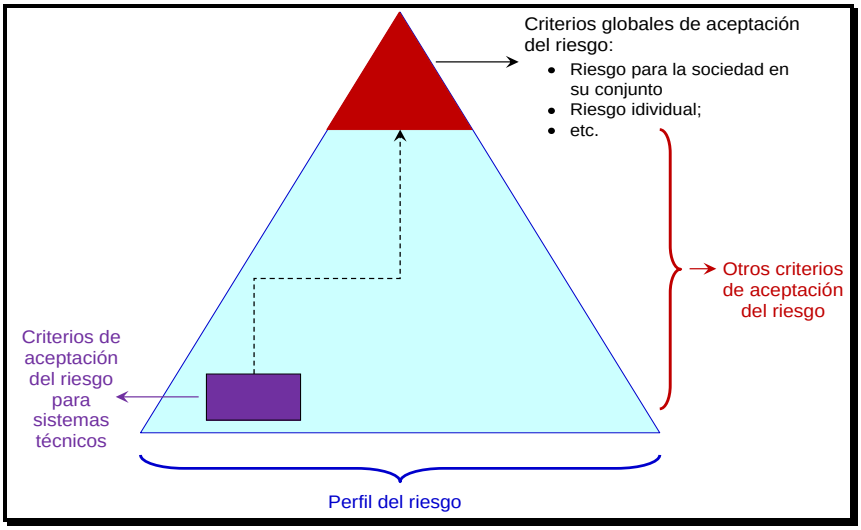


Figura 9: Pirámide de criterios de aceptación del riesgo.

[G 2] La labor en curso de la Agencia sobre los criterios de aceptación del riesgo armonizará los criterios de aceptación del riesgo explícitos necesarios para facilitar el reconocimiento mutuo entre los Estados miembros. Cuando se disponga de información adicional, ésta se incluirá en el presente documento.

[G 3] Mientras tanto, los riesgos pueden evaluarse, por ejemplo, utilizando la matriz de riesgo que figura en la sección 4.6 de la norma EN 50 126-1 {Ref. 8}. Asimismo, pueden utilizarse otros tipos de criterios adecuados, dado que se considera que estos criterios ofrecen un nivel de seguridad aceptable en el caso que nos ocupa.

2.5.3. When the risk associated with one or a combination of several hazards is considered as acceptable, the identified safety measures shall be registered in the hazard record.

[G 1] No se considera necesario ofrecer una explicación más detallada.

2.5.4. Where hazards arise from failures of technical systems not covered by codes of practice or the use of a reference system, the following risk acceptance criterion shall apply for the design of the technical system:

For technical systems where a functional failure has credible direct potential for a catastrophic consequence, the associated risk does not have to be reduced further if the rate of that failure is less than or equal to 10^{-9} per operating hour.

[G 1] En una nota aparte de la Agencia asociada al presente documento se proporcionan más detalles acerca del criterio de aceptación del riesgo para sistemas técnicos, así como en cuanto a los aspectos y funciones del sistema técnico a los que se aplican el criterio: véanse

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

la sección A.3. Criterio de aceptación del riesgo para sistemas técnicos del Apéndice APÉNDICE A: y el documento de referencia {Ref. 11}.

2.5.5. Without prejudice to the procedure specified in Article 8 of Directive 2004/49/EC, a more demanding criterion may be requested, through a national rule, in order to maintain a national safety level. However, in the case of additional authorisations for placing in service of vehicles, the procedures of Articles 23 and 25 of Directive 2008/57/EC shall apply.

[G 1] No se considera necesario ofrecer una explicación más detallada.

2.5.6. If a technical system is developed by applying the 10^{-9} criterion defined in point 2.5.4, the principle of mutual recognition is applicable in accordance with Article 7(4) of this Regulation.

Nevertheless, if the proposer can demonstrate that the national safety level in the Member State of application can be maintained with a rate of failure higher than 10-9 per operating hour, this criterion can be used by the proposer in that Member State.

[G 1] No se considera necesario ofrecer una explicación más detallada.

2.5.7. The explicit risk estimation and evaluation shall satisfy at least the following requirements:

(c) the methods used for explicit risk estimation shall reflect correctly the system under assessment and its parameters (including all operational modes);

(d) the results shall be sufficiently accurate to serve as robust decision support, i.e. minor changes in input assumptions or prerequisites shall not result in significantly different requirements.

[G 1] No se considera necesario ofrecer una explicación más detallada.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

3. DEMOSTRACIÓN DE CUMPLIMIENTO DE LOS REQUISITOS DE SEGURIDAD

3.1. Prior to the safety acceptance of the change, fulfilment of the safety requirements resulting from the risk assessment phase shall be demonstrated under the supervision of the proposer.

[G 1] Como se explica en los apartados [G 3] a [G 6] de la sección 2.1.1, la "demostración de que el sistema cumple los requisitos de seguridad" incluye las fases "6 a 10" del ciclo en V de CENELEC (véase el RECUADRO 3 de la Figura 5). Véase el apartado [G 3] de la sección 2.1.1.

[G 2] Véase, asimismo, el apartado [G 4] de la sección 2.1.1 del presente documento.

3.2. This demonstration shall be carried out by each of the actors responsible for fulfilling the safety requirements, as decided in accordance with point 1.1.5.

[G 1] Un ejemplo de evaluaciones y análisis de seguridad que pueden realizarse en el nivel del subsistema lo constituyen los análisis causales: véase la Figura 10. No obstante, puede utilizarse cualquier otro método para demostrar que el subsistema cumple los requisitos de seguridad de datos.

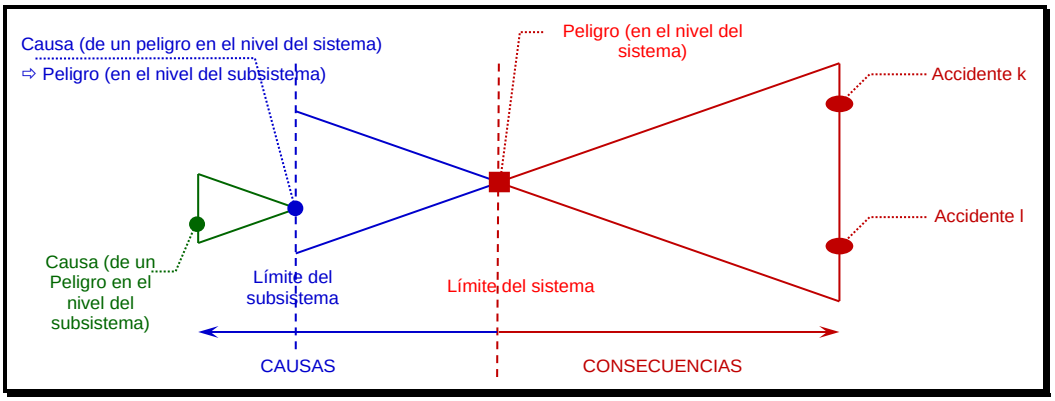


Figura 10: Figura A.4 de EN 50 129: Definición de peligros con respecto al límite del sistema.

[G 2] La estructuración jerárquica de peligros y causas, con respecto a sistemas y subsistemas, puede repetirse para cada fase de nivel inferior del ciclo en V de CENELEC de la Figura 5. Las actividades de determinación del peligro y análisis causal (o cualquier método involucrado), así como el uso de códigos prácticos, sistemas de referencia similares y valoraciones y análisis explícitos, también pueden repetirse para cada fase del ciclo de desarrollo del sistema para establecer, a partir de las medidas de seguridad identificadas en el nivel del subsistema, los requisitos de seguridad que debe cumplir la siguiente fase. Este proceso se ilustra en la Figura 11.

[G 3] Véase, asimismo, el apartado [G 4] de la sección 2.1.1 del presente documento.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

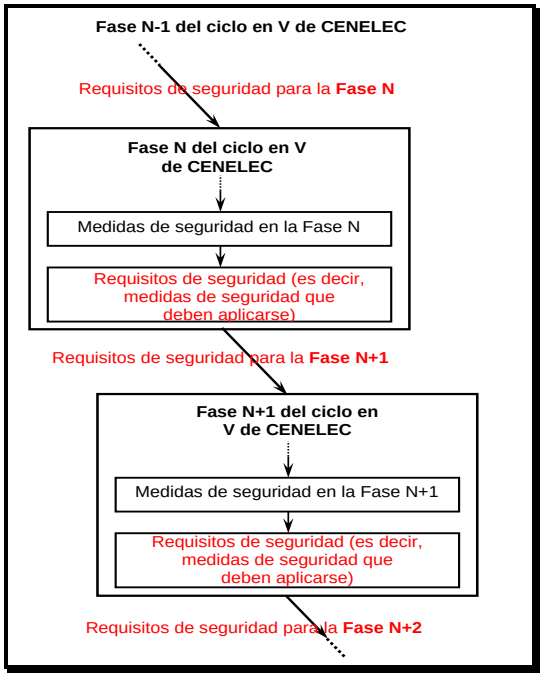


Figura 11: Establecimiento de requisitos de seguridad para fases de nivel inferior.

3.3.	*The approach chosen for demonstrating compliance with the safety requirements as well as the demonstration itself shall be independently assessed by an assessment body.*

[G 1] Por lo tanto, todas las actividades representadas en el RECUADRO 3[(14)] del ciclo en V de CENELEC de la Figura 5 son también objeto de una evaluación independiente.

[G 2] La clase y el grado de detalle correspondiente a la evaluación independiente que llevan a cabo los organismos de evaluación (es decir, evaluación detallada o microscópica) se abordan en las explicaciones contenidas en el Artículo 6.

3.4.	*Any inadequacy of safety measures expected to fulfil the safety requirements or any hazards discovered during the demonstration of compliance with the safety requirements shall lead to reassessment and evaluation of the associated risks by the proposer according to section 2. The new hazards shall be registered in the hazard record according to section 4.*

(14) *En la sección **2.1.1** se describe la correspondencia de actividades entre los MCS y la Figura 5 (es decir, la Figura 10 del ciclo en V de la norma CENELEC 50 126). En particular, en el apartado [G 3] de la sección **2.1.1** se enumeran las actividades de CENELEC incluidas en la fase de "demostración de cumplimiento de los requisitos de seguridad por parte del sistema" de los MCS.*

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

[G 1] Por ejemplo, la manera de extinguir un incendio podría dar lugar a un nuevo peligro (asfixia) que impondrá nuevos requisitos de seguridad (tal como un procedimiento específico de evacuación de pasajeros). Otro ejemplo es la utilización de vidrio templado para evitar que las ventanas se rompan en colisiones y que los pasajeros sufran lesiones por vidrio o incluso salgan despedidos. En ese caso, el nuevo peligro inducido reside en que la evacuación de emergencia de los vagones a través de las ventanas resulta mucho más difícil, lo que podría traducirse en requisitos de seguridad que exijan que algunas ventanas estén especialmente diseñadas para permitir la evacuación.

[G 2] Ejemplo de un cambio operativo: se exige que se prohíba la circulación de todos los transportes de mercancías peligrosas en una vía que atraviese zonas densamente pobladas. En lugar de ello, deben circular por una ruta alternativa con túneles, creando así diferentes tipos de peligros.

[G 3] En el Apéndice A.4.3 de la norma EN 50 129 figuran otros ejemplos de nuevos peligros que podrían identificarse durante la demostración de cumplimiento de los requisitos de seguridad por parte del sistema.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

4. GESTIÓN DE LOS PELIGROS

4.1. Proceso de gestión de los peligros

4.1.1. Hazard record(s) shall be created or updated (where they already exist) by the proposer during the design and the implementation and till the acceptance of the change or the delivery of the safety assessment report. The hazard record shall track the progress in monitoring risks associated with the identified hazards. In accordance with point 2(g) of Annex III to Directive 2004/49/EC, once the system has been accepted and is operated, the hazard record shall be further maintained by the infrastructure manager or the railway undertaking in charge with the operation of the system under assessment as an integrated part of its safety management system.

[G 1] Las normas CENELEC 50 126-1 {Ref. 8} y 50 129 {Ref. 7} también recomiendan el uso de un registro de peligros para registrar, gestionar y controlar la información relacionada con la seguridad.

[G 2] Por ejemplo, dependiendo de la complejidad del sistema, un agente podría disponer de uno o varios registros. En ambos casos, el/los registro(s) de peligros se somete(n) a la evaluación independiente del/de los organismo(s) de evaluación. Por ejemplo, una posible solución podría consistir en disponer de:

(a) un "registro de peligros interno" para gestionar todos los requisitos de seguridad internos aplicables al subsistema que compete al agente. Su tamaño y la cantidad de trabajo de gestión dependen de su estructura y, obviamente, de la complejidad del subsistema. No obstante, puesto que se usa con fines de gestión interna, el registro de peligros no debe comunicarse a otros agentes. El registro de peligros interno contiene todos los peligros identificados que se controlan, así como las medidas de seguridad asociadas que se validan;
(b) un "registro de peligros externo" para transferir a otros agentes peligros y las medidas de seguridad asociadas (que el agente no puede aplicar por sí solo en su totalidad) de conformidad con la sección 1.2.2. Normalmente, este segundo registro de peligros es más pequeño y exige menos trabajo de gestión (véase el ejemplo de la sección C.16.4. Ejemplo de un registro de peligros para transmitir información a otros agentes del Apéndice APÉNDICE C: EJEMPLOS).

[G 3] Si parece complicado gestionar varios registros de peligros, otra solución posible sería gestionar todos los peligros y las medidas asociadas a que se refieren los puntos (a) y (b) que figuran más arriba en un único registro de peligros, pero con la posibilidad de elaborar dos informes de registro de peligros (véase el ejemplo de la sección 0 del Apéndice 0):

(a) un informe del registro de peligros interno, que incluso podría no ser necesario si el registro de peligros está bien estructurado para permitir una evaluación independiente;
(b) un informe del registro de peligros externo para transferir peligros y las medidas de seguridad asociadas a otros agentes.

[G 4] Como se explica en la sección 4.2, al término del proyecto, cuando se acepta el sistema:

(a) todos los peligros que se transfieren a otros agentes se controlan en el registro de peligros externo del agente que los transfiere. Dado que se importan y gestionan en los registros de peligros internos de los otros agentes, no es necesario que el agente de que se trate siga gestionándolos durante el ciclo vital del (sub)sistema;
(b) sin embargo, no deben validarse todas las medidas de seguridad asociadas en el registro de peligros por los motivos que se exponen en el apartado [G 9] de la sección 4.2. De hecho, resulta útil que la organización que exporte las restricciones de

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

uso indique claramente en su registro de peligros que las medidas de seguridad asociadas no se validaron.

[G 5] Recíprocamente, todos los registros de peligros internos se mantienen a lo largo de todo el ciclo vital del (sub)sistema. Ello permite hacer un seguimiento de los avances realizados en el control de riesgos asociados con los peligros identificados durante la explotación y el mantenimiento del (sub)sistema, es decir, incluso después de su desmantelamiento: véase el RECUADRO 4 del ciclo en V de CENELEC de la Figura 5.

4.1.2. The hazard record shall include all hazards, together with all related safety measures and system assumptions identified during the risk assessment process. In particular, it shall contain a clear reference to the origin and to the selected risk acceptance principles and shall clearly identify the actor(s) in charge of controlling each hazard.

[G 1] La información sobre peligros y las medidas de seguridad asociadas que se recibe de otros agentes (véase la sección 1.2.2) incluye asimismo todos los supuestos [(15)] y restricciones de uso[(15)] (también denominadas condiciones de aplicación relacionadas con la seguridad) aplicables a los diferentes subsistemas y casos de seguridad de la aplicación genérica y el producto genérico creados por los fabricantes, cuando proceda.

[G 2] En la sección C.16. Ejemplos de posibles estructuras del registro de peligros del Apéndice APÉNDICE C: EJEMPLOS se describe un posible ejemplo de estructura del registro de peligros.

4.2. Intercambio de información

All hazards and related safety requirements which cannot be controlled by one actor alone shall be communicated to another relevant actor in order to find jointly an adequate solution. The hazards registered in the hazard record of the actor who transfers them shall only be "controlled" when the evaluation of the risks associated with these hazards is made by the other actor and the solution is agreed by all concerned.

[G 1] Por ejemplo, en relación con el subsistema de odometría del equipo ETCS que se encuentra a bordo, el fabricante puede validar los algoritmos en el laboratorio simulando las señales teóricas que podrían generar los sensores odométricos asociados. No obstante, el proceso completo de validación del subsistema de odometría requiere la ayuda de la empresa ferroviaria y el administrador de la infraestructura para llevar a cabo dicho proceso usando un tren real y el contacto rueda-carril del tren real.

[G 2] Otros ejemplos podrían ser las transferencias de medidas de seguridad operativas o de mantenimiento aplicables a equipos técnicos por parte de los fabricantes a las empresas ferroviarias. Estas medidas de seguridad deberán aplicarlas las empresas ferroviarias.

[G 3] A fin de que las organizaciones participantes puedan volver a evaluar conjuntamente estos peligros, las medidas de seguridad y los riesgos asociados, resulta útil que la organización

(15) *Véase el apartado [G 5] de la sección 1.1.5 y las notas a pie de página (9) y (10) en la página 30, del presente documento para obtener una explicación más detallada acerca de los casos de seguridad de "la aplicación genérica y el producto genérico" y de los "supuestos y restricciones de uso".*

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

que los haya identificado ofrezca las explicaciones necesarias para un claro entendimiento del problema. Podría ser necesario modificar la definición inicial de los peligros, las medidas de seguridad y los riesgos para que puedan entenderse sin tener que debatirlos de nuevo conjuntamente. La reevaluación conjunta de los peligros podría llevar a identificar nuevas medidas de seguridad.

[G 4] El agente receptor responsable de la aplicación, verificación y validación de las medidas de seguridad recibidas o nuevas registra en su propio registro de peligros todos los peligros de que se trate junto con las medidas de seguridad asociadas (tanto las importadas como las identificadas conjuntamente).

[G 5] Cuando una medida de seguridad no está plenamente validada, es preciso elaborar una clara restricción de uso (por ejemplo, medidas operativas de mitigación) y registrarla en el registro de peligros. En efecto, es posible que las medidas de seguridad técnicas y/o de diseño:

(a) no se hayan aplicado correctamente, o;
(b) no se hayan aplicado en su totalidad, o;
(c) no se hayan aplicado intencionadamente, por ejemplo, porque se han aplicado otras medidas de seguridad en lugar de las registradas en el registro de peligros (por ejemplo, por razones de costes). Al no haber sido validadas, tales medidas de seguridad deben identificarse claramente en el registro de peligros. Asimismo, es necesario aportar evidencias o una justificación del carácter adecuado de las medidas de seguridad que se han aplicado en lugar de las especificadas en un principio[(16)], así como demostrar que con las medidas de seguridad sustitutivas el sistema cumple los requisitos de seguridad;
(d) etc.

En estos casos, las medidas de seguridad técnicas y/o de diseño de que se trate no pueden verificarse ni validarse durante el proceso de gestión del peligro. Así pues, el/los peligro(s) y las medidas de seguridad en cuestión deben permanecer abiertos en el registro de peligros, a fin de evitar el uso inadecuado de las medidas de seguridad en otros sistemas mediante la aplicación del principio de aceptación del riesgo del “sistema de referencia similar”.

[G 6] Normalmente, las medidas de seguridad que “no se hayan aplicado correctamente” y/o “no se hayan aplicado en su totalidad” se detectan en una fase temprana del ciclo vital del sistema y se corrigen antes de que se apruebe el sistema. No obstante, si se detecta demasiado tarde para la aplicación correcta o completa de una medida de seguridad técnica, la organización responsable de la aplicación y gestión debe identificar y registrar en el registro de peligros claras restricciones de uso aplicables al sistema objeto de evaluación. A menudo, dichas restricciones de uso constituyen limitaciones operativas de aplicación para el sistema objeto de evaluación.

[G 7] Asimismo, podría resultar útil especificar en el registro de peligros si las medidas de seguridad asociadas se aplicarán correctamente en una fase ulterior del ciclo vital del sistema o si éste continuará utilizándose con las restricciones de uso identificadas. También podría resultar útil indicar en el registro de peligros el motivo por el que no se han aplicado correctamente o en su totalidad las medidas de seguridad técnicas asociadas.

[G 8] El agente que recibe las restricciones de uso:

(16) *Si se aplican otras medidas de seguridad en lugar de las especificadas inicialmente, también deben registrarse en el registro de peligros.*

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(a) las importa todas en su propio registro de peligros;
(b) vela por que las condiciones de uso del sistema objeto de evaluación cumplan todas las restricciones de uso recibidas;
(c) verifica y valida el cumplimiento de dichas restricciones de uso por parte del sistema objeto de evaluación.

[G 9] En función de las decisiones acordadas por las organizaciones participantes:

(a) o bien las medidas de seguridad técnicas de que se trate se aplican correctamente en el diseño en una fase ulterior.
La organización que exporta las restricciones de uso sigue realizando un seguimiento de la correcta aplicación técnica de las medidas de seguridad asociadas. Por consiguiente, las medidas de seguridad relacionadas no pueden validarse y los peligros asociados a las mismas no pueden controlarse en el registro de peligros de esta organización en la medida en que no se apliquen plenamente las medidas de seguridad técnicas que corresponda. Esto debe garantizarse aun cuando, entretanto, se establezcan las restricciones de uso exportadas.

(b) o bien las medidas de seguridad técnicas de que se trate no se aplicarán en el diseño en una fase ulterior. Por lo tanto, el sistema seguirá utilizándose durante todo su ciclo vital con las restricciones de uso asociadas. En este caso, podrán darse las siguientes situaciones:

(1) la organización que exporta las restricciones de uso no registra las medidas de seguridad asociadas como “validadas” en su registro de peligros. De ese modo, al utilizar el sistema en cuestión como sistema de referencia en otros proyectos, no se pasarán por alto las correspondientes preocupaciones en materia de seguridad. Así, aun cuando otro agente acepte gestionar los riesgos asociados de otra forma, resulta útil que la organización que exporta las restricciones de uso indique claramente en su registro de peligros que las medidas de seguridad asociadas no se validaron, o;

(2) puede modificarse la descripción del sistema para incluir las restricciones de uso en el ámbito de aplicación del sistema (es decir, supuestos para el sistema) y en los requisitos de seguridad. Esto permitirá controlar los peligros. Así pues, si se utiliza el sistema como sistema de referencia en otra aplicación:

(i) el nuevo sistema deberá utilizarse en las mismas condiciones (es decir, deberá cumplir las restricciones de uso asociadas a dichos supuestos), o;
(ii) el proponente realizará una nueva evaluación del riesgo para las desviaciones con respecto a dichos supuestos.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

5. PRUEBAS DE LA APLICACIÓN DEL PROCESO DE GESTIÓN DEL RIESGO

5.1.	*The risk management process used to assess the safety levels and compliance with safety requirements shall be documented by the proposer in such a way that all the necessary evidence showing the correct application of the risk management process is accessible to an assessment body. The assessment body shall establish its conclusion in a safety assessment report.*

[G 1] El sistema de gestión de la seguridad del administrador de la infraestructura y de la empresa ferroviaria ya aborda estos requisitos. En relación con los otros agentes del sector ferroviario que intervienen en el cambio significativo, aun cuando el sistema de gestión de la seguridad no sea obligatorio, en general, al menos en el nivel del proyecto, disponen de un proceso de gestión de la calidad y/o un proceso de gestión de la seguridad. Ambos procesos se basan en una jerarquía de documentación estructurada, ya sea dentro de la empresa o, al menos, dentro del proyecto. Asimismo, abordan las necesidades de documentación de la gestión en materia de RAMS. Esta documentación estructurada puede comprender esencialmente lo siguiente (véase, asimismo, la Figura 12):

(a) **Planes del proyecto** elaborados para describir la organización que va a establecerse para gestionar una actividad dentro de un proyecto.

(b) **Procedimientos del proyecto** elaborados para describir detalladamente la forma de cumplir un cometido específico. Normalmente, dentro de la empresa existen procedimientos e instrucciones, y se aplican como tales. Sólo se elaboran nuevos procedimientos en caso de que sea necesario describir un cometido específico dentro del proyecto en cuestión.

(c) **Documentos sobre el desarrollo del proyecto** elaborados a lo largo del ciclo vital del sistema representado en la Figura 5.

(d) **Existen modelos de la empresa o al menos del proyecto** para los diferentes tipos de documentos que deben elaborarse.

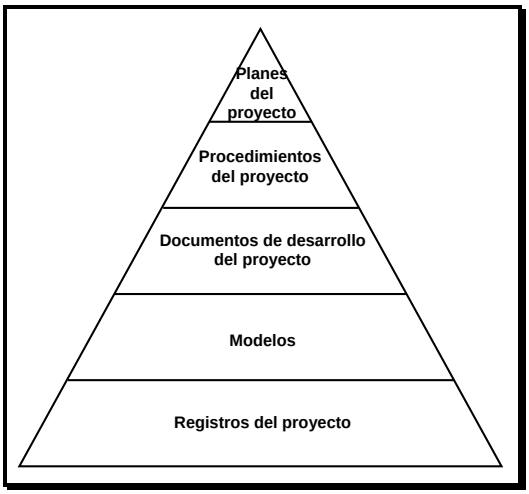


Figura 12: Estructura jerárquica de la documentación.

(e) **Registros del proyecto** elaborados a lo largo del proyecto y necesarios para demostrar el cumplimiento de los procesos de gestión de la calidad y gestión de la seguridad de la empresa.

Esa es una forma de satisfacer las necesidades de evidencias documentales. Podrán existir otras formas de satisfacer dichas necesidades siempre que cumpla los criterios del MCS.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

[G 2] Las normas CENELEC aconsejan que se demuestre que el sistema cumple los requisitos funcionales y de seguridad en un documento de caso de seguridad (o en un informe de seguridad). Aun cuando no sea obligatorio, el uso de un caso de seguridad aporta en un documento estructurado de justificación de la seguridad:

(a) evidencias de gestión de la calidad;
(b) evidencias de gestión de la seguridad;
(c) evidencias de la seguridad funcional y técnica;

Asimismo, ofrece la ventaja de brindar apoyo y orientación al organismo u organismos de evaluación en la evaluación independiente de la correcta aplicación del MCS.

[G 3] El caso de seguridad describe y resume el modo en que se interrelacionan los documentos del proyecto resultantes de la aplicación de los proceso de gestión de la calidad y/o seguridad de la empresa o el proyecto dentro del proceso de desarrollo del sistema para demostrar la seguridad del sistema. Normalmente, el caso de seguridad no incluye grandes volúmenes de evidencias detalladas ni de documentación de apoyo, pero ofrece referencias precisas a tales documentos.

[G 4] **Caso de seguridad para sistemas técnicos:** Las normas CENELEC pueden usarse a modo de orientaciones para la redacción o la estructura de los casos de seguridad:

(a) véase la norma EN 50 129 {Ref. 7} para “Aplicaciones ferroviarias. Sistemas de comunicación, señalización y procesamiento. Sistemas electrónicos de seguridad para la señalización”; en el Apéndice H.2 de la Directriz EN 50 126-2 {Ref. 9} también se propone una estructura para el caso de seguridad de los sistemas de señalización;
(b) véase el Apéndice H.1 de la Directriz EN 50 126-2 {Ref. 9} para la estructura del caso de seguridad del material rodante;
(c) véase el Apéndice H.3 de la Directriz EN 50 126-2 {Ref. 9} para la estructura del caso de seguridad de las infraestructuras.

Como se observa en estas referencias, la estructura del caso de seguridad de los sistemas técnicos, así como su contenido, depende del sistema cuyo cumplimiento en materia de seguridad se va a demostrar.

El caso de seguridad descrito en el Apéndice H de la Directriz EN 50 126-2 {Ref. 9} ofrece únicamente ejemplos, y puede que no sea adecuado para todos los sistemas de la clase de que se trate. Por lo tanto, la descripción debe utilizarse teniendo debidamente en cuenta lo que se ajusta a cada aplicación concreta.

[G 5] **Caso de seguridad para los aspectos organizativos y operativos de sistemas ferroviarios:**

Actualmente no existen normas específicas que proporcionen la estructura, el contenido y una directriz para redactar el caso de seguridad relativo a los aspectos organizativos y operativos de un sistema ferroviario. No obstante, como la finalidad del caso de seguridad es demostrar de forma estructurada que el sistema cumple sus requisitos de seguridad, puede utilizarse la misma clase de estructura de caso de seguridad para los sistemas técnicos. De hecho, las referencias que figuran en el apartado [G 4] de la sección 5.1 ofrecen consejos y una lista de comprobación de puntos que deben abordarse con independencia del tipo de sistema objeto de evaluación. La gestión de cambios organizativos y operativos requiere la misma clase de procesos de gestión de la calidad y gestión de la seguridad que los cambios técnicos, junto con una demostración de que el sistema cumple los requisitos de seguridad especificados. Los requisitos de las normas CENELEC no aplicables a los aspectos organizativos y operacionales son los meramente relacionados con instalaciones de diseño de sistemas técnicos, como, por ejemplo, principios de “seguridad intrínseca inherente a los equipos”, la compatibilidad electromagnética, etc.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

5.2. The document produced by the proposer under point 5.1. shall at least include:

(a) description of the organisation and the experts appointed to carry out the risk assessment process,

(b) results of the different phases of the risk assessment and a list of all the necessary safety requirements to be fulfilled in order to control the risk to an acceptable level.

[G 1] Dependiendo de la complejidad del sistema, estas evidencias pueden recogerse en uno o varios casos de seguridad. Véanse, respectivamente, los apartados [G 4] y [G 5] de la sección 5.1 para la estructura del caso de seguridad relativo a los sistemas técnicos y a los aspectos operativos y organizativos.

[G 2] Consúltese, asimismo, la sección A.4. Evidencias de la evaluación de la seguridad

[G 3] del Apéndice APÉNDICE A: para ver posibles ejemplos de evidencias.

[G 4] En general, se prevé que la vida efectiva de los sistemas y subsistemas técnicos del sector ferroviario sea de unos 30 años. Durante un período de tiempo tan prolongado resulta plausible prever, asimismo, una serie de cambios significativos en dichos sistemas. Por lo tanto, podrían realizarse nuevas evaluaciones de riesgos para estos sistemas y sus interfaces, y la documentación de apoyo deberá revisarse, complementarse y transferirse entre los diversos agentes y organizaciones que usen registros de peligros. Esto implica unos requisitos bastante estrictos en materia de control de la documentación y gestión de la configuración.

[G 4] Resulta útil que la empresa que archive toda la información acerca de la evaluación del riesgo y la gestión del riesgo garantice que los resultados o la información se almacenen en un soporte físico que pueda consultarse o al que pueda accederse durante toda la vida (o el ciclo vital) del sistema (por ejemplo, durante 30 años).

[G 5] Entre las principales razones que justifican este requisito se incluyen:

(a) garantizar que se pueda acceder a todos los análisis de seguridad y registros de seguridad del sistema objeto de evaluación durante toda la vida del sistema. Así:

(1) en caso de producirse nuevos cambios significativos en el mismo sistema, está disponible la documentación más reciente del sistema;

(2) en caso de que surja algún problema durante la vida del sistema, resulta útil que se pueda volver a realizar los análisis de seguridad y registros de seguridad asociados;

(b) velar por que pueda accederse a los análisis de seguridad y registros de seguridad del sistema objeto de evaluación en caso de que se utilice en otra aplicación como sistema de referencia similar.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

ANEXO II AL REGLAMENTO MCS

Criterios que deben cumplir los organismos de evaluación

1.	*The assessment body may not become involved either directly or as authorised representatives in the design, manufacture, construction, marketing, operation or maintenance of the system under assessment. This does not exclude the possibility of an exchange of technical information between that body and all the involved actors.*
2.	*The assessment body must carry out the assessment with the greatest possible professional integrity and the greatest possible technical competence and must be free of any pressure and incentive, in particular of a financial type, which could affect their judgement or the results of their assessments, in particular from persons or groups of persons affected by the assessments.*
3.	*The assessment body must possess the means required to perform adequately the technical and administrative tasks linked with the assessments; it shall also have access to the equipment needed for exceptional assessments.*
4.	*The staff responsible for the assessments must possess:* - *proper technical and vocational training,* - *a satisfactory knowledge of the requirements relating to the assessments that they carry out and sufficient practice in those assessments,* - *the ability to draw up the safety assessment reports which constitute the formal conclusions of the assessments conducted.*
5.	*The independence of the staff responsible for the independent assessments must be guaranteed. No official must be remunerated either on the basis of the number of assessments performed or of the results of those assessments.*
6.	*Where the assessment body is external to the proposer's organisation must have its civil liability ensured unless that liability is covered by the State under national law or unless the assessments are carried out directly by that Member State.*
7.	*Where the assessment body is external to the proposer's organisation its staff are bound by professional secrecy with regard to everything they learn in the performance of their duties (with the exception of the competent administrative authorities in the State where they perform those activities) in pursuance of this Regulation.*

[G 1] No se considera necesario ofrecer una explicación más detallada.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

APÉNDICE A: INFORMACIÓN ADICIONAL

A.1. Introducción

A.1.1. El objetivo de este apéndice es facilitar la comprensión del presente documento. En lugar de ofrecer una gran cantidad de información en el documento, en el presente apéndice se explican en mayor detalle las cuestiones más complejas.

A.2. Clasificación del peligro

A.2.1. En la sección 4.6.3. de la norma EN 50 126-1 {Ref. 8}, así como en el Apéndice B.2 de la Directriz EN 50 126-2 {Ref. 9}, se ofrece una directriz para la clasificación del peligro.

A.3. Criterio de aceptación del riesgo para sistemas técnicos

A.3.1. Límite superior de aceptabilidad del riesgo para sistemas técnicos

A.3.1.1. El criterio de aceptación del riesgo para sistemas técnicos se describe en la sección 2.5.4. de {Ref. 4}.

A.3.1.2. El objetivo del criterio de aceptación del riesgo para sistemas técnicos es especificar un límite superior de la aceptabilidad del riesgo que presentan los sistemas técnicos para los cuales no pueden establecerse requisitos de seguridad mediante la aplicación de códigos prácticos ni mediante la comparación con sistemas de referencia similares. Por consiguiente, define un punto de referencia, a partir del cual pueden adaptarse los métodos de análisis de riesgos para los sistemas técnicos. Como se describe en la sección A.3.6. del Apéndice A del presente documento, este punto de referencia o límite superior de aceptabilidad del riesgo podría utilizarse, asimismo, para establecer los criterios de aceptación del riesgo para otros fallos funcionales de sistemas técnicos que no tienen un potencial directo previsible de producir una consecuencia catastrófica (es decir, para otros niveles de gravedad). Con todo, el criterio de aceptación del riesgo para sistemas técnicos no es un método de análisis de riesgos.

A.3.1.3. El criterio de aceptación del riesgo para sistemas técnicos es un criterio semicuantitativo. Se aplica tanto a los fallos aleatorios de los equipos como a los fallos o errores sistemáticos del sistema técnico. Así pues, también cubre los fallos o errores sistemáticos del sistema técnico que podrían resultar de errores humanos durante el proceso de desarrollo del sistema técnico (es decir, especificación, diseño, aplicación y validación). Sin embargo, el criterio de aceptación del riesgo para sistemas técnicos no cubre los errores humanos durante la explotación y el mantenimiento de los sistemas técnicos.

A.3.1.4. De conformidad con los apéndices A.3 y A.4 de la norma CENELEC 50 129, los fallos o errores sistemáticos no pueden cuantificarse, siendo necesario demostrar el objetivo cuantitativo sólo para los fallos aleatorios de los equipos, mientras que los métodos

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

cualitativos abordan los fallos o errores sistemáticos[17]. *"Dado que no es posible evaluar la integridad del fallo sistemático mediante métodos cuantitativos, se utilizan niveles de integridad de la seguridad para agrupar métodos, herramientas y técnicas que, cuando se usan eficazmente, se considera que ofrecen un nivel adecuado de confianza en el logro de un sistema a un nivel de integridad establecido."*

A.3.1.5. Asimismo, con arreglo a las normas CENELEC, no puede cuantificarse la integridad de los programas informáticos de sistemas técnicos. La norma CENELEC 50 128 proporciona orientaciones para el proceso de desarrollo de programas informáticos relacionados con la seguridad en función del nivel de integridad de la seguridad exigido. Dicho proceso incluye los procesos de diseño, verificación, validación y aseguramiento de la calidad para el programa informático.
Con arreglo a la norma CENELEC 50 128, en relación con un sistema de control electrónico programable que ejecuta funciones de seguridad, el nivel más alto de integridad de la seguridad posible para el proceso de desarrollo del programa informático es SIL 4, que corresponde a una tasa de peligro tolerable cuantitativa de 10^{-9} h^{-1}.

A.3.1.6. Por lo tanto, puesto que no pueden cuantificarse los fallos o errores sistemáticos, deben gestionarse cualitativamente estableciendo un proceso de calidad y un proceso de seguridad que sean compatibles con el nivel de integridad de la seguridad requerido para el sistema objeto de evaluación.

(a) el objetivo del proceso de calidad es *"minimizar la incidencia de errores humanos en cada fase del ciclo vital y, por ende, reducir el riesgo de fallos sistemáticos en el sistema"*;

(b) el objetivo del proceso de seguridad es "*reducir en mayor medida la incidencia de errores humanos relacionados con la seguridad a lo largo del ciclo vital y, por ende, minimizar el riesgo residual de fallos sistemáticos relacionados con la seguridad."*

A.3.1.7. Las normas que se exponen a continuación ofrecen orientaciones para gestionar la incidencia de fallos o errores sistemáticos, así como orientaciones relativas a posibles medidas de diseño para proteger el sistema frente a fallos o averías de causa común y garantizar que el sistema técnico se encuentre en estado de seguridad de funcionamiento en caso de que se produzcan tales fallos o errores:

(a) en la norma CENELEC 50 126-1 {Ref. 8} y su Guía 50 126-2 {Ref. 9} figura una lista de las cláusulas de la norma CENELEC 50 129 y su aplicabilidad en relación con las evidencias documentales de sistemas distintos de los de señalización: véase el Cuadro 9.1 de la Guía 50 126-2 {Ref. 9}. Esta lista hace referencia a las orientaciones acerca del modo de abordar tanto los fallos del propio sistema como el efecto del medio ambiente sobre el sistema objeto de evaluación;

Por ejemplo, se presentan técnicas y medidas relativas a las características de diseño en el *"Cuadro E.5: Características de diseño (mencionadas en el apartado 5.4)"* de la norma CENELEC 50 129 {Ref. 7}, *"para evitar y controlar los fallos causados por:"*

(1) *"cualesquiera fallos de diseño residuales";*

---

(17) *De conformidad con las normas CENELEC 50 126, 50 128 y 50 129, el dato cuantitativo que se ocupa de los fallos aleatorios de los equipos deberá vincularse siempre a un nivel de integridad de la seguridad para gestionar los fallos o errores sistemáticos. Por lo tanto, el dato 10^{-9} h^{-1} del criterio de aceptación del riesgo para sistemas técnicos exige, asimismo, que se establezca un proceso adecuado para gestionar correctamente también los fallos o errores sistemáticos. No obstante, para facilitar la comprensión de la nota, a menudo se refiere sólo a los fallos aleatorios de los equipos del sistema técnico.*

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(2) *"las condiciones ambientales";*
(3) *"el uso inadecuado o errores operativos";*
(4) *"cualesquiera fallos residuales del programa informático";*
(5) *"factores humanos".*

Los Apéndices D y E de la norma CENELEC 50 129 {Ref. 7} presentan técnicas y medidas que permiten evitar que se produzcan fallos sistemáticos y controlar los fallos o errores de señalización aleatorios de los equipos y sistemáticos de sistemas electrónicos relacionados con la seguridad. Muchas de ellas pueden ampliarse a sistemas distintos de los de señalización a través de referencias a estas directrices del Cuadro 9.1 de la Guía 50 126-2 {Ref. 9}.

(b) la norma CENELEC 50 128 ofrece orientaciones relativas al proceso de desarrollo de programas informáticos relacionados con la seguridad en función del nivel de integridad de la seguridad (SIL 0 a SIL 4) que se requiere para el programa informático del sistema objeto de evaluación.

A.3.1.8. El criterio de aceptación del riesgo para sistemas técnicos representa, asimismo, el nivel más alto de integridad que puede requerirse de conformidad con las normas CENELEC e IEC. Para facilitar la consulta, se citan los requisitos de las normas IEC 61508-1 y CENELEC 50 129:

(a) IEC 61508-1: *"Esta norma establece un límite inferior en las medidas de fallo objetivo, en un tipo de fallo peligroso, que puede exigirse. Pueden especificarse como los límites inferiores para el nivel 4 de integridad de la seguridad. Sería posible lograr diseños de sistemas relacionados con la seguridad con valores inferiores para las medidas de fallo objetivo aplicables a sistemas no complejos, pero se considera que las cifras que figuran en el cuadro representan el límite de lo que puede lograrse para sistemas relativamente complejos (por ejemplo, sistemas electrónicos programables relacionados con la seguridad) hoy en día."*

(b) EN 50 129: *"Una función a la que se apliquen requisitos cuantitativos más estrictos que 10^{-9} h^{-1} se tratará de una de las siguientes formas:*

(1) *si es posible dividir la función en subfunciones independientes desde el punto de vista funcional, la tasa de peligro tolerable puede dividirse entre dichas subfunciones y un SIL asignado a cada subfunción;*
(2) *si no puede dividirse la función, se cumplirán al menos las medidas y los métodos requeridos para SIL 4, y se utilizará la función en combinación con otras medidas técnicas u operativas para alcanzar la tasa de peligro tolerable necesaria."*

A.3.1.9. Por lo tanto, todos los sistemas técnicos deben limitar el requisito de seguridad cuantitativo a esa cifra. En caso de que se requiera un nivel de protección superior, no puede alcanzarse con un solo sistema. Es necesario modificar la arquitectura del sistema, por ejemplo, utilizando dos sistemas independientes simultáneamente que realicen controles cruzados para generar resultados seguros. Sin embargo, esto aumenta sin duda alguna los costes de desarrollo del sistema técnico.

Observación: si hay funciones existentes, por ejemplo, sistemas meramente mecánicos, que, sobre la base de la experiencia operativa, podrían haber alcanzado un nivel superior de integridad, podrá recogerse la descripción del nivel de seguridad en un código práctico en particular o podrán fijarse los requisitos de seguridad mediante análisis de similitud con el sistema existente. En el ámbito del MCS, el criterio de aceptación del riesgo para sistemas técnicos sólo debe aplicarse si no existe código práctico o sistema de referencia alguno.

A.3.1.10. Lo anterior puede resumirse como sigue:

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(a) con arreglo a las normas CENELEC 50 126, 50 128 y 50 129, no pueden cuantificarse los fallos o errores sistemáticos en el desarrollo;

(b) es necesario controlar y gestionar la incidencia de fallos o errores sistemáticos, así como su riesgo residual, mediante la aplicación de un proceso de calidad y un proceso de seguridad adecuados que sean compatibles con el nivel de integridad de la seguridad requerido para el sistema objeto de evaluación;

(c) el nivel más alto de integridad de la seguridad es SIL 4 tanto para los fallos aleatorios de equipos como para los fallos o errores sistemáticos de sistemas técnicos;

(d) el límite del nivel de integridad de la seguridad SIL 4 implica que la tasa máxima de peligro tolerable (es decir, la tasa máxima de fallo) para sistemas técnicos debe limitarse también a 10^{-9} h^{-1}.

A.3.1.11. El sistema técnico puede alcanzar una tasa de peligro tolerable de 10^{-9} h^{-1}, ya sea con una "arquitectura a prueba de fallos" (que, por definición, satisface ese nivel de seguridad) o una "arquitectura redundante" (por ejemplo, dos canales de procesamiento independientes que realizan controles cruzados).

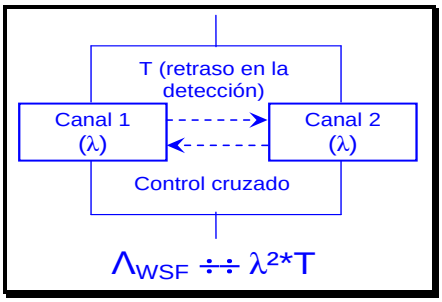


Figura 13: Arquitectura redundante para un sistema técnico

Por lo que respecta a la arquitectura redundante, puede demostrarse que el fallo general contra la seguridad (Λ_{WSF}) del sistema técnico es proporcional a λ^2*T, donde:

(a) λ^2 representa el cuadrado de la tasa de fallo contra la seguridad de un canal;

(b) T representa el tiempo necesario para que un canal detecte el/los fallo(s) contra la seguridad del otro canal. Éste suele ser un múltiplo del tiempo/ciclo de procesamiento de un canal. Normalmente, T es muy inferior a 1 segundo.

A.3.1.12. A partir de esta fórmula (λ^2*T), teóricamente puede demostrarse (considerando sólo los fallos aleatorios de los equipos del sistema técnico – véase, asimismo, el apartado A.3.1.13 del Apéndice A) que puede lograrse un requisito cuantitativo de 10^{-9} h^{-1} en relación con el criterio de aceptación de riesgos para sistemas técnicos. Los fallos o errores sistemáticos deberán gestionarse mediante un proceso: véase el apartado A.3.1.6 del Apéndice A. Por ejemplo:

(a) suponiendo un MTBF de 10 000 horas para el dato de fiabilidad de un canal, y partiendo del supuesto moderado de que todo fallo de un canal es inseguro, el fallo contra la seguridad del canal es de 10^{-4} h^{-1};

(b) incluso con un tiempo de 10 minutos (es decir, $\approx 2*10^{-3}$ horas) para detectar el/los fallo(s) contra la seguridad del otro canal, que también constituye un supuesto moderado;

El incidente general contrario a la seguridad $\Lambda_{WSF} \approx 2 * 10^{-10}$ h^{-1}

A.3.1.13. En la práctica, para una arquitectura redundante como esa, la evaluación de los fallos generales cuantitativos de equipos contra la seguridad debe tener en cuenta las medidas de diseño adoptadas para proteger el sistema frente a fallos o averías de causa común y garantizar que el sistema técnico se encuentre en estado de seguridad de funcionamiento en caso de que se produzca un fallo o error de causa común. Por lo tanto, esta evaluación del fallo general contra la seguridad (Λ_{WSF}) debe tener en cuenta, asimismo:

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(a) los componentes comunes a todos los canales, tales como un solo dato o datos comunes a todos los canales, una fuente de alimentación común, comparadores, dispositivos de toma de decisión, etc.;

(b) el tiempo necesario para detectar los fallos latentes. Para sistemas técnicos complejos, este tiempo puede ser superior en varios órdenes de magnitud a 1 segundo;

(c) el impacto de los fallos o averías de causa común.

En las normas que se recuerdan en el apartado A.3.1.7. del Apéndice A de este documento pueden encontrarse orientaciones sobre estas cuestiones.

A.3.2. Diagrama de comprobación de la aplicabilidad del criterio de aceptación del riesgo para sistemas técnicos

A.3.2.1. La forma de aplicar el criterio de aceptación del riesgo para sistemas técnicos a peligros derivados de fallos de sistemas técnicos puede representarse como se muestra en la Figura 14.

A.3.2.2. En la sección C.15. del Apéndice C se ofrece un ejemplo de la aplicación de ese diagrama.

A.3.3. Definición de un sistema técnico según el Reglamento MCS

A.3.3.1. El criterio de aceptación del riesgo para sistemas técnicos se aplica únicamente a sistemas técnicos. El 1.1.1.[G 1](22) del Reglamento MCS recoge la siguiente definición de “sistema técnico”:

«sistema técnico», un producto o un conjunto de productos, incluidos el diseño, la aplicación y la documentación de apoyo; el desarrollo de un sistema técnico comienza con la especificación de sus requisitos y termina con su aceptación; aunque el diseño de las interfaces pertinentes con el comportamiento humano se tiene en cuenta, los operadores humanos y sus acciones no se incluyen en el sistema técnico; el proceso de mantenimiento se describe en los manuales de mantenimiento pero no forma parte en sí mismo del sistema técnico;

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

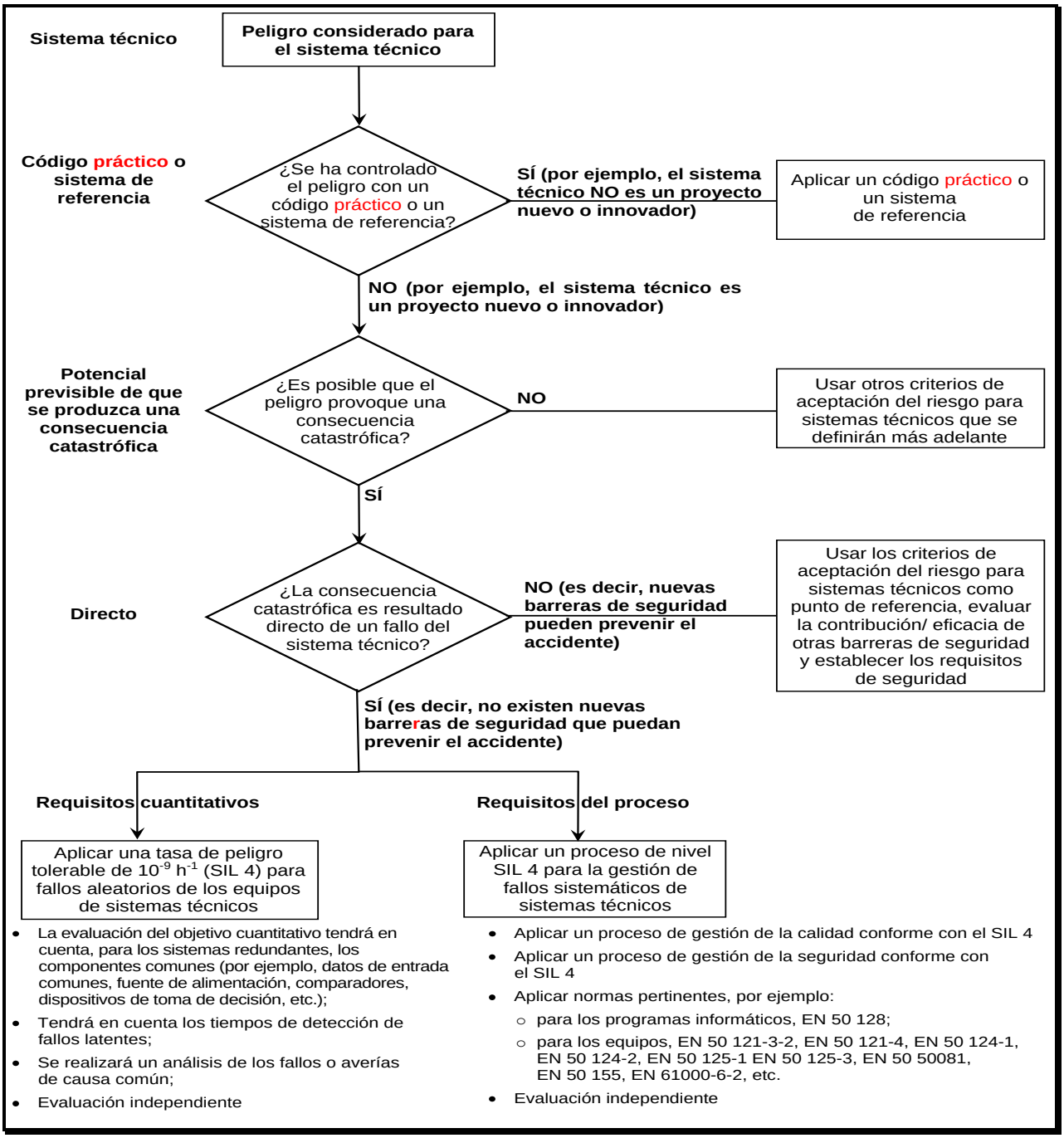


Figura 14: Diagrama de comprobación de la aplicabilidad del criterio de aceptación del riesgo para sistemas técnicos

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

A.3.4. Explicación de la definición del "sistema técnico"

A.3.4.1. La siguiente definición de sistema técnico describe el ámbito de aplicación del sistema técnico: *"un producto o un conjunto de productos, incluidos el diseño, la aplicación y la documentación de apoyo."* Por lo tanto, comprende e incluye:

(a) los elementos físicos que constituyen el sistema técnico;
(b) los programas informáticos asociados (en su caso);
(c) el diseño y la aplicación del sistema técnico, incluida, si procede, la configuración o determinación de parámetros de un producto genérico en relación con requisitos específicos de la aplicación específica;
(d) la documentación de apoyo necesaria para:

(1) el desarrollo del sistema técnico;
(2) la explotación y el mantenimiento del sistema técnico;

A.3.4.2. Las notas asociadas a esta definición especifican en mayor detalle el ámbito de aplicación del sistema técnico:

(a) *"El desarrollo de un sistema técnico comienza con la especificación de sus requisitos y termina con la aceptación de la seguridad"*. Incluye las fases 1 a 10 del ciclo en V representado en la Figura 10 de la norma CENELEC 50 126-1 {Ref. 8};

(b) *"Incluye el diseño de interfaces pertinentes que implican una intervención humana. No obstante, los operadores humanos y las medidas adoptadas por éstos no forman parte de un sistema técnico."* Si bien los errores de factor humano cometidos durante la explotación y el mantenimiento del sistema técnico no forman parte del propio sistema técnico, el diseño de las interfaces con las acciones humanas debe tenerlos en cuenta. El objetivo es minimizar la probabilidad de errores humanos debidos a un diseño deficiente de las interfaces relacionadas con las acciones humanas;

(c) *"El mantenimiento no se incluye en la definición, sino en manuales de mantenimiento."* Esto significa que es necesario aplicar el criterio de aceptación del riesgo para sistemas técnicos a la explotación y el mantenimiento del sistema técnico; éstos dependen ampliamente de procesos y acciones realizados por personal humano. No obstante, para apoyar el mantenimiento de sistemas técnicos, la definición del sistema técnico debe incluir cualesquiera requisitos involucrados (por ejemplo, mantenimiento periódico preventivo, o mantenimiento correctivo en caso de fallos), con suficiente grado de detalle. Sin embargo, el modo en que debe organizarse y efectuarse el mantenimiento del sistema técnico afectado no forma parte de la definición del sistema técnico, sino de los correspondientes manuales de mantenimiento.

A.3.4.3. Véase, asimismo, la sección A.3.1. del Apéndice A.

A.3.5. Funciones de sistemas técnicos a las que se aplican el criterio de aceptación del riesgo para sistemas técnicos

A.3.5.1. Con arreglo a la definición del criterio de aceptación del riesgo para sistemas técnicos, éste se aplica a fallos contra la seguridad de las funciones que debe cumplir el sistema técnico en caso de que tengan *"un potencial **directo** previsible de producir una consecuencia catastrófica"*: véase la sección 2.5.4. de {Ref. 4}.

A.3.5.2. El criterio de aceptación del riesgo para sistemas técnicos también puede aplicarse a funciones en las que intervienen sistemas técnicos, pero cuyos fallos **no tienen un** *"potencial **directo** previsible de producir una consecuencia catastrófica"*. En este caso, es

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

necesario aplicar el criterio de aceptación del riesgo para sistemas técnicos como objetivo general para la serie de sucesos que lleva a una consecuencia catastrófica. Sobre la base de este objetivo general, la contribución real de cada suceso, y, por tanto, de los fallos funcionales del sistema técnico involucrado en el supuesto considerado, debe establecerse de conformidad con lo dispuesto en la sección A.3.6. del Apéndice A.
Tal uso del criterio de aceptación del riesgo para sistemas técnicos todavía debe debatirse y acordarse con el grupo de trabajo de MCS.

A.3.5.3. ¿A qué funciones del sistema técnico se aplica el criterio de aceptación del riesgo para sistemas técnicos? Con arreglo a la norma IEC 61226:2005:

(a) una función se define en este contexto como un *"propósito u objetivo específico que se debe cumplir que puede especificarse o describirse sin hacer referencia a los medios físicos para lograrlo"*;
(b) una función (considerada como una caja negra) transfiere parámetros de entrada (por ejemplo, material, energía, información) en los parámetros de salida relacionados (por ejemplo, material, energía, información);
(c) el análisis de la función es independiente de su realización técnica.

A.3.5.4. El criterio de aceptación del riesgo para sistemas técnicos se aplica a los siguientes tipos de funciones:

(a) ejemplos que se refieren al subsistema ETCS de a bordo:

(1) "proporcionar al maquinista información para que pueda conducir el tren de manera segura y aplicar un frenado en caso de exceso de velocidad". Basándose en la información recibida desde tierra (velocidad permitida) y en el cálculo de la velocidad del tren obtenido del ETCS de a bordo, el maquinista y el ETCS de a bordo pueden supervisar que los trenes no excedan el límite de velocidad permitido. El criterio de aceptación del riesgo para sistemas técnicos se aplica a la evaluación de la velocidad del tren realizada por el ETCS de a bordo, ya que:

(i) no existen nuevos obstáculos (directos) en la medida en que la información facilitada al maquinista también está insuficientemente evaluada;
(ii) el exceso de velocidad del tren podría llevar al descarrilamiento, que constituye un accidente con posibles consecuencias catastróficas;

(2) "proporcionar al maquinista información para que pueda conducir el tren de manera segura y aplicar un frenado en caso de violación de la autoridad de movimiento permitida".

(b) ejemplo que se refiere a un circuito de vía: "detectar la ocupación de un tramo de vía". El criterio de aceptación del riesgo para sistemas técnicos será aplicable como tal a esta función sólo si no se ha aplicado una función de "control de secuencia" en el enclavamiento;
(c) ejemplo de un punto: "controlar la posición de un punto";

A.3.5.5. Algunas normas también definen funciones a las que podría ser aplicable el criterio de aceptación del riesgo para sistemas técnicos. Por ejemplo:

(a) la norma prEN 0015380-4 {Ref. 13} (ModTrain Work) define en su parte normativa tres niveles jerárquicos de funciones (ampliados en anexos informativos a hasta cinco niveles). En total, la norma prEN 0015380-4 define varios centenares de funciones relacionadas con trenes;
(b) en general, se recomienda seleccionar funciones de los tres primeros niveles de la norma prEN 0015380-4 (pero no inferior), teniendo en cuenta asimismo la estructura desglosada del producto;

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(c) en cuanto a las funciones que no entran en el ámbito de aplicación de la norma prEN 0015380-4, es necesario determinar el nivel funcional adecuado mediante comparación, recurriendo a la opinión de expertos.

La Agencia debe seguir trabajando en estos ejemplos de funciones de la norma prEN 0015380-4 en el marco de la labor que realiza en materia de riesgos ampliamente aceptables y criterios de aceptación del riesgo.

A.3.5.6. El criterio de aceptación del riesgo para sistemas técnicos también es aplicable, por ejemplo, a la siguiente función de la norma prEN 0015380-4: *"control de inclinación"* (código = CLB). Esta función podría utilizarse en el nivel del sistema de dos maneras:

(a) primer caso: el tren se inclinará en las curvas para la comodidad de los pasajeros y debe controlar que el gálibo del tren se ajuste a la infraestructura terrestre;
(b) segundo caso: el tren se inclinará en las curvas para la comodidad de los pasajeros, pero no es necesario que controle que el gálibo del tren se ajuste a la infraestructura terrestre;

El criterio de aceptación del riesgo para sistemas técnicos se aplicará en el primer caso, pero no en el segundo, ya que el fallo de la función de inclinación no tiene consecuencias catastróficas.

A.3.5.7. El ejemplo que figura en la letra (b) del apartado A.3.5.4. y los ejemplos que se exponen en el apartado A.3.5.6. del Apéndice A muestran claramente que no resultará viable elaborar una lista predeterminada de funciones en las que el criterio de aceptación del riesgo para sistemas técnicos se aplique en todos los casos. Esto dependerá siempre de la manera en que el sistema utilice estas funciones del subsistema.

A.3.5.8. En la sección C.15. del Apéndice C se ofrece un ejemplo de la aplicación del criterio de aceptación del riesgo para sistemas técnicos.

A.3.6. Ejemplos de aplicación del criterio de aceptación del riesgo para sistemas técnicos

A.3.6.1. Introducción

(a) en este capítulo se muestran ejemplos sobre la manera de determinar la tasa de fallo para otros niveles de gravedad del peligro y la manera de establecer requisitos de seguridad inferiores a $10^{-9}\ h^{-1}$. Este documento no da prioridad ni obliga a la aplicación de un método en particular. Tan sólo muestra, a título informativo, la manera en que puede usarse el criterio de aceptación del riesgo para sistemas técnicos a fin de adaptar algunos métodos ampliamente utilizados. La Agencia debe seguir desarrollándolo en su labor en materia de riesgos ampliamente aceptables y criterios de aceptación del riesgo.

(b) De hecho, el criterio de aceptación del riesgo para sistemas técnicos podrá aplicarse directamente sólo a un reducido número de casos, ya que en la práctica no son muchos los fallos funcionales de sistemas técnicos que provocan accidentes que podrían tener consecuencias catastróficas. Por lo tanto, a fin de aplicar el criterio a peligros que no tienen consecuencias catastróficas y determinar el objetivo de tasa de fallo, es posible realizar correlaciones (por ejemplo, adaptando una matriz de riesgo con este criterio) entre diferentes parámetros, tales como la gravedad frente a la frecuencia.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

A.3.6.2. Ejemplo 1: Correlación directa del riesgo

(a) el criterio de aceptación del riesgo para sistemas técnicos puede aplicarse fácilmente a supuestos que sólo difieren en unos pocos parámetros independientes de las condiciones de referencia definidas en el criterio de aceptación del riesgo para sistemas técnicos de la sección 2.5.4. del Reglamento MCS **Error! Reference source not found.**;

(b) supongamos que para un parámetro p en particular la relación con el riesgo es multiplicativa. Supongamos que en la condición de referencia se halla presente el parámetro p*, mientras que en el supuesto alternativo es aplicable p‘. En este caso sólo es pertinente la relación entre los parámetros p*/p’ y podrá reducirse la tasa de incidencia. Este procedimiento puede repetirse si los parámetros son independientes.

(c) Ejemplo:

(1) supongamos que la opinión de expertos ha estimado que el potencial real de la consecuencia catastrófica es diez veces inferior al potencial que tiene en las condiciones de referencia indicadas en la sección 2.5.4 del Reglamento MCS **Error! Reference source not found.**. En este caso, el requisito sería $10^{-8}\,h^{-1}$ en lugar de $10^{-9}\,h^{-1}$.

(2) supongamos que otro sistema técnico identifique una nueva barrera de seguridad (independiente de las consecuencias), que es efectiva en el 50% de los casos;

(3) en este caso, el requisito de seguridad sería $5*10^{-7}\,h^{-1}$ (es decir, $0{,}5*10^{-8}\,h^{-1}$) en lugar de $10^{-9}\,h^{-1}$.

A.3.6.3. Ejemplo 2: Adaptación de la matriz de riesgo

(a) para usar adecuadamente el criterio de aceptación del riesgo para sistemas técnicos en una matriz de riesgo, la matriz tiene que estar relacionada con el nivel correcto del sistema (comparable al que se indica en la sección A.3.5. del Apéndice A).

(b) el criterio de aceptación del riesgo para sistemas técnicos define un campo de la matriz de riesgo como tolerable, que corresponde a la coordenada (gravedad catastrófica; tasa de incidencia de $10^{-9}\,h^{-1}$): véase el campo rojo en el Cuadro 5. Todos los campos relacionados con una frecuencia superior deben marcarse como “intolerables”. Cabe señalar que, sólo en caso de que exista un potencial directo previsible de que se produzca una consecuencia catastrófica, la frecuencia de accidentes es similar a la frecuencia de fallo funcional.

(c) a continuación, puede rellenarse el resto de la matriz, no obstante, deben tenerse en cuenta los efectos como la aversión al riesgo o la proporcionalidad de las categorías. En el caso más sencillo de proporcionalidad decenal lineal (como muestra la flecha en el Cuadro 5), el campo marcado como “aceptable” por el criterio de aceptación del riesgo para sistemas técnicos es extrapolado de forma lineal al resto de la matriz. Esto significa que todos los campos que se hallan en la misma diagonal (o por debajo de la diagonal) también son marcados como “aceptables”. Los campos que se hallan por debajo de dicha diagonal también pueden marcarse como “aceptables”.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

Cuadro 5: Ejemplos típicos de una matriz de riesgo adaptada.

Frecuencia con que se produce un accidente (causado por un peligro)	**Niveles de riesgo**			
Frecuente (10^{-4} por hora)	**Intolerable**	**Intolerable**	**Intolerable**	**Intolerable**
Probable (10^{-5} por hora)	**Intolerable**	**Intolerable**	**Intolerable**	**Intolerable**
Ocasional (10^{-6} por hora)	**Aceptable**	**Intolerable**	**Intolerable**	**Intolerable**
Remoto (10^{-7} por hora)	**Aceptable**	**Aceptable**	**Intolerable**	**Intolerable**
Improbable (10^{-8} por hora)	**Aceptable**	**Aceptable**	**Aceptable**	**Intolerable**
Imprevisible (10^{-9} por hora)	**Aceptable**	**Aceptable**	**Aceptable**	**Aceptable**
	Insignificante	Marginal	Crítico	Catastrófico
	Niveles de gravedad de la consecuencia de un peligro (es decir, de un accidente)			

Valoración del riesgo	**Reducción/Control del riesgo**
Intolerable	Se eliminará el riesgo.
Aceptable	El riesgo es aceptable. Se requiere una evaluación independiente.

(d) una vez que se ha rellenado la matriz, también puede aplicarse a peligros sin consecuencias catastróficas. Por ejemplo, si la gravedad de otro fallo funcional se clasifica como “crítica”, con la matriz de riesgo adaptada la frecuencia tolerable de accidentes debería situarse en una categoría no superior a “improbable” (o incluso inferior).

(e) cabe observar que el uso de la matriz de riesgo podrá llevar a unos resultados excesivamente conservadores, cuando se aplique a la frecuencia de fallos funcionales (es decir, para fallos funcionales que no provoquen accidentes).

A.3.6.4. Principio para adaptar otros métodos de análisis de riesgos

También pueden adaptarse con un procedimiento similar al descrito para la matriz de riesgo otros métodos de análisis de riesgos, por ejemplo, el sistema de número de prioridad del riesgo o el gráfico de riesgos propuestos en VDV 331 o IEC 61508:

(a) primer paso: clasificar el punto de referencia del criterio de aceptación del riesgo para sistemas técnicos como tolerable, y los puntos de mayor frecuencia o mayor gravedad como criterios de aceptación del riesgo para sistemas técnicos intolerables.
(b) segundo paso: utilizar los mecanismos de correlación del método que se aplique para extrapolar la tolerabilidad del riesgo a peligros sin consecuencias catastróficas (usando la compensación lineal del riesgo como punto de partida).
(c) tercer paso: por lo que se refiere a los peligros sin consecuencias catastróficas, puede establecerse el criterio de aceptación del riesgo para sistemas técnicos a través del método de análisis de riesgos adaptado, comparando la coordenada (frecuencia; gravedad) con la curva FN obtenida.

A.3.7. Conclusiones sobre el criterio de aceptación del riesgo para sistemas técnicos

A.3.7.1. En el marco general de evaluación del riesgo propuesto por el MCS, los criterios de aceptación del riesgo son necesarios para determinar cuándo pasa a ser aceptable el nivel residual de riesgo(s) y, por tanto, cuándo hay que detener la estimación explícita del riesgo.

A.3.7.2. El criterio de aceptación del riesgo para sistemas técnicos es un objetivo de diseño (10^{-9} h^{-1}) para sistemas técnicos.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

A.3.7.3. Los principales objetivos del criterio de aceptación del riesgo para sistemas técnicos son:

(a) especificar un límite superior de aceptabilidad del riesgo, y por consiguiente un punto de referencia, a partir del cual puedan adaptarse los métodos de análisis de riesgos para los sistemas técnicos;
(b) permitir el reconocimiento mutuo de sistemas técnicos, ya que las evaluaciones del riesgo asociado y de la seguridad se evaluarán aplicando el mismo criterio de aceptación del riesgo en todos los Estados miembros;
(c) ahorrar costes, puesto que no exige innecesariamente elevados requisitos de seguridad cuantitativos;
(d) promover la competencia entre los fabricantes. El uso de diferentes criterios de aceptación del riesgo en función del proponente o del Estado miembro llevaría al sector a realizar muchas demostraciones diferentes en los mismos sistemas técnicos. Por consiguiente, afectaría a la competitividad de fabricantes y elevaría innecesariamente el coste de los productos.

A.3.7.4. Por lo que respecta a los sistemas técnicos, no es siempre necesario demostrar el requisito semicuantitativo incluido en el criterio de aceptación del riesgo para sistemas técnicos. De hecho, en el ámbito de aplicación del MCS, el criterio de aceptación del riesgo para sistemas técnicos sólo debe aplicarse a sistemas técnicos para los cuales los peligros identificados no pueden controlarse adecuadamente usando códigos prácticos ni estableciendo una comparación con sistemas de referencia similares. Ello permite establecer requisitos de seguridad inferiores, siempre y cuando pueda mantenerse el nivel de seguridad global.

A.3.7.5. Sólo cuando no existe código práctico ni sistema de referencia alguno se requiere un criterio de aceptación del riesgo semicuantitativo armonizado para sistemas técnicos.

A.3.7.6. Como el nivel de integridad de la seguridad para fallos o errores sistemáticos se limita a SIL 4, el nivel de integridad de la seguridad para los fallos aleatorios de equipos de sistemas técnicos también debe limitarse a SIL 4. Este nivel equivale a una tasa máxima de peligro tolerable de $10^{-9}\,h^{-1}$ (es decir, la tasa máxima de fallo). Con arreglo a la norma CENELEC 50 129, si se requieren requisitos de seguridad más estrictos, este requisito no puede cumplirse con un solo sistema; es necesario cambiar la arquitectura del sistema, por ejemplo, usando dos sistemas que inevitablemente aumentan los costes de forma drástica. Para obtener más detalles, véase la sección A.3.1. del Apéndice A.

A.3.7.7. Por último, en la sección A.3.6. del Apéndice A se describe la manera en que puede usarse el criterio de aceptación del riesgo para sistemas técnicos como punto de referencia para adaptar métodos específicos de análisis de riesgos cuando los sistemas técnicos tengan un potencial de producir consecuencias menos graves que catastróficas.

A.4. Evidencias de la evaluación de la seguridad

A.4.1. Esta sección ofrece orientaciones sobre las evidencias que normalmente se proporcionan a un organismo de evaluación a fin de que pueda realizarse una evaluación independiente y obtenerse la aceptación de la seguridad sin perjuicio de los requisitos nacionales de un Estado miembro. Éstas pueden servir a modo de lista de comprobación para verificar que se cubren y documentan todos los aspectos asociados, cuando proceda, durante la aplicación del MCS.

A.4.2. Plan de seguridad: CENELEC aconseja que se elabore un plan de seguridad al principio del proyecto o, si no resulta oportuno para el proyecto, que se incluya la descripción correspondiente en cualquier otro documento relacionado. Si se designan organismos de

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

evaluación al inicio del proyecto, también puede presentarse el plan de seguridad para que éstos emitan su dictamen. En principio, el plan de seguridad describe:

(a) la organización establecida y la competencia de las personas que participan en el desarrollo y en la evaluación del riesgo;
(b) todas las actividades relacionadas con la seguridad planificadas a lo largo de las distintas fases del proyecto, así como los resultados previstos;

A.4.3. Evidencias necesarias de la fase de definición del sistema:

(a) descripción del sistema:

(1) definición del ámbito de aplicación/de los límites del sistema;
(2) descripción de las funciones;
(3) descripción de la estructura del sistema:
(4) descripción de las condiciones operativas y ambientales;

(b) descripción de las interfaces externas;
(c) descripción de las interfaces internas;
(d) descripción de las fases del ciclo vital;
(e) descripción de los principios de seguridad;
(f) descripción de los supuestos en los que se definen los límites de la evaluación del riesgo;

A.4.4. Para que pueda realizarse la evaluación del riesgo, la definición del sistema tiene en cuenta el contexto del cambio previsto:

(a) si el cambio previsto es una modificación de un sistema existente, la definición del sistema describe tanto el sistema antes del cambio como el cambio previsto;
(b) si el cambio previsto es la construcción de un nuevo sistema, la descripción se limita a la definición del sistema, puesto que no hay descripción de sistema existente alguno.

A.4.5. Evidencias necesarias de la fase de determinación del peligro:

(a) descripción y justificación (incluidas las limitaciones) de métodos y herramientas para la determinación del peligro (método descendente, ascendente, HAZOP, etc.);
(b) resultados:

(1) listas de peligros:
(2) peligros (del límite) del sistema;
(3) peligros del subsistema;
(4) peligros de la interfaz;
(5) las medidas de seguridad que podrían identificarse durante esta fase;

A.4.6. También se requieren las evidencias de la fase de análisis de riesgos siguientes:

(a) cuando se usen códigos prácticos para controlar riesgos, demostración de que el sistema objeto de evaluación cumple todos los requisitos relevantes de los códigos prácticos. Esto incluye demostrar la correcta aplicación de los códigos prácticos afectados;

(b) cuando se usen sistemas de referencia similares para controlar peligros:

(1) definición de los requisitos de seguridad de los sistemas de referencia similares aplicables al sistema objeto de evaluación;
(2) demostración de que el sistema objeto de evaluación se usa en condiciones operativas y ambientales similares a las del sistema de referencia involucrado. De ser posible se requiere una demostración de que se han evaluado correctamente las desviaciones con respecto al sistema de referencia;

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(3) evidencia de que los requisitos de seguridad de los sistemas de referencia se aplican correctamente en el sistema objeto de evaluación;

(c) cuando se recurra a una estimación del riesgo para controlar peligros:

(1) descripción y justificación (incluidas las limitaciones) del método y las herramientas de análisis de riesgos (análisis cualitativo, cuantitativo, semicuantitativo, de no regresión,...);
(2) determinación de medidas de seguridad y factores de reducción del riesgo existentes para cada peligro (incluidos los aspectos del factor humano);
(3) evaluación y clasificación del riesgo para cada peligro:

(i) estimación de consecuencias de peligro y justificación (con supuesto y condiciones);
(ii) estimación de la frecuencia del peligro y justificación (con supuesto y condiciones);
(iii) clasificación de peligros según su carácter crítico y frecuencia de aparición;

(4) determinación de nuevas medidas de seguridad adecuadas que resulten en riesgos aceptables para cada peligro (proceso iterativo tras la fase de valoración del riesgo);

A.4.7. Evidencias necesarias de la evaluación del riesgo:

(a) cuando se realice una estimación explícita del riesgo:

(1) definición y justificación de los criterios de evaluación del riesgo para cada peligro;
(2) demostración/justificación de que las medidas de seguridad y los requisitos de seguridad cubren cada uno de los peligros a un nivel aceptable (según el criterio de evaluación del riesgo anteriormente referido);

(b) en virtud de las secciones 2.3.5 y 2.4.3 del Reglamento MCS, los riesgos cubiertos por la aplicación de códigos prácticos y por la comparación con sistemas de referencia se consideran implícitamente aceptables siempre que, respectivamente, (véanse los puntos delimitados por un círculo de puntos de la Figura 1):

(1) se reúnan las condiciones de aplicación de códigos prácticos de la sección 2.3.2;
(2) se reúnan las condiciones de uso de un sistema de referencia de la sección 2.4.2;

Los criterios de aceptación del riesgo son implícitos para estos dos principios de aceptación del riesgo.

A.4.8. Evidencias de la gestión del peligro:

(a) registro de todos los peligros en un registro de peligros, incluidos los siguientes elementos:

(1) peligro identificado;
(2) medidas de seguridad que prevengan la aparición de peligros o mitiguen sus consecuencias;
(3) requisitos de seguridad de las medidas;
(4) parte relevante del sistema;
(5) agente responsable de las medidas de seguridad;
(6) estatus del peligro (por ejemplo, no controlado, resuelto, eliminado, transferido, controlado, etc.);
(7) fecha de registro, revisión y control de cada peligro;

(b) descripción de cómo se gestionarán eficazmente los peligros durante todo el ciclo vital;
(c) descripción del intercambio de información entre las partes relativa a los peligros en las interfaces y la asignación de responsabilidades.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

A.4.9. Evidencias relacionadas con la calidad de la valoración del riesgo y el proceso de evaluación:

(a) descripción de las personas que participan en el proceso y su competencia;
(b) por lo que respecta a las estimaciones explícitas del riesgo: descripción de la información, datos y otras estadísticas utilizados en el proceso, y justificación de su idoneidad (por ejemplo, análisis de sensibilidad de los datos utilizados).

A.4.10. Evidencias de cumplimiento de los requisitos de seguridad:

(a) lista de normas utilizada;
(b) descripción del diseño y de los principios operativos;
(c) evidencias de la aplicación de un sistema de gestión de la calidad y seguridad satisfactorio para el proyecto: véase el apartado [G 3] de la sección 1.1.2.
(d) resumen de informes de análisis de la seguridad (por ejemplo, análisis de la causa del peligro) que demuestren el cumplimiento de los requisitos de seguridad;
(e) descripción y justificación de métodos y herramientas (FMECA, FTA, …) que se usan para analizar la causa del peligro;
(f) resumen de evidencias de verificación y validación de la seguridad.

A.4.11. Caso de seguridad: CENELEC aconseja que todas las evidencias anteriormente mencionadas se reagrupen y resuman en un documento que deberá presentarse al organismo de evaluación: véanse los apartados [G 4] y [G 5] de la sección 5.1.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

APÉNDICE B: EJEMPLOS DE TÉCNICAS Y HERRAMIENTAS DE APOYO AL PROCESO DE EVALUACIÓN DEL RIESGO

B.1. En el Anexo E de la guía EN 50126-2 {Ref. 9} figuran ejemplos de técnicas y herramientas para llevar a cabo las actividades de evaluación del riesgo cubiertas por el MCS. En el Cuadro E.1 se ofrece un resumen de técnicas y herramientas, en el que se describe cada una de las técnicas y, en la medida de lo necesario, se hace referencia a otra norma para más información.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

APÉNDICE C: EJEMPLOS

C.1. Introducción

C.1.1. El objetivo de este apéndice es facilitar la comprensión del presente documento. Reúne todos los ejemplos recabados que tienen por objeto facilitar la aplicación del MCS.

C.1.2. Los ejemplos de evaluaciones del riesgo o de la seguridad que se ofrecen en este apéndice no se derivan de la aplicación del proceso del MCS, dado que se llevaron a cabo con anterioridad al Reglamento MCS. Los ejemplos pueden clasificarse en:

(a) ejemplos que hacen referencia a su origen recibidos de expertos del grupo de trabajo MCS
(b) ejemplos que, de manera intencionada, no hacen referencia a su origen también recibidos de expertos del grupo de trabajo MCS Los expertos en cuestión pidieron que se mantuviera la confidencialidad de su origen;
(c) ejemplos cuyo origen no se menciona elaborados por miembros del personal de la Agencia basándose en su experiencia profesional personal anterior.

Para cada ejemplo se ofrece un seguimiento de correlación entre el proceso aplicado y el establecido por el MCS, así como el razonamiento y el valor añadido para realizar los pasos adicionales (si hubiera) que exige el MCS.

C.2. Ejemplos de aplicación de criterios para un cambio significativo del Artículo 1.Artículo 4 (2)

C.2.1. La Agencia está trabajando en la definición de lo que puede considerarse un “cambio significativo”. En esta sección se ofrece un ejemplo extraído de ese trabajo de cómo aplicar los criterios del Artículo 1.Artículo 4 (2).

C.2.2. El cambio consiste en modificar en un paso a nivel de accionamiento manual la manera en que los responsables de circulación comunican al operador del paso a nivel la información acerca de la dirección de un tren que se aproxima. Este cambio se representa en la Figura 15.

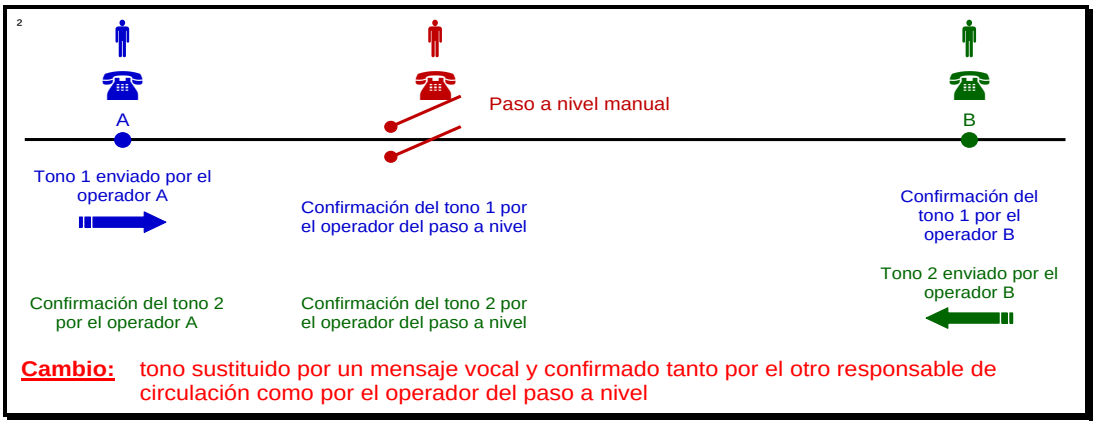


Figura 15: Ejemplo de un cambio no significativo Mensaje telefónico para controlar un paso a nivel.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

C.2.3. Sistema existente: antes de realizar el cambio previsto, la información acerca de la dirección de un tren que se aproxima se comunicaba automáticamente al operador del paso a nivel mediante el tono de llamada del teléfono. El tono variaba dependiendo de la procedencia de la llamada.

C.2.4. Cambio previsto: dado que el antiguo sistema telefónico queda obsoleto y debe sustituirse por un nuevo sistema digital, técnicamente ya no puede incluirse la información pertinente en el tono. El tono es exactamente el mismo, independientemente del responsable de circulación que realice la llamada. Así pues, se ha decidido realizar la misma función con un procedimiento operativo:

(a) a la salida del tren, el responsable de circulación informa verbalmente al operador del paso a nivel de la dirección del tren que se aproxima;
(b) la información se coteja con el horario y la confirman tanto el operador del paso a nivel como el otro responsable de circulación a fin de evitar un malentendido por parte del operador.

El cambio previsto y el procedimiento operativo asociado se ilustran en la Figura 15.

C.2.5. Aunque parezca que el cambio tiene un posible impacto para la seguridad (riesgo de no cerrar a tiempo la barrera del paso a nivel), otros criterios que figuran en el Artículo 1.Artículo 4 (2) como:

(a) baja complejidad;
(b) falta de innovación, y;
(c) facilidad de control;

podrán sugerir que el cambio previsto no es un cambio significativo.

C.2.6. En cualquier caso, en este ejemplo se precisa un análisis de la seguridad o argumento para demostrar que, en relación con esta importante función de seguridad, al sustituir un antiguo sistema técnico por un procedimiento operativo (en el que el personal realiza controles cruzados) se obtendría un nivel de seguridad similar. La cuestión consiste en saber si esto requeriría la aplicación de todo el proceso MCS, que incluye un registro de peligros, una evaluación independiente a cargo de un organismo de evaluación, etc. En este caso, es cuestionable si esto aportaría algún valor añadido, lo que implica que un cambio como ese podría, entonces, no considerarse significativo.

C.3. Ejemplos de interfaces entre agentes del sector ferroviario

C.3.1. A continuación se exponen algunos ejemplos de interfaces y motivos de la cooperación entre agentes del sector ferroviario:

(a) Administrador de la infraestructura – Administrador de la infraestructura: por ejemplo, ambas infraestructuras contemplarán la adopción de medidas de seguridad para garantizar una transición de trenes segura desde una infraestructura a la otra;

(b) Administrador de la infraestructura – Empresa ferroviaria: por ejemplo, podría haber normas operativas específicas supeditadas a la infraestructura que deberá cumplir el maquinista del tren;

(c) Administrador de la infraestructura – Fabricante: por ejemplo, los subsistemas del fabricante podrían tener restricciones de uso que deberá cumplir el administrador de la infraestructura;

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(d) Administrador de la infraestructura – Proveedor de servicios: por ejemplo, podrían haber limitaciones específicas en el mantenimiento de infraestructuras que deberá cumplir el subcontratista de las actividades de mantenimiento;

(e) Empresa ferroviaria – Fabricante: por ejemplo, los subsistemas del fabricante podrían tener restricciones de uso que deberá cumplir la empresa ferroviaria;

(f) Empresa ferroviaria – Proveedor de servicios: por ejemplo, podrían haber limitaciones específicas en el mantenimiento de infraestructuras que deberá cumplir el subcontratista de las actividades de mantenimiento;

(g) Empresa ferroviaria – Poseedores: por ejemplo, podría haber restricciones de uso específicas de un vehículo que deberá cumplir la empresa ferroviaria que explota dichos vehículos;

(h) Fabricante – Fabricante: por ejemplo, la gestión de interfaces técnicas relacionadas con la seguridad entre subsistemas de dos fabricantes diferentes;

(i) Fabricante – Proveedor de servicios: por ejemplo, la gestión del registro de peligros por el fabricante cuando subcontrate algunos trabajos a una empresa cuyo tamaño es demasiado pequeño para disponer de una organización de seguridad en el proyecto de que se trate;

(j) Proveedor de servicios – Proveedor de servicios: ejemplo similar al expuesto en el punto (i) anterior ;

C.3.2. Los proveedores de servicios cubren todas las actividades subcontratadas por el administrador de la infraestructura, la empresa ferroviaria o el fabricante, como el mantenimiento, la venta de billetes, los servicios de ingeniería, etc.

C.3.3. En el siguiente ejemplo se ilustra el proceso de gestión de la interfaz e determinación del peligro asociado. Se tiene en cuenta una interfaz entre un fabricante de trenes y un proponente (empresa ferroviaria). A continuación, se describe cómo podrían cumplirse los principales criterios señalados en el apartado [G 3] de la sección 1.2.1:

(a) Liderazgo: el proponente (empresa ferroviaria);

(b) Datos:

(1) lista(s) de peligros pertinentes derivados de proyectos similares;
(2) descripción de todos los datos de entrada y salida relacionados con la interfaz, incluidas las características de prestación;

(c) Métodos: véase el Apéndice A.2 de la Directriz EN 50 126-2 {Ref. 9};

(d) Participantes requeridos:

(1) responsable de garantía de la seguridad del proponente (empresa ferroviaria);
(2) responsable de garantía de la seguridad del fabricante del tren;
(3) autoridad de diseño del proponente del tren;
(4) autoridad de diseño del fabricante del tren;
(5) personal de mantenimiento del proponente del tren (en parte, en función de los datos de entrada y salida analizados);
(6) maquinistas (en parte, en función de los datos de entrada y salida analizados);

(e) Resultados:

(1) informe de determinación del peligro de común acuerdo;
(2) medidas de seguridad que se consignarán en el registro de peligros con una clara descripción de la responsabilidad.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

C.4. Ejemplos de métodos para determinar riesgos ampliamente aceptables

C.4.1. Introducción

C.4.1.1. En el Reglamento MCS, los riesgos ampliamente aceptables se definen como riesgos que son *"tan pequeños que no resulta razonable aplicar medida de seguridad adicional alguna (para seguir reduciendo el riesgo)"*. En la determinación del peligro, el hecho de clasificar algunos peligros como asociados con riesgos ampliamente aceptables permite omitir el análisis ulterior de dichos peligros en el proceso de evaluación del riesgo. La definición de riesgos ampliamente aceptables antes citada ofrece cierto margen de interpretación, de ahí que en el Reglamento se establezca que la decisión de clasificar los peligros con riesgos ampliamente aceptables corresponde a la opinión de expertos.

C.4.1.2. En efecto, por lo general es difícil definir un criterio más explícito para riesgos ampliamente aceptables que se aplique a los diferentes niveles posibles del sistema en los que podrían identificarse tales peligros, y que también represente los diferentes factores de aversión al riesgo que podrían prevalecer para diferentes aplicaciones. Ahora bien, ante la importancia de garantizar que las opiniones de expertos sean fáciles de comprender y controlar, resulta útil ofrecer algunas orientaciones sobre la manera de definir riesgos como ampliamente aceptables. Los criterios para definir riesgos ampliamente aceptables pueden ser cuantitativos, cualitativos o semicualitativos. A continuación figuran algunos ejemplos sobre cómo establecer criterios que permitan realizar una evaluación cuantitativa o semicuantitativa de riesgos ampliamente aceptables.

C.4.1.3. Los ejemplos que se exponen más abajo ilustran ese principio. Dichos ejemplos se han extraído del documento titulado: *"Die Gefaehrdungseinstufung im ERA-Risikomanagementprozess", Kurz, Milius, Signal +Draht (100) 9/2008.*

C.4.2. Establecimiento del criterio cuantitativo

C.4.2.1. Los riesgos ampliamente aceptables podrían definirse como riesgos mucho más pequeños que el riesgo aceptable que representa una clase de peligros establecida. Mediante el uso de datos estadísticos podría calcularse el nivel actual de riesgo que presentan los sistemas ferroviarios y, por lo tanto, declararse como aceptable ese nivel calculado. Al dividir ese nivel de riesgo por el número (N) de peligros (por ejemplo, de forma arbitraria, se puede suponer que existen alrededor de N = 100 principales categorías de peligros en el sistema ferroviario), se obtiene un nivel aceptable de riesgo por cada categoría de peligro. A continuación, puede afirmarse que un peligro con un riesgo inferior en dos órdenes de magnitud al nivel aceptable de riesgo por peligro (éste es el parámetro x % mencionado en el apartado [G 1] de la sección 2.2.3) se consideraría como un riesgo ampliamente aceptable.

C.4.2.2. No obstante, se comprobará que la contribución de todos los peligros asociados con riesgos ampliamente aceptables supera un porcentaje establecido (por ejemplo, y%) del riesgo general en el nivel del sistema. véase la sección 2.2.3 y la explicación dada en el apartado [G 2] de la sección 2.2.3.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

C.4.3. Evaluación de riesgos ampliamente aceptables

C.4.3.1. A continuación, pueden utilizarse los valores límite para riesgos ampliamente aceptables, obtenidos a partir de los ejemplos anteriores, para calibrar herramientas cualitativas, como una matriz de riesgo, un gráfico de riesgo o números de prioridad de riesgo, a fin de ayudar al experto a tomar su decisión para clasificar el riesgo como ampliamente aceptable. Es importante señalar que el hecho de disponer de valores cuantitativos como criterios para determinar riesgos ampliamente aceptables no implica que sea necesario realizar una estimación o un análisis meticuloso del riesgo para decidir sobre la amplia aceptabilidad del riesgo. Aquí es donde se solicita la opinión de expertos para realizar esta estimación aproximada en la fase de determinación del riesgo.

C.4.3.2. Asimismo, es importante comprobar que la contribución de todos los peligros asociados con riesgos ampliamente aceptables supera un porcentaje establecido (por ejemplo, y%) del riesgo general en el nivel del sistema. véase la sección 2.2.3 y la explicación dada en el apartado [G 2] de la sección 2.2.3.

C.5. Ejemplo de evaluación del riesgo de un cambio organizativo significativo

C.5.1. **Observación:** este ejemplo de evaluación del riesgo no es el resultado de la aplicación del proceso MCS, sino que se expuso antes de que existiera el MCS. El objetivo de este ejemplo es:

(a) identificar las similitudes entre los métodos de evaluación del riesgo existentes y el proceso MCS;

(b) mostrar la trazabilidad entre el proceso existente y el establecido por el MCS;

(c) justificar el valor añadido que supone realizar los pasos adicionales (si hubiera) establecidos por el MCS.

Cabe subrayar que este ejemplo sólo se ofrece a título informativo. Su objetivo es ayudar al lector a comprender el proceso MCS. Sin embargo, dicho ejemplo no se incorporará a un sistema de referencia ni se usará como tal para otro cambio significativo. La evaluación del riesgo se llevará a cabo para cada cambio significativo, de conformidad con el Reglamento MCS.

C.5.2. El ejemplo se refiere a un cambio organizativo. El proponente pertinente lo consideró significativo. Se aplicó un enfoque basado en la evaluación del riesgo para evaluar el cambio.

C.5.3. Una división de la organización del administrador de la infraestructura, que realizaba algunas actividades de mantenimiento (distintas de las de señalización o telemáticas)hasta que se produjo el cambio, tuvo que entrar en competencia con otras empresas que trabajaban en el mismo ámbito. La repercusión directa fue la necesidad de recortar y redistribuir el personal y las funciones dentro de la división separada de la organización del administrador de la infraestructura que entró en competencia.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

C.5.4. Consideraciones del administrador de la infraestructura afectado:

(a) el personal del administrador de la infraestructura afectado por el cambio se encargaba del mantenimiento y de las reparaciones de emergencia por fallos imprevistos en la infraestructura. El personal también realizaba algunas actividades de mantenimiento planificadas o basadas en el proyecto, tales como el calzado de la vía, la limpieza de balasto o el control de la vegetación;

(b) estas tareas se consideraron cruciales para la seguridad y puntualidad de la operación. Por lo tanto, tenían que analizarse para encontrar las medidas adecuadas que permitieran garantizar que la situación no se deteriorara, pues son muchas las personas encargadas de cuestiones de seguridad que abandonan la organización del administrador de la infraestructura.

(c) es necesario mantener el mismo nivel de seguridad y puntualidad del tren durante el cambio de la organización y después del mismo.

C.5.5. En comparación con el proceso MCS, se realizaron los siguientes pasos (véase, asimismo, la Figura 1):

(a) descripción del sistema [sección 2.1.2]:

(1) descripción de las tareas desempeñadas por la organización existente (es decir, por la organización del administrador de la infraestructura antes del cambio);

(2) descripción de los cambios planificados en la organización del administrador de la infraestructura;

(3) las interfaces de la “división destinada a escindirse” con otras organizaciones próximas o con el entorno físico tan sólo podrían describirse sucintamente. Los límites no podrían presentarse con claridad absoluta;

(b) determinación de los peligros [sección 2.2]:

(1) “Tormenta de ideas” por parte de un grupo de expertos:

(i) para encontrar todos los peligros con una importante influencia en el riesgo que supone el cambio organizativo previsto;

(ii) para identificar posibles acciones dirigidas a controlar el riesgo;

(2) clasificación del peligro:

(i) en función de la gravedad del riesgo asociado: riesgo alto, medio o bajo;

(ii) en función de la repercusión del cambio: riesgo aumentado, no modificado, reducido;

(c) uso de un sistema de referencia [sección 2.4]:

Se consideró que el sistema antes del cambio presentaba un nivel aceptable de seguridad. Por lo tanto, se usó como “sistema de referencia” para establecer los criterios de aceptación del riesgo respecto al cambio de organización;

(d) estimación explícita y valoración del riesgo [sección 2.5]:

Para cada peligro que presenta un riesgo aumentado debido al cambio de organización se identifican medidas de reducción del riesgo. El riesgo residual se coteja con los criterios de aceptación del riesgo del sistema de referencia para comprobar si es necesario identificar medidas adicionales;

(e) demostración del cumplimiento de los requisitos de seguridad [sección 3]:

(1) el análisis de riesgos y el registro de peligros muestran que los peligros no pueden controlarse hasta que se verifiquen y hasta que se demuestre que se han aplicado los requisitos de seguridad (es decir, las medidas de seguridad seleccionadas);

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(2) el análisis de riesgos y el registro de peligros eran documentos vivos. La eficacia de las intervenciones acordadas se controló a intervalos regulares para comprobar si se habían alterado las condiciones y si es necesario actualizar el análisis y la valoración del riesgo;
(3) si las medidas aplicadas no eran lo suficientemente eficientes, el análisis de riesgos, la valoración del riesgo y el registro de peligros volvían a ser objeto de actualización y control;

(f) gestión de los peligros [sección 4.1]:

Los peligros identificados y las medidas de seguridad se registraron y gestionaron en un registro de peligros. Una de las conclusiones de este ejemplo era actualizar continuamente el análisis de riesgos y el registro de peligros en la medida en que se adoptaran decisiones y realizaran intervenciones durante el cambio de la organización. El riesgo en las interfaces con, por ejemplo, subcontratistas y empresarios, también quedaba cubierto por el análisis de riesgos.

En la sección C.16.2. del Apéndice C figuran la estructura y los campos utilizados para el registro de peligros, así como un extracto de algunas líneas.

(g) evaluación independiente [Artículo 6]:

Asimismo, se llevó a cabo una evaluación independiente a cargo de terceros para:

(1) comprobar que la gestión del riesgo y la evaluación del riesgo se realizaron correctamente;
(2) comprobar que el cambio organizativo es adecuado y permitirá mantener el mismo nivel de seguridad existente antes del cambio.

C.5.6. El ejemplo muestra que los principios establecidos por el método común de seguridad son métodos existentes en el sector ferroviario que ya se aplican para evaluar los riesgos que plantean los cambios organizativos. La evaluación del riesgo presentada en el ejemplo cumple todos los requisitos del MCS. Ésta utiliza dos de los tres principios de aceptación del riesgo permitidos por el enfoque armonizado del MCS:

(a) se aplica un “sistema de referencia” con el objeto de establecer los criterios de aceptación del riesgo necesarios para evaluar la aceptación del riesgo del cambio organización;

(b) “estimación explícita y valoración del riesgo”

(1) para analizar las desviaciones del cambio con respecto al sistema de referencia;
(2) para identificar medidas de reducción del riesgo en lo que atañe al riesgo aumentado derivado del cambio;
(3) para evaluar si se alcanza un nivel aceptable de riesgo.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

C.6. Ejemplo de evaluación del riesgo de un cambio operativo significativo – Cambio de horas de conducción

C.6.1. **Observación:** este ejemplo de evaluación del riesgo no es el resultado de la aplicación del proceso MCS, sino que se expuso antes de que existiera el MCS. El objetivo de este ejemplo es:

(a) identificar las similitudes entre los métodos de evaluación del riesgo existentes y el proceso MCS;
(b) mostrar la trazabilidad entre el proceso existente y el establecido por el MCS;
(c) justificar el valor añadido que supone realizar los pasos adicionales (si hubiera) establecidos por el MCS.

Cabe subrayar que este ejemplo sólo se ofrece a título informativo. Su objetivo es ayudar al lector a comprender el proceso MCS. Sin embargo, dicho ejemplo no se incorporará a un sistema de referencia ni se usará como tal para otro cambio significativo. La evaluación del riesgo se llevará a cabo para cada cambio significativo, de conformidad con el Reglamento MCS.

C.6.2. Este ejemplo ilustra un cambio operativo en el que la empresa ferroviaria quería asignar nuevas rutas y posiblemente nuevas horas de trabajo (que incluían rotaciones y un sistema de turnos) a los maquinistas.

C.6.3. En comparación con el proceso MCS, se realizaron los siguientes pasos (véase, asimismo, la Figura 1):

(a) importancia del cambio [Artículo 4]:

La empresa ferroviaria realizó una evaluación preliminar del riesgo que concluyó que el cambio operativo era significativo. Como los maquinistas tenían que circular por nuevas rutas, y posiblemente fuera de sus horas de trabajo habituales, no se podía desdeñar la posibilidad de que el tren pasase por señales de peligro, excediese la velocidad o ignorase las limitaciones temporales de velocidad.

Al comparar esta evaluación preliminar del riesgo con los criterios especificados en el Artículo 1.Artículo 4 (2) del Reglamento MCS, el cambio también podía clasificarse como significativo sobre la base de los siguientes criterios:

(1) importancia para la seguridad: el cambio está relacionado con la seguridad en la medida en que el hecho de modificar la forma de trabajar de los maquinistas podría tener una consecuencia catastrófica;
(2) consecuencia de fallo: los errores de los maquinistas anteriormente referidos podrían tener consecuencias catastróficas;
(3) novedad: la empresa ferroviaria podría estar introduciendo nuevas maneras de trabajar para los maquinistas;
(4) complejidad del cambio: podría resultar complejo modificar las horas de conducción, ya que ello podría requerir una evaluación completa y una modificación de las condiciones de trabajo existentes;

(b) definición del sistema [sección 2.1.2]:

Inicialmente, la definición del sistema describía:

(1) las condiciones de trabajo existentes: horas de trabajo, sistema turnos, etc.;
(2) los cambios de las horas de trabajo;
(3) los aspectos relacionados con la interfaz (por ejemplo, con el administrador de la infraestructura)

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

Durante las diferentes iteraciones, la definición del sistema se actualizó con los requisitos de seguridad resultantes del proceso de evaluación del riesgo. Los principales representantes del personal participaron en este proceso iterativo de determinación de los peligros y actualización de la definición del sistema.

(c) determinación de los peligros [sección 2.2]:

Se identificaron los peligros y las posibles medidas de seguridad para las nuevas rutas y el sistema de turnos mediante un ejercicio de reflexión a cargo de un grupo de expertos, que incluía a representantes de maquinistas. Se examinaron las tareas de los maquinistas con arreglo a las nuevas condiciones, a fin de evaluar si afectaban a los maquinistas, su carga de trabajo, el alcance geográfico y el sistema de turnos de trabajo.
La empresa ferroviaria también consultó a los sindicatos para ver si podían facilitar más información y examinó el riesgo de niveles de fatiga y enfermedad que podría inducir un posible incremento de horas extraordinarias debido a recorridos ampliados en rutas desconocidas.
Se asignó un nivel de gravedad del riesgo (alto, medio o bajo) y de las consecuencias a cada uno de los peligros, y se revisó la repercusión del cambio propuesto a la luz de los mismos (riesgo aumentado, no modificado, reducido).

(d) uso de códigos prácticos [sección 2.3]:

Se usaron códigos prácticos relacionados con las horas de trabajo y los riesgos de fatiga de los operadores humanos para revisar las condiciones de trabajo existentes y determinar los nuevos requisitos de seguridad. Las normas operativas necesarias se redactaron con arreglo a los códigos prácticos para el nuevo sistema de turnos de trabajo. Todas los agentes involucrados participaron en los procedimientos operativos revisados y en el acuerdo para llevar a cabo el cambio.

(e) demostración de que el sistema cumple los requisitos de seguridad [sección 3]:

Los procedimientos operativos revisados se introdujeron en el sistema de gestión de la seguridad de la empresa ferroviaria. Se sometieron a un control y se estableció un proceso de revisión para garantizar que los peligros identificados continuaran siendo objeto de controles adecuados durante la explotación del sistema ferroviario.

(f) gestión de los peligros [sección 4.1]:

Véase el apartado anterior, ya que, por lo que respecta a las empresas ferroviarias, el proceso de gestión del peligro puede formar parte de su sistema de gestión de la seguridad respecto a los riesgos de registro y gestión. Los peligros identificados se incluyeron en un registro de peligros con los requisitos de seguridad (es decir, haciendo referencia a los procedimientos operativos revisados) que permiten controlar el riesgo asociado.
Los procedimientos revisados se sometieron a un control, y se revisaron en la medida de lo necesario, para garantizar que los peligros identificados continuaran siendo objeto de controles adecuados durante la explotación del sistema ferroviario.

(g) evaluación independiente [Artículo 6]:

Una persona competente de la empresa ferroviaria e independiente del proceso de evaluación evaluó los procesos de gestión del riesgo y evaluación del riesgo. Esta persona competente evaluó tanto los procesos como los resultados, es decir, los requisitos de seguridad identificados.

La empresa ferroviaria ha basado su decisión de poner en marcha el nuevo sistema en el informe de evaluación independiente elaborado por la persona competente.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

C.6.4. El ejemplo muestra que los principios y procesos utilizados por la empresa ferroviaria son conformes con el método de seguridad común. Los procesos de gestión del riesgo y evaluación del riesgo cumplían todos los requisitos del MCS.

C.7. Ejemplo de evaluación del riesgo de un cambio técnico significativo (control, mando y señalización, MCS)

C.7.1. **Observación:** este ejemplo de evaluación del riesgo no es el resultado de la aplicación del proceso MCS, sino que se expuso antes de que existiera el MCS. El objetivo de este ejemplo es:

(a) identificar las similitudes entre los métodos de evaluación del riesgo existentes y el proceso MCS;
(b) mostrar la trazabilidad entre el proceso existente y el establecido por el MCS;
(c) justificar el valor añadido que supone realizar los pasos adicionales (si hubiera) establecidos por el MCS.

Cabe subrayar que este ejemplo sólo se ofrece a título informativo. Su objetivo es ayudar al lector a comprender el proceso MCS. Sin embargo, dicho ejemplo no se incorporará a un sistema de referencia ni se usará como tal para otro cambio significativo. La evaluación del riesgo se llevará a cabo para cada cambio significativo, de conformidad con el Reglamento MCS.

C.7.2. Este ejemplo se refiere a un cambio técnico significativo del sistema de control y mando. El fabricante pertinente lo consideró significativo. Se aplicó un enfoque basado en la evaluación del riesgo para evaluar el cambio.

C.7.3. Descripción del cambio: el cambio consiste en sustituir un lazo en tierra situado antes de una señal por un subsistema de “información adicional por radio + GSM” (véase la Figura 16).

C.7.4. Consideración: mantener el nivel de seguridad del sistema después del cambio.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

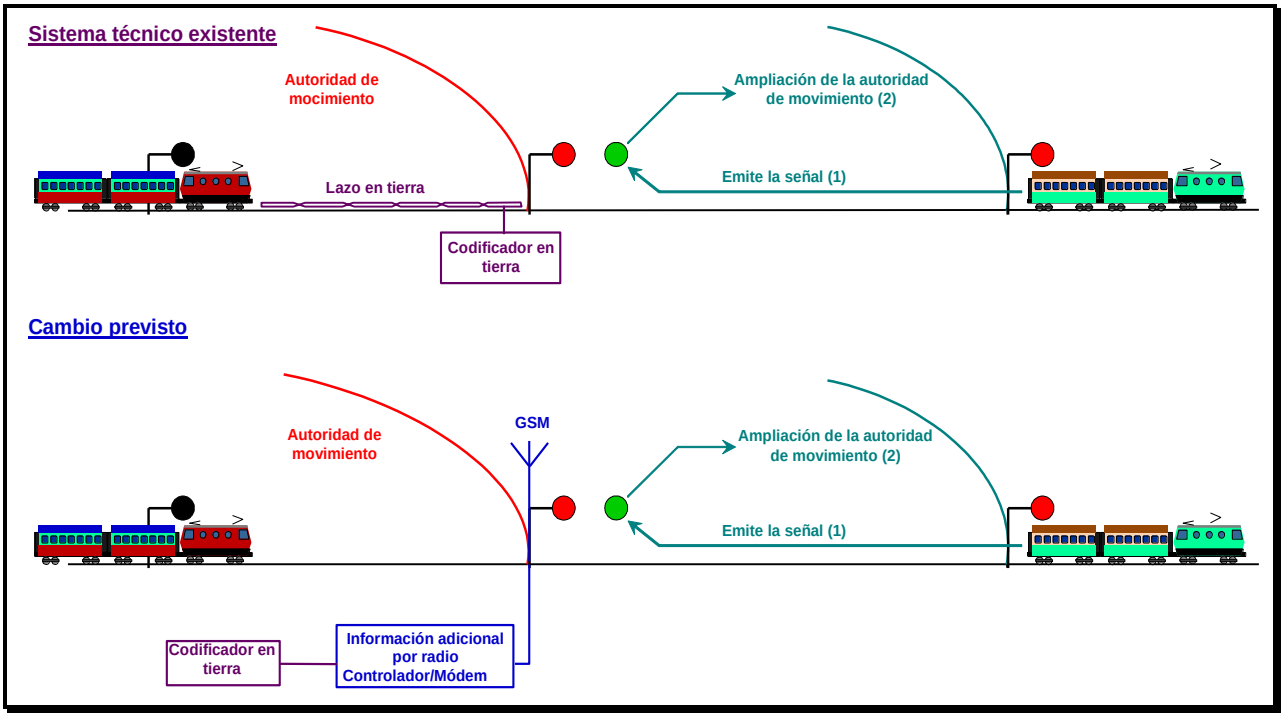


Figura 16: Cambio de un bucle en tierra por un subsistema de información adicional por radio.

C.7.5. En comparación con el proceso MCS, se realizaron los siguientes pasos (véase, asimismo, la Figura 1):

(a) evaluación de la importancia del cambio [Artículo 4]

Los criterios especificados en el Artículo 1.Artículo 4 (2) se utilizan para evaluar la importancia de un cambio. Principalmente se utilizaron la complejidad y la novedad para decidir que el cambio es significativo.

(b) descripción del sistema [sección 2.1.2]:

(1) descripción del sistema existente: lazo y sus funciones en el sistema de mando y control;
(2) descripción del cambio propuesto por el proponente y el fabricante;
(3) descripción de las interfaces funcionales y físicas del bucle con el resto del sistema;

La función del “lazo+codificador” en el sistema existente consiste en emitir la señal al aproximarse un tren cuando el tramo situado bajo la señal (es decir, frente al tren que se aproxima) quede desocupado: véase la Figura 16.

(c) determinación de los peligros [sección 2.2]:

Se aplica el proceso iterativo de evaluación del riesgo y la determinación del riesgo (véase la sección 2.1.1), sobre la base de una “tormenta de ideas” a cargo de un grupo de expertos para:

(1) determinar todos los peligros con una influencia importante en el riesgo que supone el cambio previsto;
(2) identificar posibles acciones dirigidas a controlar el riesgo;

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

Como el lazo, y, por ende, la información adicional con radio, emite la señal, existe un riesgo de otorgar una autoridad de movimiento inseguro al tren que se aproxima, mientras el tren que precede siga ocupando el tramo situado frente a la señal. El riesgo deberá controlarse a un nivel aceptable.

(d) uso de un sistema de referencia [sección 2.4]:

Se considera que el sistema antes del cambio (bucle) presenta un nivel aceptable de seguridad. Por lo tanto, se utiliza como "sistema de referencia" para establecer los requisitos de seguridad aplicables al subsistema de información adicional con radio.

(e) estimación y evaluación del riesgo explícito [sección 2.5]:

(1) las diferencias entre los subsistemas de "lazo" y de "información adicional con radio+GSM" se analizan mediante una estimación explícita y valoración del riesgo. En relación con el subsistema de "información adicional por radio+GSM", se determinan los siguientes peligros:

(i) transmisión de información insegura por parte de piratas informáticos en la interfaz por aire, dado que el subsistema de "información adicional con radio+GSM" es un subsistema de transmisión abierto;
(ii) transmisión con retraso o transmisión de paquetes de datos memorizados en la interfaz por aire;

(2) estimación explícita del riesgo y uso del criterio de aceptación del riesgo para sistemas técnicos para la parte del controlador de información adicional con radio;

(f) uso de códigos prácticos [sección]:

(1) la norma EN 50159-2 (*"Railway Applications: Part 2: Safety related communication in open transmission systems"* [Aplicaciones ferroviarias – Sistemas de comunicación, de señalización y de procesado. Parte 2: Comunicación de seguridad en los sistemas de transmisión abiertos]) establece los requisitos de seguridad para controlar los nuevos peligros a un nivel aceptable, por ejemplo:

(i) codificación y protección de datos;
(ii) secuenciación de mensajes y consignación de fecha y hora;

(2) uso, por ejemplo, de la norma EN 50 128 para el desarrollo del programa informático del controlador de información adicional con radio;

(g) demostración del cumplimiento de los requisitos de seguridad [sección 3]:

(1) seguimiento de la aplicación de los requisitos de seguridad a través del proceso de desarrollo del subsistema de "información adicional con radio+GSM";
(2) verificación de que el sistema, tal como se ha diseñado e instalado, cumple los requisitos de seguridad;

(h) gestión de los peligros [sección 4.1]:

Los peligros identificados, las medidas de seguridad y los requisitos de seguridad resultantes derivados de la evaluación del riesgo y la aplicación de los tres principios de aceptación del riesgo se consignan y gestionan en un registro de peligros.

(i) evaluación independiente [Artículo 6]:

Asimismo, se lleva a cabo una evaluación independiente a cargo de terceros para:

(1) comprobar que la gestión del riesgo y la evaluación del riesgo se realizan correctamente;

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(2) comprobar que el cambio técnico es adecuado y permitirá mantener el mismo nivel de seguridad existente antes del cambio.

C.7.6. El ejemplo muestra que los tres principios de aceptación del riesgo establecidos por el método común de seguridad se usan como complemento para definir los requisitos de seguridad del sistema objeto de evaluación. La evaluación del riesgo presentada en el ejemplo cumple todos los requisitos del MCS que se resumen en la Figura 1, incluidos los relativos a la gestión del registro de peligros y la evaluación independiente de la seguridad por terceros.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

C.8. Ejemplo de la directriz sueca BVH 585.30 para la evaluación del riesgo de túneles ferroviarios

C.8.1. **Observación:** este ejemplo de evaluación del riesgo no es el resultado de la aplicación del proceso MCS, sino que se expuso antes de que existiera el MCS. El objetivo de este ejemplo es:

(a) identificar las similitudes entre los métodos de evaluación del riesgo existentes y el proceso MCS;
(b) mostrar la trazabilidad entre el proceso existente y el establecido por el MCS;
(c) justificar el valor añadido que supone realizar los pasos adicionales (si hubiera) establecidos por el MCS.

Cabe subrayar que este ejemplo sólo se ofrece a título informativo. Su objetivo es ayudar al lector a comprender el proceso MCS. Sin embargo, dicho ejemplo no se incorporará a un sistema de referencia ni se usará como tal para otro cambio significativo. La evaluación del riesgo se llevará a cabo para cada cambio significativo, de conformidad con el Reglamento MCS.

C.8.2. El objetivo de este ejemplo es comparar el proceso previsto en el MCS con la directriz BVH 585.30 utilizada por el administrador de la infraestructura sueco Banverket, para diseñar y verificar la consecución de un nivel de seguridad suficiente en la planificación y construcción de nuevos túneles ferroviarios. A continuación se enumeran los puntos comunes y las diferencias que existen entre la directriz y el MCS; los requisitos detallados de evaluación de la seguridad figuran en la directriz BVH 585.30.

C.8.3. En comparación con el proceso descrito en la Figura 1:

(a) la directriz BVH 585.30 presenta los siguientes puntos comunes:

(1) descripción del sistema [sección 2.1.2]:

La directriz exige una descripción detallada del sistema que incluya:

(i) una descripción del túnel;
(ii) una descripción de la vía;
(iii) una descripción del tipo de material rodante (incluido el personal de a bordo);
(iv) una descripción del tráfico y de las operaciones previstas;
(v) una descripción de la asistencia externa (incluidos los servicios de salvamento);

(2) determinación de los peligros [sección 2.2]:

La directriz no exige explícitamente una determinación de los peligros. Exige una determinación del riesgo y un “catálogo de accidentes” que incluya los tipos de accidentes potenciales identificados que se considere tengan un impacto significativo en el nivel de riesgo del túnel y que deberán quedar cubiertos por la evaluación posterior. Ejemplos de accidentes:

(i) “descarrilamiento de un tren de viajeros”;
(ii) “descarrilamiento de un tren de mercancías”;
(iii) “accidente que afecte a mercancías peligrosas”;
(iv) “incendio en un vehículo”;
(v) “colisión entre un tren de viajeros y un objeto ligero/pesado”;
(vi) etc.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(3) no contempla disposiciones sobre la aplicación de códigos prácticos o sistemas de referencia similares. Se considera que el análisis de riesgos debería llevarse a cabo en todos los casos;

(4) estimación explícita y valoración del riesgo [sección 2.5]:

(i) en general, la directriz recomienda que para cada tipo de accidente se realice un análisis secuencial de averías completo, basado en el análisis cuantitativo del riesgo. No obstante, como el análisis de riesgos se propone analizar el nivel global de la seguridad del túnel, en lugar de analizar la seguridad de forma individual en niveles más detallados, las consecuencias de todos los supuestos se suman para obtener el nivel global de riesgo que presenta el túnel;

(ii) la aceptabilidad de este nivel global de riesgo que presenta el túnel se comparará con el siguiente criterio de aceptación del riesgo cuantitativo. *"el tráfico ferroviario por kilómetro en túneles deberá presentar el mismo nivel de seguridad que el tráfico ferroviario por kilómetro en vías al aire libre, con exclusión de los pasos a nivel"*. Este criterio se convierte en una curva F-N sobre la base de datos históricos de accidentes ferroviarios en Suecia y se extrapola para cubrir, asimismo, las consecuencias que no figuran en las estadísticas;

(iii) además de este criterio para el nivel global de riesgo del túnel, también existen otros requisitos que deben cumplirse específicamente para la evacuación en túneles, así como posibilidades para los servicios de salvamento:

(a) verificar que es posible el auto-rescate en el caso de un incendio en un tren para "el peor de los casos previsible" (también se ofrecen los criterios para esta evaluación);

(b) el túnel debería estar diseñado para permitir que se realicen operaciones de salvamento para una serie de supuestos específicos;

(5) resultado de la evaluación del riesgo [sección 2.1.6]:

Los resultados de la evaluación del riesgo son:

(i) una lista de medidas de seguridad de la norma mínima basadas en la ETI sobre seguridad de túneles ferroviarios y normas nacionales que se aplicarán a la hora de diseñar el túnel, y;

(ii) todas las medidas de seguridad adicionales que el análisis de riesgo considere necesarias, indicando el propósito de las mismas. Se afirma que las medidas deberían decidirse con arreglo al siguiente orden de prioridad:

(a) previenen los accidentes;
(b) reducen las consecuencias de los accidentes;
(c) facilitan la evacuación;
(d) facilitan las operaciones de salvamento;

(6) gestión del peligro [sección 4.1]:

La directriz no exige explícitamente que se lleve un registro de peligros. Ello guarda relación con el hecho de que la evaluación se realiza a nivel global y, por lo tanto, los peligros no se evalúan ni controlan de forma individual. La aceptabilidad del riesgo global del túnel se evalúa sin que se distribuya el criterio de aceptación del riesgo global hasta los diferentes tipos de accidentes o peligros subyacentes.

No obstante, existe una lista de todas las medidas de seguridad, tanto las resultantes de la "norma mínima" como las que el análisis de riesgos considera necesarias: véase el apartado (1)(i) más arriba. En la lista de medidas de seguridad debe indicarse si éstas atañen a la infraestructura del túnel, la vía, las

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

operaciones o el material rodante, así como el efecto que se espera de las mismas de conformidad con la lista numerada que figura en el apartado (1)(i). Ahora bien, la directriz no exige que se indique explícitamente qué peligros controlan las medidas de seguridad ni quién es responsable de cada medida.

(7) evaluación independiente [Artículo 6]:

La evaluación independiente a cargo de terceros es obligatoria para:

(i) comprobar que el proceso de evaluación del riesgo recomendado por la directriz BVH 585.30 se ha realizado correctamente;
(ii) considerar aceptable el análisis de riesgos;
(iii) comprobar que se ha indicado con claridad cómo debería realizarse la futura gestión del riesgo en el proyecto;

El documento final de análisis de riesgos lo firman el evaluador independiente y el coordinador de la seguridad del proyecto.

(b) la directriz BVH 585.30 difiere del MCS en los aspectos siguientes:

(1) demostración del cumplimiento de los requisitos de seguridad [sección 3]:

La directriz BVH 585.30 no exige que se realice un seguimiento de la aplicación de los requisitos de seguridad identificados ni que se verifique que el proyecto final del túnel cumple los requisitos de seguridad establecidos. Tan sólo describe cómo deberían transferirse estos requisitos para garantizar que se apliquen en la fase de construcción.

La directriz establece los requisitos de seguridad que deben aplicarse para verificar que el análisis de riesgos se ha realizado de forma adecuada y transparente, y que el proyecto puede aceptarlos.

C.8.4. En conclusión, la comparación con el MCS demuestra que:

(a) la directriz BVH 585.30 cumple las partes pertinentes del MCS, aunque su ámbito de aplicación y objetivo no son exactamente los mismos;

(b) la directriz BVH 585.30 evalúa el nivel global de riesgo del túnel ferroviario;

(c) los peligros no se controlan de forma individual y, por ende, se presta menos atención a la gestión del peligro;

(d) la demostración del cumplimiento y la verificación de la correcta aplicación de todas las medidas de seguridad no se establece de manera tan explícita. No obstante, la directriz establece que la función del coordinador de la seguridad en el marco del proyecto (una función y competencia que exige la directriz BVH 585.30) es verificar que las conclusiones del análisis de riesgos se aplican en los documentos y planos del diseño, así como controlar que se aplican correctamente en la fase de construcción;

C.8.5. Los MCS son más generales que la directriz BVH 585.30 en la medida en que contemplan la aplicación de tres principios de aceptación del riesgo diferentes. No obstante, la aplicación de la directriz BVH 585.30 en el marco del MCS no plantea problema alguno, ya que es compatible con el uso del tercer principio de estimación explícita del riesgo.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

C.9. Ejemplo de evaluación del riesgo en el nivel del sistema para el metro de Copenhague

C.9.1. **Observación:** este ejemplo de evaluación del riesgo no es el resultado de la aplicación del proceso MCS, sino que se expuso antes de que existiera el MCS. El objetivo de este ejemplo es:

(a) identificar las similitudes entre los métodos de evaluación del riesgo existentes y el proceso MCS;

(b) mostrar la trazabilidad entre el proceso existente y el establecido por el MCS;

(c) justificar el valor añadido que supone realizar los pasos adicionales (si hubiera) establecidos por el MCS.

Cabe subrayar que este ejemplo sólo se ofrece a título informativo. Su objetivo es ayudar al lector a comprender el proceso MCS. Sin embargo, dicho ejemplo no se incorporará a un sistema de referencia ni se usará como tal para otro cambio significativo. La evaluación del riesgo se llevará a cabo para cada cambio significativo, de conformidad con el Reglamento MCS.

C.9.2. Este ejemplo se refiere a un sistema completo y complejo de metro sin maquinista, incluidos los subsistemas técnicos subyacentes (por ejemplo, protección automática del tren y material rodante), así como la explotación y el mantenimiento del sistema. Se aplicó un enfoque basado en la evaluación del riesgo para evaluar el sistema y los subsistemas subyacentes. Asimismo, el proyecto cubrió la certificación del sistema de gestión de la seguridad de la empresa que tenía que explotar el sistema. Ésta se refiere a la capacidad de la empresa ferroviaria y el administrador de la infraestructura para explotar y mantener el sistema global a lo largo del ciclo vital del sistema.

C.9.3. En comparación con el proceso MCS, se realizaron los siguientes pasos (véase, asimismo, la Figura 1):

(a) descripción del sistema [sección 2.1.2]:

(1) descripción de los requisitos de rendimiento del sistema;
(2) descripción de las normas operativas;
(3) clara descripción de las interfaces y responsabilidades entre los diferentes agentes, en particular entre los subsistemas técnicos;
(4) definición de requisitos de alto nivel del sistema (en términos de frecuencia aceptable de accidentes y definición de una región ALARP);

(b) determinación de los peligros [sección 2.2]:

(1) un análisis preliminar del peligro a nivel del sistema;
(2) un análisis funcional a nivel del sistema que destaque todos los subsistemas, y no sólo aquellos que revisten de manera obvia una importancia crítica para la seguridad (por ejemplo, protección automática del tren y material rodante), que intervengan en funciones de seguridad y tengan un papel activo a la hora de garantizar la seguridad de los viajeros y el personal;

(3) intensa coordinación entre los agentes (contratistas, proveedores del subsistema de los subsistemas técnicos y de las obras de ingeniería civil):

(i) para determinar de manera sistemática todos los peligros razonablemente previsibles;
(ii) para identificar posibles acciones dirigidas a controlar todos los riesgos asociados a los peligros identificados a un nivel aceptable;

(c) uso de códigos prácticos [sección 2.3]:

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

Se usaron diferentes códigos prácticos, normas y reglamentos, por ejemplo

(1) el reglamento BOStrab sobre la construcción y explotación de tranvías (reglamento alemán aplicable a sistemas ferroviarios urbanos) y sobre la explotación sin maquinista;
(2) documentos VDV (códigos prácticos alemanes) relacionados con los requisitos aplicables a equipos para garantizar la seguridad de los viajeros en las estaciones en los casos de explotación sin maquinista;
(3) normas CENELEC para sistemas ferroviarios (EN 50 126, 50 128 y 50 129). Estas normas se ocupan de los sistemas técnicos ferroviarios en particular. No obstante, como incluyen un enfoque metodológico de validez general, se han adoptado de manera generalizada para el metro de Copenhague:

(i) la norma EN 50 126 se usó para las actividades de gestión de la seguridad y evaluación del riesgo del sistema ferroviario completo;
(ii) la norma EN 50 129 se usó para el sistema completo de señalización;
(iii) la norma EN 50 128 se usó para el desarrollo de programas informáticos (incluidas su verificación y validación) de los subsistemas técnicos;

(4) normas de protección contra incendios para túneles (NEPA 130);
(5) normas para la ingeniería civil y las obras de ingeniería civil (Eurocódigos);

(d) uso de un sistema de referencia [sección 2.4]:

El metro tenía que alcanzar el nivel de seguridad de las correspondientes modernas instalaciones de Alemania, Francia o Gran Bretaña. Estos sistemas existentes se usaron como sistemas de referencia similares para establecer los criterios de aceptación del riesgo en términos de frecuencia aceptable de accidentes para el metro de Copenhague;

(e) estimación explícita y valoración del riesgo [sección 2.5]:

(1) para realizar una estimación de los riesgos relacionados con peligros específicos;
(2) para controlar la ventilación de emergencia del túnel (incluidos los factores humanos del cuerpo de bomberos);
(3) para identificar medidas de reducción del riesgo;
(4) para evaluar si se alcanza un nivel aceptable de riesgo para el sistema completo;

(f) demostración del cumplimiento de los requisitos de seguridad [sección 3]:

(1) esfuerzos de gestión y técnicos acordes con la complejidad del sistema para demostrar la seguridad del sistema;

(2) distribución de requisitos de seguridad del sistema hasta los subsistemas técnicos y las obras de ingeniería civil, así como a todas las funciones del metro relacionadas con la seguridad;

(3) demostración de que cada uno de los subsistemas, tal como se ha construido, cumple los requisitos de seguridad aplicables;

(4) en cuanto a las funciones de seguridad realizadas por diversos subsistemas, la demostración de que cumplen los requisitos de seguridad no pudo concluirse en el nivel del subsistema. Ésta se realizó en el nivel del sistema mediante la integración de diferentes subsistemas, herramientas y procedimientos;

(5) demostración de que el sistema global cumple los requisitos de seguridad de alto nivel;

(g) gestión de los peligros [sección 4.1]:

Los peligros determinados, las medidas de seguridad asociadas y los requisitos de seguridad resultantes se registraron y gestionaron en el registro central de peligros. El

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

responsable de la seguridad global del proyecto se hizo cargo de este registro de peligros. Los peligros operativos que surgieron durante las fases de diseño e instalación, así como los peligros relacionados con la explotación y el mantenimiento, se incluyeron en el registro de peligros;

(h) evidencias de la gestión del riesgo y evaluación del riesgo [sección 5]:

Un caso de seguridad documentó y apoyó oficialmente los resultados de la evaluación del riesgo, de conformidad con los requisitos de las normas CENELEC:

(1) caso de seguridad del sistema global;
(2) caso de seguridad para cada subsistema técnico (incluidos los subsistemas de señalización y las obras de ingeniería civil);
(3) caso de seguridad para las obras de ingeniería civil (estaciones, túneles, viaductos, o terraplenes);
(4) caso de seguridad de la instalación;
(5) caso de seguridad de vehículos;
(6) caso de seguridad del operador (que apoye la certificación del sistema de gestión de la seguridad de la empresa ferroviaria y el administrador de la infraestructura, es decir, en el que se demuestre la capacidad del proponente para explotar y mantener el sistema en condiciones de seguridad);

(i) evaluación independiente [Artículo 6]:

El proceso global fue objeto de seguimiento y evaluación a cargo de un evaluador de la seguridad, que actuó junto con una delegación de la autoridad de supervisión técnica (es decir, el Ministerio de Transportes danés). Las funciones del evaluador independiente de la seguridad se describen en un código de prácticas pertinente, en el que se incluyen las siguientes:

(1) comprobar la correcta gestión del riesgo y evaluación del riesgo;
(2) comprobar que el sistema se adapta a su función, y que se explotará y mantendrá durante su ciclo vital completo;
(3) recomendar su aceptación a la autoridad de supervisión técnica.

C.9.4. El proyecto completo se sometió a un proceso adecuado de gestión de la calidad.

C.9.5. En el marco del proyecto se proporcionó al responsable de la seguridad de la entidad proponente las evidencias facilitadas por los proveedores (es decir, casos de seguridad y documentación detallada de apoyo en relación con los subsistemas técnicos y las obras de ingeniería civil). Posteriormente, dichas evidencias se sometieron al examen de la organización encargada de la gestión de la seguridad, así como del evaluador independiente de la seguridad, cuyas conclusiones se recogieron en un informe de evaluación.
El responsable de la seguridad de la entidad proponente examinó el informe de evaluación independiente de la seguridad, que se presentó al proponente, que remitió todos los expedientes a la autoridad de supervisión técnica (es decir, el Ministerio de Transportes danés) para su aceptación final.

C.9.6. El ejemplo demuestra que los principios establecidos por el método común de seguridad son métodos existentes en el sector ferroviario. La evaluación del riesgo presentada en el ejemplo cumple todos los requisitos del MCS. En particular, ésta utiliza los tres principios de aceptación del riesgo permitidos por el enfoque armonizado del MCS.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

C.10. Ejemplo de la directriz de la OTIF para calcular el riesgo debido al transporte de mercancías peligrosas por ferrocarril

C.10.1. **Observación:** este ejemplo de evaluación del riesgo no es el resultado de la aplicación del proceso MCS, sino que se expuso antes de que existiera el MCS. El objetivo de este ejemplo es:

(a) identificar las similitudes entre los métodos de evaluación del riesgo existentes y el proceso MCS;

(b) mostrar la trazabilidad entre el proceso existente y el establecido por el MCS;

(c) justificar el valor añadido que supone realizar los pasos adicionales (si hubiera) establecidos por el MCS.

Cabe subrayar que este ejemplo sólo se ofrece a título informativo. Su objetivo es ayudar al lector a comprender el proceso MCS. Sin embargo, dicho ejemplo no se incorporará a un sistema de referencia ni se usará como tal para otro cambio significativo. La evaluación del riesgo se llevará a cabo para cada cambio significativo, de conformidad con el Reglamento MCS.

C.10.2. La filosofía general de la directriz de la OTIF es conforme con el propósito del MCS, si bien aquella tiene un alcance reducido. El objetivo de la directriz de la OTIF es *"obtener un enfoque más uniforme de la evaluación del riesgo del transporte de mercancías peligrosas en los Estados miembros de la COTIF y, de ese modo, hacer que las distintas evaluaciones de riesgos sean comparables"*. Así pues, apoya la aceptación recíproca, entre los Estados miembros de la COTIF, de evaluaciones de riesgos del transporte de mercancías peligrosas por ferrocarril.

C.10.3. Comparada con el MCS y el diagrama de la Figura 1:

(a) la directriz de la OTIF presenta los siguientes puntos comunes:

(1) es un enfoque común de la evaluación del riesgo, no obstante, sólo se basa en la estimación explícita del riesgo (es decir, el tercer principio de aceptación del riesgo del MCS);

(2) la evaluación del riesgo de la OTIF consiste en:

(i) una fase de análisis de riesgos que incluye:

- una fase de determinación de los peligros;
- una fase de estimación del riesgo;

(ii) una fase de valoración del riesgo basada en criterios (de aceptación) del riesgo que todavía no están armonizados. De hecho, muchas especificaciones nacionales pueden influir en dichos criterios;

(b) la directriz de la OTIF difiere del MCS en los aspectos siguientes:

(1) el ámbito de aplicación es diferente. Mientras que el MCS tiene que aplicarse únicamente para cambios significativos en el sistema ferroviario, la directriz de la OTIF debería aplicarse para evaluar los riesgos que supone transportar mercancías peligrosas por ferrocarril, ya constituya o no un cambio significativo en el sistema ferroviario;

(2) no cabe la posibilidad de elegir entre tres principios de aceptación del riesgo para controlar el/los riesgo(s). El tercer principio, a saber, la estimación explícita del riesgo, es el único permitido. Por otra parte, debe basarse exclusivamente en una estimación cuantitativa del riesgo, en lugar de una estimación cualitativa. El análisis

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

cualitativo del riesgo puede ser adecuado únicamente para comparar opciones de medidas (de seguridad) de reducción del riesgo;

(3) se exige la aplicación del principio ALARP para determinar si otras medidas de seguridad podrían seguir reduciendo el riesgo evaluado a un coste razonable;

(4) no contempla el concepto de "peligros asociados con riesgos ampliamente aceptables", que permite centrar la atención de la evaluación del riesgo en los peligros más coadyuvantes. No obstante, recomienda que se reduzca el número de supuestos de accidentes potenciales a un número razonable de supuestos básicos (véase la sección 3.2 de {Ref. 10});

(5) el proceso se centra en la evaluación del riesgo, pero no incluye:

(i) el proceso de selección y aplicación de medidas (de seguridad) para modificar el riesgo;
(ii) el proceso de aceptación del riesgo;
(iii) el proceso de demostración del cumplimiento de los requisitos de seguridad;
(iv) el proceso de comunicación del riesgo a otros agentes interesados (véase el apartado siguiente);

(6) no da instrucciones acerca de las evidencias que debe proporcionar el proceso de evaluación del riesgo;

(7) no exige que se proceda a la gestión del peligro;

(8) no exige que terceros realicen una evaluación independiente de la correcta aplicación del enfoque común.

C.10.4. Tras comparar la directriz de la OTIF con el MCS se constata que ambos son compatibles, pese a que su ámbito de aplicación y objetivo no sean exactamente los mismos. El MCS es más general que la directriz de la OTIF, en ese sentido es más flexible. Por otra parte, el MCS también abarca más actividades de gestión del riesgo:

(a) permite usar tres principios de aceptación del riesgo que se basan en prácticas existentes en los ferrocarriles: véase la sección 2.1.4;

(b) se aplica únicamente para los cambios significativos, y sólo se procede a un análisis de riesgos adicional para peligros que no estén asociados con riesgos ampliamente aceptables;

(c) contempla la selección y aplicación de las medidas de seguridad que se espera controlen los peligros identificados y los riesgos asociados;

(d) armoniza el proceso de gestión del riesgo, lo que incluye:

(1) la armonización de los criterios de aceptación del riesgo que se trata en el ámbito de los trabajos de la Agencia sobre riesgos ampliamente aceptables y criterios de aceptación del riesgo;
(2) la demostración de que el sistema cumple los requisitos de seguridad;
(3) los resultados y las evidencias del proceso de evaluación del riesgo;
(4) el intercambio de información relacionada con la seguridad entre los agentes que intervienen en las interfaces;
(5) la gestión de todos los peligros identificados y medidas de seguridad asociadas en un registro de peligros;
(6) la evaluación independiente de la correcta aplicación del MCS a cargo de terceros.

C.10.5. Sin embargo, la aplicación de la directriz de la OTIF en el marco del MCS (en caso de que el transporte de mercancías peligrosas constituya un cambio significativo para un administrador de la infraestructura o una empresa ferroviaria) no plantea problemas, ya que es compatible con el uso del tercer principio de estimación explícita del riesgo.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

C.11. Ejemplo de evaluación del riesgo de una solicitud de aceptación de un nuevo tipo de material rodante

C.11.1. **Observación:** este ejemplo de evaluación del riesgo no es el resultado de la aplicación del proceso MCS, sino que se expuso antes de que existiera el MCS. El objetivo de este ejemplo es:

(a) identificar las similitudes entre los métodos de evaluación del riesgo existentes y el proceso MCS;

(b) mostrar la trazabilidad entre el proceso existente y el establecido por el MCS;

(c) justificar el valor añadido que supone realizar los pasos adicionales (si hubiera) establecidos por el MCS.

Cabe subrayar que este ejemplo sólo se ofrece a título informativo. Su objetivo es ayudar al lector a comprender el proceso MCS. Sin embargo, dicho ejemplo no se incorporará a un sistema de referencia ni se usará como tal para otro cambio significativo. La evaluación del riesgo se llevará a cabo para cada cambio significativo, de conformidad con el Reglamento MCS.

C.11.2. Este ejemplo de evaluación del riesgo se refiere a una solicitud de aceptación de un nuevo tipo de material rodante. Se realizó un análisis de riesgos para evaluar los riesgos relacionados con la introducción de nuevos vagones de mercancías.

C.11.3. El objetivo del cambio era aumentar la eficacia, la capacidad, el rendimiento y la fiabilidad del transporte de mercancías a granel en una línea de mercancías específica. Dado que los vagones estaban destinados al tráfico transfronterizo, también se requería la aceptación de dos autoridades nacionales de seguridad diferentes. El proponente era el operador de transporte, que, a su vez, pertenece a la empresa que produce las mercancías que se van a transportar.

C.11.4. El desarrollo del proyecto consistió en la construcción, la fabricación, el montaje, la entrada en servicio y la verificación del nuevo material rodante. Se realizó un análisis de riesgos para verificar que el nuevo diseño cumplía los requisitos de seguridad para cada uno de los subsistemas, así como para el sistema completo.

C.11.5. En el análisis de riesgos se hace referencia a los procedimientos y definiciones de la norma CENELEC EN 50126, y la valoración se realiza conforme a esta norma.

C.11.6. En comparación con el proceso MCS, se realizaron los siguientes pasos:

(a) descripción del sistema [sección 2.1.2]:

Para cada una de las fases de diseño existían requisitos en materia de documentación relativa a la verificación de la seguridad y descripción del diseño del sistema:

(1) fase conceptual: descripción preliminar de las exigencias de funcionamiento del operador;

(2) fase de especificación: especificación funcional, normas técnicas aplicables, plan de ensayos y verificación. Asimismo, se incluyeron los requisitos del operador sobre el uso y mantenimiento de los vagones;

(3) fase de fabricación: documentación técnica del fabricante, incluidos planos, normas, cálculos, etc. Análisis detallado del riesgo para diseños nuevos o innovadores o nuevos ámbitos de uso;

(4) fase de verificación:

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(i) verificación por el fabricante del comportamiento técnico de los vagones (informes de ensayos, cálculos y verificaciones de conformidad con las normas y los requisitos funcionales);
(ii) documentación de medidas que reducen el riesgo e informes de ensayos para demostrar la compatibilidad de los vagones con la infraestructura ferroviaria;
(iii) documentos de mantenimiento y formación, manuales de usuario, etc.

(5) fase de aceptación:

(i) declaración de seguridad y evidencias de seguridad (caso de seguridad) del fabricante;
(ii) la aceptación por el operador de los vagones de mercancías y la documentación sobre los mismos;

(b) determinación de los peligros [sección 2.2]:

se realizó una determinación del peligro continua en todas las fases del diseño. En primer lugar, se aplicó un enfoque “ascendente” en los casos en que los diferentes fabricantes evaluaron las secuencias de riesgo resultantes del fallo de componentes dentro de su subsistema. La división en subsistemas fue la siguiente:

(1) chasis;
(2) sistema de frenado;
(3) acoplamiento central;
(4) etc.

A continuación, se aplicó un enfoque “descendente” para buscar lagunas o información no facilitada. Los riesgos que no pudieron aceptarse inmediatamente se transfirieron al registro de peligros para su posterior tratamiento y clasificación.

(c) uso de principios de aceptación del riesgo [sección 2.1.4]:

Se realizó una estimación del riesgo explícito del sistema en su conjunto. No obstante, podían usarse códigos prácticos y sistemas de referencia similares para evaluar los distintos peligros. El principio es que cada uno de los nuevos subsistemas debería presentar al menos el mismo nivel de seguridad que el subsistema que sustituye, obteniéndose así un nuevo sistema completo con un nivel de seguridad superior al del sistema anterior. Se utilizó la matriz de riesgo de la norma EN50126 para trazar los peligros identificados. Asimismo, se aplicaron diferentes criterios de aceptación del riesgo adicionales, entre los que se incluyen los siguientes:

(1) un fallo único no debería llevar a una situación en que las personas, el material o el medio ambiente puedan verse seriamente afectados;
(2) si esto no puede evitarse con medios técnicos de construcción, deberían aplicarse normas operativas o requisitos de mantenimiento. Esto sólo era aplicable a peligros en caso de que fuera posible identificar el fallo ocurrido antes de que cree una situación peligrosa;
(3) para componentes con una gran probabilidad de fallo, o en caso de que los fallos no puedan detectarse de antemano o evitarse a través de normas operativas o de mantenimiento, debería considerarse la posibilidad de aplicar nuevas funciones y barreras de seguridad;
(4) los sistemas redundados con componentes en los que puedan surgir fallos no detectables deberían protegerse mediante la aplicación de medidas de mantenimiento para evitar una pérdida de la redundancia;
(5) el nivel de seguridad final resultante fue una decisión de gestión, que se basó en el análisis de riesgos cuantitativo y cualitativo;

(d) demostración del cumplimiento de los requisitos de seguridad [sección 3]:

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

Se registraron todos los riesgos y peligros identificados, y la lista se consultó y actualizó continuamente. El resto de los peligros se incluyó en el registro de peligros, junto con la correspondiente lista de medidas de reducción del riesgo que debían adoptarse en la construcción, explotación y mantenimiento del sistema. Sobre la base de dicho registro, se elaboró un informe final de seguridad, en el que se verificaba que se habían aplicado los requisitos de seguridad;

(e) gestión de los peligros [sección 4.1]:

Tal como se ha expuesto anteriormente, se registraron los peligros y las medidas de seguridad asociadas a los mismos en un registro de peligros, lo que permitía seguir la pista de todos los peligros identificados y medidas de seguridad. Sin embargo, en el registro de peligros no se incluyeron los peligros relacionados con riesgos que se consideraban aceptables sin necesidad de adoptar medidas;

(f) evaluación independiente [Artículo 6]:

En los documentos recibidos no se mencionaba la evaluación independiente en relación con este cambio significativo.

C.11.7. Este ejemplo de evaluación del riesgo se basa en la norma CENELEC EN 50126, por lo que se ajusta al proceso MCS. La evaluación del riesgo presentada en el ejemplo cumple todos los requisitos del MCS con la excepción del requisito para la evaluación independiente, que no quedó explícitamente aclarado en los documentos recibidos. Se usaron y se indicaron claramente los criterios de aceptación del riesgo.

C.12. Ejemplo de evaluación del riesgo de un cambio operativo significativo – Operación exclusiva por parte del maquinista

C.12.1. **Observación:** este ejemplo de evaluación del riesgo no es el resultado de la aplicación del proceso MCS, sino que se expuso antes de que existiera el MCS. El objetivo de este ejemplo es:

(a) identificar las similitudes entre los métodos de evaluación del riesgo existentes y el proceso MCS;

(b) mostrar la trazabilidad entre el proceso existente y el establecido por el MCS;

(c) justificar el valor añadido que supone realizar los pasos adicionales (si hubiera) establecidos por el MCS.

Cabe subrayar que este ejemplo sólo se ofrece a título informativo. Su objetivo es ayudar al lector a comprender el proceso MCS. Sin embargo, dicho ejemplo no se incorporará a un sistema de referencia ni se usará como tal para otro cambio significativo. La evaluación del riesgo se llevará a cabo para cada cambio significativo, de conformidad con el Reglamento MCS.

C.12.2. Este ejemplo ilustra un cambio operativo por el que la empresa ferroviaria decidió que el tren debía operarlo exclusivamente el maquinista en una ruta en la que anteriormente había un jefe de tren a bordo que ayudaba al maquinista en la circulación del tren.

C.12.3. En comparación con el proceso MCS, se realizaron los siguientes pasos (véase, asimismo, la Figura 1):

(a) importancia del cambio [Artículo 4]:

La empresa ferroviaria realizó una evaluación preliminar del riesgo que concluyó que el cambio operativo era significativo. Como el maquinista tenía que operar el tren solo, sin asistencia, no se podía desdeñar la posibilidad de que los viajeros pudieran quedar

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

atrapados entre las puertas o caer a la vía (por ejemplo, si las puertas se abren por el lado contrario).

Al comparar esta evaluación preliminar del riesgo con los criterios especificados en el Artículo 4 del Reglamento MCS, el cambio también podría clasificarse como significativo sobre la base de los siguientes criterios:

(1) importancia para la seguridad: el cambio repercute en la seguridad, ya que, al implicar una manera completamente diferente de gestionar la prestación del servicio ferroviario, podría tener consecuencias catastróficas;
(2) consecuencia de fallo: el efecto potencial del comportamiento del maquinista podría tener consecuencias catastróficas si no se controla eficazmente la prestación del servicio;
(3) novedad: la operación exclusiva por parte del maquinista podría requerir formas innovadoras de operar trenes cuyos riesgos han de evaluarse;

(b) definición del sistema [sección 2.1.2]:

La definición del sistema describía:

(1) el sistema existente, explicando claramente las funciones que desempeñaba el maquinista y las que llevaba a cabo el personal de a bordo (o el jefe de tren) para ayudar al maquinista;
(2) el cambio de las responsabilidades del maquinista, debido a la supresión del personal auxiliar de a bordo;
(3) los requisitos técnicos del sistema para cubrir los cambios de funcionamiento;
(4) las interfaces existentes entre el personal auxiliar de a bordo, el maquinista y el personal en tierra del administrador de la infraestructura;

Durante las diferentes iteraciones, la definición del sistema se actualizó con los requisitos de seguridad resultantes del proceso de evaluación del riesgo. En este proceso iterativo de determinación del peligro y actualización de la definición del sistema participaron personas clave (incluidos los maquinistas, representantes del personal y el administrador de la infraestructura).

(c) determinación de los peligros [sección 2.2]:

Se identificaron los peligros y las posibles medidas de seguridad mediante una tormenta de ideas a cargo de un grupo de expertos, que incluía, entre otros, a:

(1) representantes de los maquinistas y del personal, por su experiencia operativa;
(2) representantes del administrador de la infraestructura, ya que la infraestructura también podría verse afectada por el cambio, que implicaba, por ejemplo, cambios en las estaciones (tales como la instalación de espejos o un circuito cerrado de televisión en los andenes);

Se examinaron las funciones adicionales que debía desempeñar el maquinista a fin de identificar todos los peligros previsibles que pudieran aparecer a raíz de la supresión del personal auxiliar de a bordo. En particular, en la determinación del peligro se analizaron los principales peligros operativos que podrían presentarse en las estaciones, en las rutas existentes en las que el personal de a bordo o en tierra prestaba asistencia, incluido en la regulación segura de la circulación de los trenes, cuestiones específicas relacionadas con el maquinista, el material rodante (por ejemplo, apertura de puertas/comprobación del cierre), requisitos de mantenimiento, etc.

Se asignó un nivel de gravedad del riesgo (alto, medio o bajo) y de las consecuencias a cada uno de los peligros identificados, y se revisó la repercusión del cambio propuesto a la luz de los mismos (riesgo aumentado, no modificado, reducido).

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

(d) uso de códigos prácticos [sección **Error! Reference source not found.**] y uso de sistemas de referencia similares [sección 2.4]:

Se usaron tanto códigos prácticos (esto es, un conjunto de normas para la operación exclusiva por parte del maquinista) como sistemas de referencia similares para definir los requisitos de seguridad en relación con los peligros identificados. Estos requisitos de seguridad incluían:

(1) los procedimientos operativos revisados que el maquinista debía seguir para operar trenes en condiciones seguras sin asistencia a bordo;
(2) cualesquiera equipos adicionales necesarios a bordo o en tierra para garantizar unos medios seguros y fiables de expedición del tren;
(3) una lista de comprobación para garantizar la adecuación del puesto de conducción, teniendo en cuenta la interfaz existente entre el sistema ferroviario (a bordo y en tierra) y el maquinista;

Las normas operativas necesarias se revisaron con arreglo a los requisitos de los códigos prácticos y los sistemas de referencia pertinentes. Todos los agentes involucrados participaron en los procedimientos operativos revisados y en el acuerdo para llevar a cabo el cambio.

(e) demostración del cumplimiento de los requisitos de seguridad [sección 3]:

El sistema se aplicó de conformidad con los requisitos de seguridad identificados (equipos adicionales y procedimientos revisados). Se comprobó que éstos constituían medios adecuados para garantizar un nivel de seguridad suficiente para el sistema objeto de evaluación.

Los procedimientos operativos revisados se introdujeron en el sistema de gestión de la seguridad de la empresa ferroviaria. Se sometieron a un control y se revisaron, en la medida de lo necesario, para garantizar que los peligros identificados continuaran siendo objeto de controles adecuados durante la explotación del sistema ferroviario.

(f) gestión de los peligros [sección 4.1]:

Véase el apartado anterior, ya que, por lo que respecta a las empresas ferroviarias, el proceso de gestión del peligro puede formar parte de su sistema de gestión de la seguridad para el registro y control de riesgos. Los peligros identificados se incluyeron en un registro de peligros con los requisitos de seguridad que permiten controlar el riesgo asociado, es decir, haciendo referencia a los equipos adicionales a bordo y en tierra, así como a los procedimientos operativos revisados.
Los procedimientos revisados se sometieron a un control, y se revisaron en la medida de lo necesario, para garantizar que los peligros identificados continuaran siendo objeto de controles adecuados durante la explotación del sistema ferroviario.

(g) evaluación independiente [Artículo 6]:

Una persona competente de la empresa ferroviaria e independiente del proceso de evaluación evaluó los procesos de gestión del riesgo y evaluación del riesgo. Esta persona competente evaluó tanto los procesos como los resultados, es decir, los requisitos de seguridad identificados.

La empresa ferroviaria ha basado su decisión de poner en marcha el nuevo sistema en el informe de evaluación independiente elaborado por la persona competente.

C.12.4. El ejemplo muestra que los principios y procesos utilizados por la empresa ferroviaria son conformes con el método de seguridad común. Los procesos de gestión del riesgo y evaluación del riesgo cumplían todos los requisitos del MCS.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

C.13. Ejemplo del uso de un sistema de referencia para establecer requisitos de seguridad aplicables a sistemas de enclavamiento electrónico en Alemania

C.13.1. **Observación:** este ejemplo de evaluación del riesgo no es el resultado de la aplicación del proceso MCS, sino que se expuso antes de que existiera el MCS. El objetivo de este ejemplo es:

(a) identificar las similitudes entre los métodos de evaluación del riesgo existentes y el proceso MCS;

(b) mostrar la trazabilidad entre el proceso existente y el establecido por el MCS;

(c) justificar el valor añadido que supone realizar los pasos adicionales (si hubiera) establecidos por el MCS.

Cabe subrayar que este ejemplo sólo se ofrece a título informativo. Su objetivo es ayudar al lector a comprender el proceso MCS. Sin embargo, dicho ejemplo no se incorporará a un sistema de referencia ni se usará como tal para otro cambio significativo. La evaluación del riesgo se llevará a cabo para cada cambio significativo, de conformidad con el Reglamento MCS.

C.13.2. A fin de establecer requisitos de seguridad normalizados para futuros sistemas de enclavamiento electrónico, Deutsche Bahn había llevado a cabo un análisis de riesgos de un sistema electrónico ya aprobado. Este sistema se había aprobado anteriormente con arreglo a códigos prácticos alemanes (Mü 8004).

C.13.3. El análisis de riesgos se efectuó de conformidad con las normas CENELEC (EN 50126 y EN 50129), e incluía los pasos siguientes:

(a) definición del sistema;
(b) determinación de los peligros;
(c) análisis y cuantificación del peligro.

C.13.4. Para la definición del sistema, se había tenido cuidado de definir los límites del sistema, sus funciones y sus interfaces. La principal dificultad consistía en definir del sistema de manera que fuera independiente de la arquitectura interna de un sistema de enclavamiento y siguiera siendo compatible con los sistemas de enclavamiento existentes. Por lo tanto, se hizo especial hincapié en la necesidad de definir con precisión las interfaces con sistemas externos que interactuaban con el enclavamiento, sin detallar las funciones internas del enclavamiento.

C.13.5. A continuación, se identificaron los peligros únicamente en las interfaces para que siguieran siendo genéricos (esto es, para evitar cualquier tipo de dependencia con arquitecturas específicas). Sólo se tuvieron en cuenta los peligros derivados de fallos técnicos. Así pues, se identificaron dos peligros genéricos para cada una de las interfaces:

(a) valor incorrecto registrado por el enclavamiento transmitido a la interfaz
(b) los datos (correctos) de entrada se ven alterados en la interfaz

C.13.6. Por lo tanto, se atribuyeron características más específicas a estos peligros genéricos para cada una de las interfaces.

C.13.7. En la siguiente fase se analizaron los aspectos de los componentes del sistema existente que contribuían a cada uno de los peligros identificados, y se representaron en un diagrama de fallos. Esto permitió, sobre la base de las tasas de fallo estimadas de los componentes,

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

calcular una tasa de incidencia para cada peligro, y utilizar dichas tasas como tasas de peligro tolerable para futuras generaciones de enclavamientos electrónicos.

C.13.8. La autoridad nacional de seguridad (EBA) realizó un seguimiento y una evaluación del análisis de riesgos.

C.13.9. Como parte del análisis de riesgos, también se llevó a cabo un análisis de las funciones de control y visualización del sistema electrónico. Una vez más, se tomó como sistema de referencia un sistema de enclavamiento electrónico existente aprobado a fin de establecer requisitos de seguridad de las funciones de la interfaz hombre-máquina para controlar los errores y fallos aleatorios, así como los fallos sistemáticos, a resultas de lo cual, se determinaron los niveles de integridad de la seguridad (SIL) para diferentes funciones: para funciones de la interfaz hombre-máquina en operaciones normales, para funciones de la interfaz hombre-máquina en las operaciones de accionamiento de mando (modo degradado), y para la funcionalidad de visualización.

C.13.10. La autoridad nacional de seguridad (EBA) también realizó un seguimiento y una evaluación de este análisis de riesgos.

C.13.11. Esos ejemplos de evaluación del riesgo ilustran cómo puede utilizarse el segundo principio de aceptación del riesgo (sistema de referencia) del MCS para establecer requisitos de seguridad para un nuevo sistema. Además, se basaron en las normas CENELEC, por lo que se ajustan al proceso MCS. La evaluación del riesgo presentada en los ejemplos cumple los requisitos del MCS relativos a las fases cubiertas por la misma. Sin embargo, como no incluye la actividad de diseño, no hace referencia a la gestión del registro de peligros ni a la demostración de que el sistema objeto de evaluación cumple los requisitos de seguridad identificados.

C.13.12. Puede encontrarse más información sobre estos análisis de riesgos en:

(a) Ziegler, P., Kupfer, L., Wunder, H.: *"Erfahrungen mit der Risikoanalyse ESTW (DB AG)"*, Signal+Draht, 10, 2003, 10-15, y;

(b) Bock, H., Braband, J., y Harborth, M.: "*Safety Assessment of Vital Control and Display Functions in Electronic Interlockings, in Proc. AAET2005 Automation, Assistance and Embedded Real Time Platforms for Transportation*", GZVB, Braunschweig, 2005, 234-253.

C.14. Ejemplo de un criterio explícito de aceptación del riesgo para la explotación de trenes basada en la radio (FFB) en Alemania

C.14.1. **Observación:** este ejemplo de evaluación del riesgo no es el resultado de la aplicación del proceso MCS, sino que se expuso antes de que existiera el MCS. El objetivo de este ejemplo es:

(a) identificar las similitudes entre los métodos de evaluación del riesgo existentes y el proceso MCS;

(b) mostrar la trazabilidad entre el proceso existente y el establecido por el MCS;

(c) justificar el valor añadido que supone realizar los pasos adicionales (si hubiera) establecidos por el MCS.

(d) Cabe subrayar que este ejemplo sólo se ofrece a título informativo. Su objetivo es ayudar al lector a comprender el proceso MCS. Sin embargo, dicho ejemplo no se

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

incorporará a un sistema de referencia ni se usará como tal para otro cambio significativo. La evaluación del riesgo se llevará a cabo para cada cambio significativo, de conformidad con el Reglamento MCS.

C.14.2. Se llevó a cabo un análisis de riesgos de conformidad con las normas CENELEC en relación con un procedimiento operativo totalmente nuevo que se había previsto (pero nunca introducido) en Alemania para líneas ferroviarias convencionales. El concepto consistía en la explotación de trenes en condiciones de seguridad sólo mediante un sistema de control basado en la radio (ruta y tren). Como no existían códigos prácticos (reglas de ingeniería reconocidas) ni sistemas de referencia para un nuevo sistema de esas características, se realizó una estimación explícita del riesgo para demostrar la seguridad del nuevo procedimiento. Había que demostrar que el nivel de riesgo que presentaba el nuevo sistema para un viajero no excedería un valor de riesgo aceptable (criterio de aceptación del riesgo explícito).

C.14.3. Este criterio de aceptación del riesgo explícito se estimó sobre la base de estadísticas de accidentes en Alemania que habían sido atribuibles a sistemas de señalización y control, y se comprobó su plausibilidad con el criterio MEM. Tal demostración de la seguridad es conforme con el requisito de la EBO alemana de presentar “el mismo nivel de seguridad” en caso de desviaciones con respecto a las reglas de ingeniería. La autoridad nacional de seguridad (EBA) también realizó un seguimiento y una evaluación del análisis de riesgos.

C.14.4. Este ejemplo de evaluación del riesgo muestra cómo puede establecerse un criterio global explícito (en relación con el tercer principio de aceptación del riesgo del MCS) para nuevos sistemas en ausencia de códigos prácticos y sistemas de referencia aplicables. El análisis de riesgos que se llevó a cabo posteriormente para el nuevo sistema se basa en las normas CENELEC, por lo que se ajusta al proceso MCS. La evaluación del riesgo presentada en el ejemplo cumple los requisitos del MCS, sin embargo, no se hace referencia a la gestión del registro de peligros ni a la demostración de que el sistema objeto de evaluación cumple los requisitos de seguridad identificados.

C.14.5. Puede encontrarse más información sobre este análisis de riesgos en: Braband, J., Günther, J., Lennartz, K., Reuter, D.: “*Risikoakzeptanzkriterien für den FunkFahrBetrieb (FFB)*”, Signal + Draht, Nr.5, 2001, 10-15

C.15. Ejemplo de comprobación de la aplicabilidad del criterio de aceptación del riesgo para sistemas técnicos

C.15.1. El objetivo del presente apéndice es mostrar con un ejemplo de la función del subsistema ETCS de a bordo la manera de usar el criterio referido en la sección 2.5.4 y de determinar si el criterio de aceptación del riesgo para sistemas técnicos es aplicable.

C.15.2. El subsistema ETCS de a bordo es un sistema técnico. Se tiene en cuenta la siguiente función: “*proporcionar al maquinista información para que pueda conducir el tren de manera segura y aplicar un frenado en caso de exceso de velocidad*”.

Descripción de la función: basándose en la información recibida desde tierra (velocidad permitida) y en la velocidad del tren calculada por el subsistema ETCS de a bordo:

(a) el maquinista conduce el tren y vela por que la velocidad del tren no exceda el límite de velocidad permitido;

(b) simultáneamente, el subsistema ETCS de a bordo supervisa que los trenes nunca excedan el límite de velocidad permitido. En caso de exceso de velocidad, aplica automáticamente los frenos.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

Tanto el maquinista como el subsistema ETCS de a bordo utilizan la evaluación de la velocidad del tren calculada por el subsistema ETCS de a bordo.

C.15.3. Cuestión: "¿Se aplica el criterio de aceptación del riesgo para sistemas técnicos a la evaluación de la velocidad del tren calculada por el ETCS a bordo?"

C.15.4. Aplicación del organigrama de la Figura 14 y respuestas a las diferentes preguntas:

(a) Peligro considerado para el sistema técnico:

"Exceso de la velocidad de seguridad recomendada al ETCS" (véase UNISIG SUBSET 091).

(b) ¿Puede controlarse el peligro mediante el uso de un código de prácticas o un sistema de referencia?

NO. Se presupone que el sistema ETCS es un proyecto nuevo e innovador. Por lo tanto, no existen códigos prácticos ni sistemas de referencia que permitan controlar el peligro a un nivel aceptable de riesgo.

(c) ¿Es probable que el peligro pueda tener una consecuencia catastrófica?

SÍ, ya que un *"exceso de la velocidad de seguridad recomendada al ETCS"* puede provocar el descarrilamiento de un tren, que podría causar *"víctimas mortales y/o múltiples lesiones corporales graves y/o importantes daños al medio ambiente"*.

(d) ¿La consecuencia catastrófica es consecuencia directa del fallo del sistema técnico?

SÍ, en caso de que no existan nuevas barreras de seguridad. Se proporciona la misma evaluación de la velocidad del tren calculada por el subsistema ETCS de a bordo al maquinista y a la función de control de freno del subsistema ETCS de a bordo. Por lo tanto, suponiendo que el maquinista conduce el tren (por motivos de rendimiento) a la velocidad máxima permitida desde tierra, el maquinista y el subsistema ETCS de a bordo no detectarán que el tren excede el límite de velocidad en caso de subestimación de la velocidad del tren. Esa situación podría provocar un descarrilamiento del tren con consecuencias catastróficas.

(e) Conclusiones:

(1) en relación con los requisitos cuantitativos: aplicar una tasa de peligro tolerable de 10^{-9} h^{-1} para los fallos aleatorios de los equipos del subsistema ETCS de a bordo, velando por que:

(i) la evaluación de este objetivo cuantitativo tenga en cuenta, para los sistemas redundantes, los componentes comunes (tales como un solo dato o datos comunes a todos los canales, una fuente de alimentación común, comparadores, dispositivos de toma de decisión, etc.);
(ii) queden cubiertos los tiempos de detección de fallos latentes;
(iii) se realice un análisis de los fallos o averías de causa común;
(iv) se lleve a cabo una evaluación independiente;

(2) en relación con los requisitos del proceso: aplicar un proceso SIL 4 para la gestión de los fallos o errores sistemáticos del subsistema ETCS de a bordo. Para ello es necesario aplicar:

(i) un proceso de gestión de la calidad conforme con el SIL 4;
(ii) un proceso de gestión de la seguridad conforme con el SIL 4;
(iii) las normas pertinentes, por ejemplo:

- la norma EN 50 128 para el desarrollo de programas informáticos;

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

- las normas EN 50 121-3-2, EN 50 121-4, EN 50 124-1, EN 50 124-2, EN 50 125-1 EN 50 125-3, EN 50 50081, EN 50 155, EN 61000-6-2, etc. para el desarrollo de equipos;

(3) una evaluación independiente del/de los proceso(s).

C.16. Ejemplos de posibles estructuras del registro de peligros

C.16.1. Introducción

C.16.1.1. En la sección 4.1.2 del Reglamento MCS se especifican los requisitos mínimos que deben incluirse en el registro de peligros. Éstos aparecen con un fondo sombreado en los ejemplos de registros de peligros que figuran a continuación.

C.16.1.2. Pueden existir diferentes formas de estructurar un registro de peligros, así como toda información adicional que podría caracterizar los peligros y las medidas de seguridad asociadas. Por ejemplo, los peligros y medidas de seguridad asociadas pueden incluirse en un campo por elemento informativo. No obstante, sea cual sea la estructura utilizada, es importante que el registro de peligros establezca una vinculación clara entre los peligros y las medidas de seguridad asociadas. Una posible solución consiste en que el registro de peligros contenga, para cada peligro y para cada medida de seguridad, al menos un campo con:

(a) una clara descripción que incluya referencias de su origen y del principio de aceptación del riesgo seleccionado para controlar el peligro asociado. este campo permite entender el peligro y las medidas de seguridad asociadas, así como saber en qué análisis de la seguridad se han identificado.

Como el registro de peligros se utiliza y mantiene durante todo el ciclo de vida del sistema (es decir, durante la explotación y el mantenimiento del sistema), resulta útil establecer una clara trazabilidad, o vinculación, entre cada peligro y:

(1) el riesgo asociado;
(2) las causas del peligro cuando ya han sido identificadas;
(3) las medidas de seguridad asociadas, así como los supuestos que definen los límites del sistema objeto de evaluación;
(4) los análisis de la seguridad asociados, en caso de que se haya identificado el peligro;

Asimismo, la definición de las medidas de seguridad (en particular, las que se transfieran a otros agentes tales como el proponente) y de los peligros y riesgos asociados debe ser clara y suficiente. “Clara y suficiente” significa que pueden entenderse qué riesgos se espera controlen las medidas de seguridad y los peligros asociados, sin necesidad de volver a realizar los análisis de seguridad que corresponda.

(b) el principio de aceptación del riesgo utilizado para controlar el peligro, a fin de apoyar el reconocimiento recíproco y ayudar al organismo de evaluación a evaluar la correcta aplicación del MCS;

(c) información clara sobre su estado: este campo indica si el peligro o la medida de seguridad de que se trate sigue sin estar controlado o está controlado/validado.

(1) se hace un seguimiento del peligro o la medida de seguridad que no está controlado hasta que esté controlado/validado;
(2) recíprocamente, ya no se realizan seguimientos de los peligros/las medidas de seguridad controlados/validados salvo que se produzcan cambios significativos en

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

la explotación o el mantenimiento del sistema: véase la letra (b) del apartado [G 6] de la sección 2.1.1. En tal caso:

(i) se vuelve a aplicar el MCS sobre los cambios requeridos de conformidad con el Artículo 2. Véase, asimismo, el punto (1) de la letra (b) del apartado [G 6] de la sección 2.1.1;

(ii) se vuelven a examinar todos los peligros y medidas de seguridad controlados para comprobar que no se ven afectados por los cambios. En caso de verse afectados, los peligros y medidas de seguridad asociadas se vuelven a considerar pendientes y se gestionan en el registro de peligros;

Podría ocurrir que se aplicasen otras medidas de seguridad en lugar de las registradas en el registro de peligros (por ejemplo, por razones de costes). Entonces, se incluyen las medidas de seguridad en el registro de peligros con las evidencias o la justificación de su carácter adecuado y la demostración de que, con estas medidas, el sistema simple los requisitos de seguridad.

(d) la referencia a las evidencias asociadas que permiten controlar un peligro o validar una medida de seguridad. Este campo permite encontrar más adelante las evidencias que han permitido controlar el peligro y validar la(s) medida(s) de seguridad asociada(s);

Podría controlarse un peligro en el registro de peligros únicamente cuando todas las medidas de seguridad asociadas, vinculadas al peligro, han sido validadas de antemano;

(e) la(s) organización(es) o entidad(es) encargada(s) de gestionarlo.

C.16.1.3. En el Apéndice A.3. de la directriz EN 50126-2 {Ref. 9} se ofrece otro ejemplo del posible contenido de un registro de peligros.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

C.16.2. Ejemplo del registro de peligros para el cambio organizativo a que se refiere la sección C.5 del Apéndice C

Cuadro 6: Ejemplo del registro de peligros para el cambio organizativo a que se refiere la sección C.5. del Apéndice C.

Descripción del peligro	**Medidas de seguridad**	**Prioridad/ Efecto en la seguridad**	**Aplicación[18]**	**Notas**	**Responsable[18]**	**Origen**	**Principio de aceptación del riesgo utilizado**	**Responsable de la verificación**	**Forma de verifi-cación**	**Estado xx.xx.xx**
Menor motivación entre los empleados que permanecen en la empresa. De ahí que el personal siga abandonando la empresa de forma constante. Administradores desmotivados y agotados	Nueva ronda de trabajos de motivación para el personal, que se llevará a cabo en grupos más pequeños Reasignación de fondos para que la empresa pueda desempeñar tareas útiles. Inspecciones más frecuentes por parte del administrador de la vía. Asignar fondos para garantizar la permanencia del personal clave a lo largo del proceso. Prestar especial atención para garantizar que la información y los conocimientos se transfieran entre los empleados que abandonan la empresa y aquellos que asumen sus tareas. etc.	Alta/Alta	Coordinadas por XYZ. Las regiones deben estudiar medidas para aumentar el control de las vías, el solapamiento de funciones de empleados y el seguimiento por el administrador de la línea	Es necesario incluir inspecciones en los contratos. Etc.	Administrador de la empresa	Tormenta de ideas Informe de identificación del peligro R_X	N/A			El cambio en las condiciones de las circunstancias ha reducido este riesgo de forma significativa. Realización de trabajos de análisis del entorno y de formación del personal.
Los subcontratistas de los empresarios carecen de aptitudes y competencia u no disponen de controles de calidad	Mayor exigencia de competencia documentada. Control sistemático de las tareas desempeñadas	Alta/ Media	El administrador de la infraestructura sebe coordinar las medidas. Las regiones deben aplicar las medidas para exigir la compe-tencia y controlar los trabajos	Aplicación mediante un seguimiento del contrato. Aportación de datos a la planificación de la revisión.	Administrador de la infra-estructura	Ejercicio de reflexión Informe de identificación del peligro R_X	N/A	Administrador de la seguridad		Mayor prioridad a las rutinas de los controles (2 controles operativos mensuales por ámbito operativo)
Incertidumbre de las funciones y responsabilidades en la interfaz entre la empresa y el administrador de la infraestructura (administrador de la vía).	Definir las funciones y responsabilidades. Reflejar todas las interfaces y definir quién es el responsable de las interfaces.	Media/ Media	En cada región por separado	Aplicación mediante un contrato de mantenimiento y el plan de estrategia para la reorganización	Directores regionales	Ejercicio de reflexión Informe de identificación del peligro R_X	N/A	Administrador de la seguridad		Las regiones han presentado su estrategia.

(18) *Estas dos columnas se refieren a la información y al campo acerca de los agentes encargados de controlar los peligros identificados.*

(18). *Estas dos columnas corresponden a la información/ al campo referente a las partes responsables del control de los riesgos identificados.*

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

C.16.3. Ejemplo de un registro de peligros completo para un subsistema de mando y control a bordo

C.16.3.1. En esta sección se ofrece un ejemplo de un único registro de peligros (véase el apartado [G 3] de la sección 4.1.1) para gestionar:

todos los requisitos de seguridad internos aplicables al subsistema que compete al agente; y,

todos los peligros identificados y las medidas de seguridad asociadas que el agente no puede aplicar y que deben transferirse a otros agentes.

Cuadro 7: Ejemplo de registro de peligros de un fabricante para un subsistema de mando y control a bordo.

N° del peligro	Origen	Descripción del peligro	Información adicional	Agente responsable	Medida de seguridad	Principio de aceptación del riesgo utilizado	Expor-tado	Estado
1	Informe de riesgos y operabilidad tipo HAZOP RX	Velocidad máxima del tren establecida demasiado alta (Vmax)	Configuración específica incorrecta del subsistema de a bordo (personal de mantenimiento). Introducción de datos incorrectos a bordo (maquinista)	Empresa ferroviaria	• Definir un procedimiento para la aceptación de los datos de la configuración del subsistema de a bordo; • Definir un procedimiento operativo para el proceso de introducción de datos por el maquinista;	Estimación explícita del riesgo explícito	Sí	Controlado (exportado a la empresa ferroviaria) Véase, asimismo, la sección C.16.4.2. del Apéndice C
2	Informe de riesgos y operabilidad tipo HAZOP RX	Curvas de frenado (es decir, autoridad de movimiento) de la configuración del subsistema de a bordo demasiado permisivas	El procedimiento para establecer la configuración específica del subsistema de a bordo depende de: • los márgenes de seguridad adoptados para el sistema de frenado del tren; • el retraso de reacción del sistema de frenado del tren (éste depende directamente de la longitud del tren, en particular para los trenes de mercancías)	Empresa ferroviaria	• Especificar correctamente los requisitos del sistema en la definición del sistema; • Adoptar márgenes de seguridad suficientes para el sistema se frenado del tren de que se trate;	Estimación explícita del riesgo	Sí	Controlado (exportado a la empresa ferroviaria) Véase, asimismo, la sección C.16.4.2. del Apéndice C
3	Informe de riesgos y operabilidad tipo HAZOP RX	• Velocidad máxima del tren establecida demasiado alta (Vmax) • Curvas de frenado (es decir, autoridad de movimiento) de la configuración del subsistema de a bordo	Incapacidad para actualizar el diámetro de rueda del tren en la configuración específica del subsistema de a bordo (personal de mantenimiento).	Empresa ferroviaria	• Definir un procedimiento para la medición del diámetro de rueda del tren por el personal de mantenimiento; • Definir un procedimiento para actualizar regularmente el diámetro de rueda del tren en el	Estimación explícita del riesgo	Sí	Controlado (exportado a la empresa ferroviaria) Véase, asimismo, la sección C.16.4.2. del Apéndice C

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

Cuadro 7: Ejemplo de registro de peligros de un fabricante para un subsistema de mando y control a bordo.

N° del peligro	Origen	Descripción del peligro	Información adicional	Agente responsable	Medida de seguridad	Principio de aceptación del riesgo utilizado	Expor-tado	Estado
		demasiado permisivas			subsistema de a bordo;			
			Incapacidad en el marco del procedimiento del fabricante para preparar y cargar los datos de configuración en el subsistema de a bordo	Fabricante	Definir un procedimiento para actualizar los datos de configuración de a bordo relativos al diámetro de rueda del tren	Estimación explícita del riesgo	Sí	Controlado Mediante el procedimiento P_X
4	Informe de riesgos y operabilidad tipo HAZOP RX	Entrada del tren a gran velocidad (160 km/h en caso de señal en tierra libre) en la vía sin subsistema a bordo activo y sin señalización en tierra	Podría controlarse únicamente mediante una labor de vigilancia del maquinista. El acceso a zona provista de una ATP desde tierra se basa en un procedimiento de reconocimiento por el maquinista antes de llegar al lugar de transición. En caso de ausencia de reconocimiento, el subsistema de mando de control de a bordo aplica automáticamente los frenos del tren.	Administrador de la infraestructura	El administrador de la infraestructura debe garantizar que los trenes que no estén dotados de un subsistema de mando de control a bordo activo no entren en la vía de que se trate. Definir un procedimiento para la gestión del tráfico.	Estimación explícita del riesgo	Sí	Controlado (exportado al administrador de la infraestructura) Véase, asimismo, la sección C.16.4.2. del Apéndice C
				Empresa ferroviaria	Garantizar la formación del maquinista para acceder a una zona provista de una ATP desde tierra	Estimación explícita del riesgo	Sí	Controlado (exportado a la empresa ferroviaria) Véase, asimismo, la sección C.16.4.2. del Apéndice C
5	Informe de riesgos y operabilidad tipo HAZOP RX	Velocidad máxima del tren establecida que se muestra al maquinista demasiado alta (Vmax)	La información mostrada en la interfaz del maquinista es controlada por el subsistema de mando de control de a bordo SIL 4, que aplica los frenos de emergencia en caso de discrepancia entre el valor mostrado y el valor esperado. En caso de incumplimiento de la autoridad de movimiento, el subsistema de mando de control de a bordo aplica los frenos de emergencia	Fabricante	Desarrollar un subsistema de mando de control de a bordo SIL 4	Estimación explícita del riesgo	Sí	Caso de seguridad que demuestre un subsistema de nivel SIL 4 evaluado por un evaluador independiente de la seguridad
6	Informe de riesgos y operabilidad tipo HAZOP RX	El tren sale sin interfaz maquinista-máquina	Pérdida de arquitectura redundante del subsistema de a bordo	Fabricante	Desarrollar un subsistema de mando de control de a bordo SIL 4	Estimación explícita del riesgo	Sí	Caso de seguridad que demuestre un subsistema de nivel SIL 4 evaluado por un evaluador independiente de la seguridad

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

Cuadro 7: Ejemplo de registro de peligros de un fabricante para un subsistema de mando y control a bordo.

N° del peligro	Origen	Descripción del peligro	Información adicional	Agente responsable	Medida de seguridad	Principio de aceptación del riesgo utilizado	Expor-tado	Estado
etc.								

C.16.4. Ejemplo de un registro de peligros para transmitir información a otros agentes

C.16.4.1. En esta sección se ofrece un ejemplo de registro de peligros para transferir a otros agentes los peligros identificados y medidas de seguridad asociadas que no puede aplicar el agente de que se trate. Véase el apartado [G 1] de la sección 4.1.1.
Este ejemplo es el mismo que el presentado en la sección C.16.3. del Apéndice C. La única diferencia estriba en que se suprimen todos los peligros internos y las medidas de seguridad que podría controlar el agente en cuestión.

C.16.4.2. La última columna del Cuadro 8 se usa para cumplir el requisito de la sección 4.2 del Reglamento MCS. Existen diferentes soluciones para lograrlo. Una de ellas podría consistir en hacer referencia a las evidencias utilizadas por el agente que recibe la información exportada en materia de seguridad. Otra podría consistir en celebrar una reunión entre los dos agentes para hallar conjuntamente una solución adecuada para controlar el/los riesgo(s) asociado(s). Los resultados de dicha reunión podrían recogerse en un documento acordado (por ejemplo, un acta de la reunión) al que pueda hacer referencia el agente que exporta la información relacionada con la seguridad para cerrar los peligros asociados en su registro de peligros.

Cuadro 8: Ejemplo de un registro de peligros para transmitir información relacionada con la seguridad a otros agentes.

N° del peligro	Origen del peligro		Descripción del peligro	Información adicional	Agente responsable	Medida de seguridad	Observaciones del receptor
	N° en el Cuadro 7	Otros					
1	N°1	Informe de riesgos y operabilidad tipo HAZOP RX	Velocidad máxima del tren establecida demasiado alta (Vmax)	Configuración específica incorrecta del subsistema de a bordo (personal de mantenimiento). Introducción de datos incorrectos a bordo (maquinista)	Empresa ferroviaria	• Definir un procedimiento para la aceptación de los datos de la configuración del subsistema de a bordo; • Definir un procedimiento operativo para el proceso de introducción de datos por el maquinista;	• Los datos de la configuración del subsistema de mando de control de a bordo dependen de las características físicas del material rodante. • Se aplican los márgenes de seguridad a estos datos en coordinación entre el administrador de la infraestructura y la empresa ferroviaria. • A continuación, estos datos se cargan en el subsistema de a bordo con arreglo al procedimiento del fabricante que corresponda

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

Cuadro 8: Ejemplo de un registro de peligros para transmitir información relacionada con la seguridad a otros agentes.

N° del peligro	Origen del peligro		Descripción del peligro	Información adicional	Agente responsable	Medida de seguridad	Observaciones del receptor
	N° en el Cuadro 7	Otros					
							durante la instalación, integración en el material rodante y aceptación del subsistema de mando de control. • Se forma y evalúa a los maquinistas siguiendo el procedimiento D_P. • Asimismo, el administrador de la infraestructura evalúa a los maquinistas con arreglo a las normas aplicables a la infraestructura del administrador de la infraestructura.
2	N°2	Informe de riesgos y operabilidad tipo HAZOP RX	Curvas de frenado (es decir, autoridad de movimiento) de la configuración del subsistema de a bordo demasiado permisivas	El procedimiento para establecer la configuración específica del subsistema de a bordo depende de: • los márgenes de seguridad adoptados para el sistema de frenado del tren; • el retraso de reacción del sistema de frenado del tren (éste depende directamente de la longitud del tren, en particular para los trenes de mercancías)	Empresa ferroviaria	• Especificar correctamente los requisitos del sistema en la definición del sistema; • Adoptar márgenes de seguridad suficientes para el sistema se frenado del tren de que se trate;	Véanse las observaciones relativas a la línea 1 más arriba.
3	N°3	Informe de riesgos y operabilidad tipo HAZOP RX	• Velocidad máxima del tren establecida demasiado alta (Vmax) • Curvas de frenado (es decir, autoridad de movimiento) de la configuración del subsistema de a bordo demasiado permisivas	Incapacidad para actualizar el diámetro de rueda del tren en la configuración específica del subsistema de a bordo (personal de mantenimiento).	Empresa ferroviaria	• Definir un procedimiento para la medición del diámetro de rueda del tren por el personal de mantenimiento; • Definir un procedimiento para actualizar regularmente el diámetro de rueda del tren en el subsistema de a bordo;	• El mantenimiento del subsistema de mando de control de a bordo se realiza de conformidad con el “Procedimiento de mantenimiento MP_Z”. • El diámetro de rueda del tren se actualiza en intervalos definidos de acuerdo al procedimiento P_W. • Pos lo que respecta al proceso de introducción de datos, se forma y evalúa a los maquinistas de acuerdo al “Procedimiento P_{DE}”.

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

Cuadro 8: Ejemplo de un registro de peligros para transmitir información relacionada con la seguridad a otros agentes.

N° del peligro	Origen del peligro		Descripción del peligro	Información adicional	Agente responsable	Medida de seguridad	Observaciones del receptor
	N° en el Cuadro 7	Otros					
4	N°4	Informe de riesgos y operabilidad tipo HAZOP RX	Entrada del tren a gran velocidad (160 km/h en caso de señal en tierra libre) en la vía sin subsistema a bordo activo y sin señalización en tierra	Podría controlarse únicamente mediante una labor de vigilancia del maquinista. El acceso a zona provista de una ATP desde tierra se basa en un procedimiento de reconocimiento por el maquinista antes de llegar al lugar de transición. En caso de ausencia de reconocimiento, el subsistema de mando de control de a bordo aplica automáticamente los frenos del tren..	Administrador de la infraestructura	El administrador de la infraestructura debe garantizar que los trenes que no estén dotados de un subsistema de mando de control a bordo activo no entren en la vía de que se trate. Definir un procedimiento para la gestión del tráfico.	La gestión del tráfico en la infraestructura del administrador de la infraestructura se rige por el conjunto de normas R_{TM}
					Empresa ferroviaria	Garantizar la formación del maquinista para acceder a una zona provista de una ATP desde tierra	• Se forma a los maquinistas a intervalos regulares siguiendo el procedimiento P_{IM_DP} del administrador de la infraestructura. • El administrador de la infraestructura también evalúa a los maquinistas con arreglo al conjunto de normas (S_R) aplicables a la infraestructura del administrador de la infraestructura.
etc.							

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

C.17. Ejemplo de una lista de peligros genéricos para la explotación ferroviaria

C.17.1. ROSA (Rail Optimisation Safety Analysis – Análisis de la optimización de la seguridad ferroviaria), un proyecto en el marco de la DEUFRAKO (cooperación franco-alemana), trató de establecer una lista de peligros genéricos y globales que cubriera la explotación normal de ferrocarriles. El objetivo y la dificultad consistían en definir estos peligros con un grado de detalle máximo, pero sin reflejar las características específicas de los ferrocarriles franceses y alemanes. La lista se estableció usando listas de peligros actualmente existentes de ambos países (SNCF y DB), siendo asimismo objeto de controles cruzados con listas de peligros de otros países. A pesar de que el objetivo declarado sea una lista global y genérica, la lista sólo se ofrece aquí a modo de ejemplo ilustrativo que podría servir de ayuda a los agentes cuando tienen que identificar peligros para un determinado proyecto. Se prevé que los peligros enumerados en esta lista deban, probablemente, refinarse o completarse para que reflejen cualquier característica específicas de un proyecto.

C.17.2. Los peligros que figuran en la lista posterior se denominan “peligros de punto de partida” (“starting point hazards” (SPH)), es decir, peligros a partir de los cuales podrían llevarse a cabo un análisis de consecuencia y un análisis causal a fin de determinar medidas de seguridad, barreras a la seguridad y requisitos de seguridad para controlar los peligros.

C.17.3. Lista de peligros del proyecto ROSA:

SPH 01	Determinación inicial incorrecta del límite de velocidad (relacionado con la infraestructura)
SPH 02	Determinación incorrecta del límite de velocidad (relacionado con el tren)
SPH 03	Determinación de distancia de frenado incorrecta / perfil de velocidad incorrecto / curvas de frenado incorrectas
SPH 04	Deceleración insuficiente (causas físicas)
SPH 05	Mando de velocidad / frenado incorrecto o inapropiado
SPH 06	Velocidad registrada incorrecta (velocidad del tren incorrecta)
SPH 07	Fallo en la comunicación del límite de velocidad
SPH 08	Tren a la deriva
SPH 09	Dirección de marcha incorrecta / movimiento intencionado hacia atrás - (combinación de SPH 08 y SPH 14)
SPH 10	Posición registrada absoluta / relativa incorrecta
SPH 11	Fallo en la detección de los trenes
SPH 12	Pérdida de integridad del tren
SPH 13	Posible ruta equivocada del tren
SPH 14	Fallo en la transmisión / comunicación del calendario / de la autoridad de movimiento
SPH 15	Fallo estructural de guiado
SPH 16	Componente de la aguja roto
SPH 17	Mando de la aguja equivocado
SPH 18	Estado de la aguja equivocado
SPH 19	Objeto del sistema en la vía/ en el espacio libre (excl. el balasto)
SPH 20	Objeto extraño en la vía/ en el espacio libre
SPH 21	Usuario del tráfico por carretera en el paso a nivel
SPH 22	Efecto estela sobre el balasto
SPH 23	Impacto de fuerzas aerodinámicas en el tren
SPH 24	Equipo, elemento o carga del tren contraviene el espacio libre del tren
SPH 25	Dimensión del espacio libre inadecuada para el tren (en tierra)
SPH 26	Incorrecta distribución de la carga
SPH 27	Rueda rota, eje roto

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

SPH 28	Eje, rueda o cojinete caliente
SPH 29	Fallo del bogie / de la suspensión o el amortiguador
SPH 30	Fallo del chasis del vehículo / de la caja del coche
SPH 31	Sobrepaso (aspecto relacionado con la seguridad)
SPH 32	Persona autorizada cruza la vía
SPH 33	Personal que trabaja en la vía
SPH 34	Persona no autorizada invade la vía (negligencia)
SPH 35	Persona cae del borde del andén a la vía
SPH 36	Efecto estela / persona demasiado cerca del borde del andén
SPH 37	Personal que trabaja cerca de la vía, por ejemplo, en la vía contigua
SPH 38	Persona abandona el tren intencionadamente (excl. el intercambio de pasajeros)
SPH 39	Persona cae por la puerta (lateral)
SPH 40	Persona cae por la puerta de la pared del extremo
SPH 41	Tren sale / circula con las puertas abiertas (espacio libre no infringido)
SPH 42	Persona cae en la zona del puente de servicio entre dos coches
SPH 43	Pasajero se asoma por la puerta
SPH 44	Pasajero se asoma por la ventana
SPH 45	Personal / personal auxiliar del tren se asoma por la puerta
SPH 46	Personal / personal auxiliar del tren se asoma por la ventana
SPH 47	Personal de maniobra en el vehículo se asoma desde el escalón
SPH 48	Persona cae o sube desde el andén al espacio existente entre el vehículo y el andén
SPH 49	Persona cae del tren o abandona el tren sin presencia de andén
SPH 50	Persona cae en la zona de la puerta en el intercambio de pasajeros
SPH 51	Las puertas del tren se cierran con una persona en la zona de la puerta
SPH 52	El tren se mueve durante el intercambio de pasajeros
SPH 53	Posibilidad de persona herida en el tren
SPH 54	Peligro de incendio / explosión (en el tren) – categoría de accidente, Consecuencia del SPH 55 y del SPH 56)
SPH 55	Temperatura inadecuada (en el tren)
SPH 56	Intoxicación / asfixia (en el tren)
SPH 57	Electrocución (en el tren)
SPH 58	Persona cae sobre el andén (excluido el intercambio de pasajeros)
SPH 59	Temperatura inadecuada (en el andén)
SPH 60	Intoxicación / asfixia (en el andén)
SPH 61	Electrocución (en el andén)

European Railway Agency ● Boulevard Harpignies, 160 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu