Agenzia Ferroviaria Europea

Raccolta di esempi di valutazioni del rischio e di alcuni possibili strumenti a supporto del regolamento sul metodo comune di sicurezza

Riferimento ERA:	ERA/GUI/02-2008/SAF
Versione ERA:	1.1
Data:	06/01/2009

Documento elaborato da	European Railway Agency Boulevard Harpignies, 160 BP 20392 F-59307 Valenciennes Cedex France
Tipo di documento:	Guida
Stato del documento:	Pubblico

	Nome	**Funzione**
Rilasciato da	Marcel VERSLYPE	Direttore esecutivo
Rivisto da	Anders LUNDSTRÖM Thierry BREYNE	Capo unità, Sicurezza Capo Settore di valutazione della sicurezza
Scritto da (autore)	Dragan JOVICIC	Unità sicurezza – Responsabile del progetto

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

INFORMAZIONI SUL DOCUMENTO

Registro delle modifiche

Tabella 1: Stato del documento.

Data versione	Autore(i)	Numero sezione	Descrizione della modifica
Titolo e struttura del vecchio documento: *"Guida all'uso della Raccomandazione sulla prima serie di metodi comuni di sicurezza"*			
Guida Versione 0.1 15/02/2007	Dragan JOVICIC	Tutte	Prima versione della "guida all'uso" relativa alla versione 1.0 della prima serie di raccomandazioni sul metodo comune di sicurezza". È anche la prima versione del documento trasmesso al gruppo di lavoro sul metodo comune di sicurezza per una revisione formale.
Guida Versione 0.2 07/06/2007	Dragan JOVICIC	Tutte	Riorganizzazione del documento per adeguarlo alla struttura della versione 4.0 della raccomandazione sul metodo comune di sicurezza. Aggiornamento vs. Procedimento di revisione formale da parte del gruppo di lavoro sul metodo comune di sicurezza sulla versione 1.0 della raccomandazione.
		Tutte	Aggiornamento del documento con informazioni aggiuntive raccolte durante le riunioni interne dell'ERA, nonché con le richieste fatte dal gruppo ristretto e dal gruppo di lavoro sul metodo comune di sicurezza di sviluppare nuovi punti.
		Figura 1	Modifica della figura che rappresenta il "quadro di gestione del rischio per la prima serie di metodi di sicurezza comune" conformemente sia alle osservazioni della revisione sia alla terminologia ISO.
Guida Versione 0.3 20/07/2007	Dragan JOVICIC	Appendici	Riorganizzazione delle appendici esistenti e creazione di nuove. Nuova appendice per riunire tutti i diagrammi che illustrano e facilitano la lettura e la comprensione della Guida;
		Tutte le sezioni	Documento aggiornato al fine di: • sviluppare il più possibile le sezioni esistenti; • sviluppare ulteriormente il significato di "dimostrazione della conformità del sistema ai requisiti di sicurezza"; • collegarsi con il ciclo a V delle norme CENELEC (cioè Figura 8 e Figura 10 della EN 50 126); • sviluppare ulteriormente la necessità di collaborazione e coordinamento fra i diversi operatori del settore ferroviario le cui attività possono avere un impatto sulla sicurezza del sistema; • chiarire i documenti (p.es. *hazard log* e *safety case*) atti a dimostrare agli organismi di valutazione la corretta applicazione del procedimento di valutazione del rischio del metodo comune di sicurezza; Documento aggiornato anche in base a una prima revisione interna dell'Agenzia.
Guida Versione 0.4 16/11/2007	Dragan JOVICIC	Tutte le sezioni	Documento aggiornato seguendo il Procedimento di revisione formale in base alle osservazioni ricevute sulla versione 0.3 dai seguenti membri del gruppo di lavoro sul metodo comune di sicurezza o organismi, e concordate con loro telefonicamente: • NSA belga, spagnola, finlandese, norvegese, francese e danese; • SIEMENS (membro dell'UNIFE); • Gestore dell'infrastruttura norvegese (Jernbaneverket – Membro EIM);
Guida Versione 0.5	Dragan JOVICIC	Tutte le sezioni	Documento aggiornato in base alle osservazioni ricevute sulla versione 0.3 dai seguenti membri del gruppo di lavoro sul metodo comune di sicurezza o organismi, e concordate con loro telefonicamente:

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

Tabella 1: Stato del documento.

Data versione	Autore(i)	Numero sezione	Descrizione della modifica
27/02/2008			• CER • NSA olandese
		Tutte le sezioni	Documento aggiornato conformemente alla versione firmata della raccomandazione sul metodo comune di sicurezza. Documento aggiornato in base alle osservazioni della revisione interna dell'Agenzia presentate da Christophe CASSIR e Marcus ANDERSSON
		Tutte le sezioni Appendici	Rinumerazione completa dei paragrafi del documento in base alla raccomandazione Inserimento di esempi di applicazione della raccomandazione sul metodo comune di sicurezza.
Titolo e struttura del nuovo documento: *"Raccolta di esempi di valutazioni del rischio e di alcuni possibili strumenti a supporto del regolamento sul metodo comune di sicurezza"*			
Guida Versione 0.1 23/05/2008	Dragan JOVICIC	Tutte	Prima versione del documento derivante dalla divisione della "guida all'uso" versione 0.5 in due documenti complementari.
Guida Versione 02 03/09/2008	Dragan JOVICIC	Tutte	Aggiornamento del documento conformemente a: • Regolamento sul metodo comune di sicurezza della Commissione europea {Ref. 3}; • osservazioni del workshop del 1º luglio 2008 con membri del RISC (Railway Interoperability and Safety Committee) [Comitato sull'interoperabilità e la sicurezza ferroviaria]; • le osservazioni fatte dai membri del gruppo di lavoro sul metodo comune di sicurezza (NSA norvegese, finlandese, britannica, francese, CER, EIM, Jens BRABAND [UNIFE] e Stéphane ROMEI [UNIFE]
Guida Versione 1.0 10/12/2008	Dragan JOVICIC	Tutte	Aggiornamento del documento conformemente al regolamento della Commissione europea sull'adozione di un metodo di sicurezza comune sulla valutazione del rischio e la valutazione {Ref. 3} adottato dal RISC (Railway Interoperability and Safety Committee) in occasione dell'assemblea plenaria del 25 novembre 2008
Guida Versione 1.1 06/01/2009	Dragan JOVICIC	Tutte	Documento aggiornato in base alle osservazioni fatte sul regolamento sul metodo comune di sicurezza dai servizi giuridico e linguistico della Commissione 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

Indice

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

Elenco di figure

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

Elenco di tabelle

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. INTRODUZIONE

0.1. Campo di applicazione

0.1.1. L'obiettivo del presente documento è quello di offrire un ulteriore chiarimento sul "regolamento della Commissione relativo all'adozione di un metodo comune di determinazione e di valutazione dei rischi di cui all'articolo 6, paragrafo 3, lettera a), della direttiva 2004/49/CE del Parlamento Europeo e del Consiglio" {Ref. 3}. Tale regolamento sarà denominato in seguito "Regolamento sul metodo comune di sicurezza".

0.1.2. Il documento non è legalmente vincolante e il suo contenuto non deve essere interpretato come l'unico modo per soddisfare i requisiti del metodo comune di sicurezza. Esso mira a integrare la guida all'applicazione del regolamento sul metodo comune di sicurezza {Ref. 4} su come poter utilizzare e applicare il processo descritto nel regolamento sul metodo comune di sicurezza. Inoltre, fornisce informazioni pratiche senza imporre in alcun modo procedure da seguire obbligatoriamente e senza stabilire alcuna prassi vincolante dal punto di vista giuridico. Tali informazioni, infatti, possono essere utili a tutti gli operatori interessati [(1)] le cui attività possono avere un impatto sulla sicurezza dei sistemi ferroviari e che, direttamente o indirettamente, devono applicare il regolamento sul metodo comune di sicurezza. Il documento illustra esempi di valutazioni del rischio ed offre alcuni strumenti possibili a supporto dell'applicazione del metodo comune di sicurezza. Tali esempi sono illustrati esclusivamente a titolo di consiglio e aiuto. I soggetti interessati possono adottare metodi alternativi o continuare ad usare i propri metodi e strumenti di conformità al metodo comune di sicurezza qualora li ritengano più adatti.
Inoltre, gli esempi e le informazioni supplementari forniti in questo documento non sono esaustivi e non contemplano tutte le possibili situazioni in cui si propongono modifiche significative; pertanto, il documento può essere considerato meramente informativo.

0.1.3. Questo documento informativo deve essere letto esclusivamente come ausilio supplementare per l'applicazione del regolamento sul metodo comune di sicurezza. Per agevolare maggiormente l'applicazione del metodo comune di sicurezza è opportuno leggere il documento unitamente al regolamento sul metodo comune di sicurezza {Ref. 3} e alla relativa guida {Ref. 4}; ad ogni modo, questo documento non sostituisce il regolamento sul metodo comune di sicurezza.

0.1.4. Il documento è stato elaborato dall'Agenzia Ferroviaria Europea (ERA) con il supporto degli esperti delle associazioni ferroviarie e delle autorità nazionali di sicurezza tramite i gruppi di lavoro sul metodo comune di sicurezza. Il documento presenta una raccolta elaborata delle idee e delle informazioni raccolte dall'Agenzia durante le riunioni con il gruppo di lavoro ed i gruppi ristretti (task-force) sul metodo comune di sicurezza.. All'occorrenza, l'ERA revisionerà e aggiornerà il documento affinché rifletta gli sviluppi delle norme europee, le modifiche apportate al regolamento sul metodo comune di sicurezza in materia di valutazione del rischio e i possibili feedback derivanti dall'esperienza fatta sull'uso del regolamento sul metodo comune di sicurezza. Poiché al momento in cui si scrive non è possibile fornire un calendario del processo di revisione, il lettore deve rivolgersi

(1) *I soggetti interessati sono gli enti aggiudicatori definiti nell'articolo 2, comma r, della direttiva 2008/57/CE sull'interoperabilità del sistema ferroviario comunitario, o i produttori, definiti nel regolamento come "proponenti", oppure i loro fornitori di beni e servizi.*

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

direttamente all'Agenzia ferroviaria europea per richiedere l'ultima edizione disponibile del documento.

0.2. Fuori dall'ambito di applicazione

0.2.1. Il presente documento non fornisce informazioni su come organizzare, gestire o progettare (e produrre) un sistema ferroviario o parti di esso. Né definisce gli accordi contrattuali e i patti esistenti fra alcuni dei soggetti interessati per l'applicazione del procedimento di gestione del rischio. Gli specifici accordi contrattuali relativi a un progetto non rientrano nell'ambito di applicazione né del regolamento sul metodo comune di sicurezza né della relativa guida e del presente documento.

0.2.2. Sebbene non rientrino nell'ambito di applicazione di questo documento, gli accordi raggiunti dai relativi operatori interessati possono essere annotati nei relativi contratti all'inizio del progetto, fatte salve le disposizioni del metodo comune di sicurezza. Essi possono riguardare, per esempio:

(1) i costi relativi alla gestione di rischi che interessano la sicurezza nei punti d'interazione fra i diversi operatori;
(2) i costi relativi al trasferimento degli eventi pericolosi e delle misure di sicurezza connesse fra i diversi operatori non ancora noti all'inizio del progetto;
(3) le modalità di gestione dei conflitti che potrebbero sorgere durante il progetto;
(4) ecc.

Qualora sorgano disaccordi o conflitti fra il proponente e i suoi subappaltatori durante lo sviluppo del progetto, si può ricorrere ai relativi contratti che saranno di aiuto per la soluzione di qualsiasi problema di questo tipo.

0.3. Principio del presente documento

0.3.1. Sebbene questo documento possa sembrare un documento a sé stante a scopo informativo, esso non sostituisce il regolamento sul metodo comune di sicurezza {Ref. 3}. Per agevolarne la consultazione, il documento riporta ogni articolo del regolamento sul metodo comune di sicurezza. All'occorrenza, il relativo articolo è prima spiegato nella guida all'applicazione del regolamento sul metodo comune di sicurezza {Ref. 4}. I paragrafi successivi forniscono ulteriori informazioni, laddove si ritiene necessario, volte a migliorare la comprensione del regolamento sul metodo comune di sicurezza.

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 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. Per agevolare il lettore la struttura di questo documento rispecchia quella del regolamento sul metodo comune di sicurezza e della relativa guida.

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. Descrizione del documento

0.4.1. Il documento è diviso nelle seguenti parti:

a) il capitolo a) che definisce l'ambito di applicazione del documento e fornisce l'elenco dei documenti di riferimento;
b) Gli Allegati I e II forniscono informazioni supplementari per le corrispondenti sezioni del regolamento {Ref. 3} e della relativa guida {Ref. 4};
c) nuove appendici sviluppano ulteriormente alcuni aspetti e forniscono degli esempi.

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

0.5. Documenti di riferimento

Tabella 2: Tabella di documenti di riferimento.

{N. Rif.}	Titolo	Riferimento	Versione
{Ref. 1}	Direttiva 2004/49/CE del parlamento europeo e del consiglio del 29 aprile 2004 relativa alla sicurezza delle ferrovie comunitarie e recante modifica della direttiva 95/18/CE del Consiglio relativa alle licenze delle imprese ferroviarie e della direttiva 2001/14/CE relativa alla ripartizione della capacità di infrastruttura ferroviaria, all'imposizione dei diritti per l'utilizzo dell'infrastruttura ferroviaria e alla certificazione di sicurezza (direttiva sulla sicurezza delle ferrovie)	2004/49/CE GU L 164, del 30.4.2004, pag. 44, corretta dalla GU L 220, del 21.6.2004, pag. 16.	-
{Ref. 2}	Direttiva 2008/57/CE del Parlamento europeo e del Consiglio, del 17 giugno 2008 relativa all'interoperabilità del sistema ferroviario comunitario	2008/57/CE GU L 191, del 18/7/2008, pag.1.	-
{Ref. 3}	Regolamento della Commissione (CE) N° ,,,/… del […] relativo all'adozione di un metodo comune di determinazione e di valutazione dei rischi di cui all'articolo 6, paragrafo 3, lettera a), della direttiva 2004/49/CE del Parlamento Europeo e del Consiglio	xxxx/yy/EC	votato dal RISC il 25/11/2008
{Ref. 4}	Guida all'applicazione del regolamento della Commissione relativo all'adozione di un metodo comune di determinazione e di valutazione dei rischi di cui all'articolo 6, paragrafo 3, lettera a), della direttiva 2004/49/CE del Parlamento Europeo e del Consiglio	ERA/GUI/01-2008/SAF	1.0
{Ref. 5}	Direttiva 2008/57/CE del Parlamento europeo e del Consiglio, del 17 giugno 2008 relativa all'interoperabilità del sistema ferroviario comunitario	2008/57/CE GU L 191, del 18.7.2008, pag. 1.	-
{Ref. 6}	Sistema di gestione della sicurezza - Criteri di valutazione per le imprese ferroviarie e i gestori dell'infrastruttura	Criteri di valutazione dei sistemi di gestione della sicurezza Parte A Certificati e autorizzazioni di sicurezza	31/05/2007
{Ref. 7}	Applicazioni ferroviarie – Sistemi di comunicazione, segnalamento ed elaborazione – Sistemi elettronici di segnalamento relativi alla sicurezza	EN 50129	Febbraio 2003
{Ref. 8}	Applicazioni ferroviarie – La specificazione e la dimostrazione di Affidabilità, Disponibilità, Manutenibilità e Sicurezza (RAMS) – Parte 1: Requisiti di base e processo generico	EN 50126-1	Settembre 2006
{Ref. 9}	Applicazioni ferroviarie – La specificazione e la dimostrazione di Affidabilità, Disponibilità, Manutenibilità e Sicurezza (RAMS) Parte 2: Guida all'applicazione della norma EN 50126-1 per la sicurezza	EN 50126-2 (orientamento)	Progetto finale (agosto 2006)
{Ref. 10}	Orientamenti generici per il calcolo del rischio inerente al trasporto di merci pericolose per ferrovia	OTIF guideline approved by the RID Committee of experts	24 novembre 2005.
{Ref. 11}	Criterio di accettazione del rischio per sistemi tecnici	Comunicazione 01/08	1.1 (25/01/2008)
{Ref. 12}	Unità sicurezza ERA: Studio di fattibilità – "Ripartizione di obiettivi di sicurezza (a sottosistemi oggetti di STI) e consolidamento della STI da un punto di vista della sicurezza" WP1.1 – Valutazione della fattibilità per ripartire gli obiettivi comuni di sicurezza	WP1.1	1.0

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

Tabella 2: Tabella di documenti di riferimento.

{N. Rif.}	Titolo	Riferimento	Versione
{Ref. 13}	"Applicazioni ferroviarie — Sistema di classificazione per i veicoli ferroviari — Parte 4: EN 0015380 Parte 4: Gruppi di funzioni".	EN 0015380 Parte 4	

0.6. Definizioni, termini e abbreviazioni standard

0.6.1. Le definizioni, i termini e le abbreviazioni generali utilizzate nel presente documento figurano in un dizionario standard.

0.6.2. Le definizioni, i termini e le abbreviazioni nuove di questa guida sono definite nei paragrafi successivi.

0.7. Definizioni specifiche

0.7.1. See Articolo 3

0.8. Termini e abbreviazioni specifici

0.8.1. Questo paragrafo definisce le abbreviazioni e i termini specifici nuovi utilizzati con frequenza nel presente documento.

Tabella 3: Tabella dei termini.

Termine	Definizione
Agenzia	L'Agenzia ferroviaria europea (ERA)
Guida	la "guida all'applicazione del Regolamento della Commissione (CE) N° ,,,/… del […] relativo all'adozione di un metodo comune di determinazione e di valutazione dei rischi di cui all'articolo 6, paragrafo 3, lettera a), della direttiva 2004/49/CE del Parlamento Europeo e del Consiglio"
Regolamento sul metodo comune di sicurezza	il "Regolamento della Commissione (CE) N° ,,,/… del […] relativo all'adozione di un metodo comune di determinazione e di valutazione dei rischi di cui all'articolo 6, paragrafo 3, lettera a), della direttiva 2004/49/CE del Parlamento Europeo e del Consiglio" {Ref. 3}

Tabella 4: Tabella delle abbreviazioni.

Abbreviazione	Significato
CCS	Controllo-comando e segnalamento *[Control Command and Signalling]*
CSM	Metodo(i) comune(i) di sicurezza [*Common Safety Method(s)*]
CST	Obiettivi comuni di sicurezza [*Common Safety Targets*]
CE	Commissione europea [*European Commission*]
ERA	Agenzia ferroviaria europea [*European Railway Agency]*
IM	Gestore(i) dell'infrastruttura [*Infrastructure Manager(s)*]
ISA	Valutatore indipendente della sicurezza [*Independent Safety Assessor*]
OTIF	Organizzazione intergovernativa per i trasporti internazionali per ferrovia

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

Tabella 4: Tabella delle abbreviazioni.

Abbreviazione	**Significato**
	[Intergovernmental Organisation for International Carriage by Rail]
SM	Stato membro [*Member State*]
ON	Organismo notificato [*Notified Body*]
NSA	Autorità nazionale di sicurezza [*National Safety Authority*]
QMP	Procedimento di gestione della qualità *[Quality Management Process]*
QMS	Sistema di gestione qualità *[Quality Management System]*
RISC	Comitato per l'interoperabilità e la sicurezza ferroviaria *[Railway Interoperability and Safety Committee]*
RU	Impresa(i) ferroviaria(e) *[Railway Undertaking(s)]*
SMP	Procedimento di gestione della sicurezza *[Safety Management Process]*
SMS	Sistema di gestione della sicurezza *[Safety Management System]*
SRT	Sicurezza nelle gallerie ferroviarie *[Safety in Railway Tunnels]*
TBC	Da completare *[To be completed]*
STI	Specifiche tecniche di interoperabilità *[Technical Specifications for Interoperability]*

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

SPIEGAZIONE DEGLI ARTICOLI DEL REGOLAMENTO SUL METODO COMUNE DI SICUREZZA

Articolo 1. Finalità

Articolo 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] Non si ritengono necessarie ulteriori spiegazioni.

Articolo 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] Non si ritengono necessarie ulteriori spiegazioni.

Articolo 2. Ambito di applicazione

Articolo 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] Il metodo comune di sicurezza riguarda l'intero sistema ferroviario e prevede la valutazione delle seguenti modifiche ai sistemi ferroviari, qualora esse siano ritenute significative dall'applicazione dell'Articolo 4:

(a) costruzione di nuove linee o modifiche alle linee esistenti,

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

(b) introduzione di sistemi tecnici nuovi e/o modificati;
(c) modifiche operative (ad esempio norme operative nuove o modificate e procedure di manutenzione);
(d) modifiche alla struttura organizzativa di RU/IM.

Nel metodo comune di sicurezza, il termine "sistema" si riferisce a tutti gli aspetti di un sistema compresi, fra gli altri, il suo sviluppo, il funzionamento, la manutenzione ecc., fino allo smantellamento o allo smaltimento

[G 2] Il metodo comune di sicurezza copre le modifiche significative di:

(a) sistemi "piccoli e semplici" che potrebbero essere composti da pochi sottosistemi o elementi tecnici e,
(b) sistemi "grandi e più complessi" (p.es. che possono comprendere stazioni e gallerie).

Articolo 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] Per esempio, conformemente alla direttiva sulla sicurezza delle ferrovie {Ref. 1} e alla direttiva sull'interoperabilità ferroviaria {Ref. 2}, un nuovo tipo di materiale rotabile per una linea ad alta velocità deve essere conforme alla STI sul materiale rotabile ad alta velocità. Sebbene la STI contempli la maggior parte dei sistemi sottoposti a valutazione, non comprende la questione chiave dei fattori umani legati alla cabina del macchinista. Di conseguenza, al fine di garantire che siano identificati e controllati adeguatamente tutti gli eventi pericolosi ragionevolmente prevedibili legati al fattore umano (vale a dire ai punti d'interazione fra il macchinista, il materiale rotabile e il resto del sistema ferroviario), si deve applicare il procedimento del metodo comune di sicurezza.

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

Articolo 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] Non si ritengono necessarie ulteriori spiegazioni.

Articolo 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] Non si ritengono necessarie ulteriori spiegazioni.

Articolo 3. Definizioni

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 Articolo 5 (2);

(9) 'safety requirements' means the safety characteristics (qualitative or quantitative) of a

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

system and its operation (including operational rules) necessary in order to meet legal or company safety targets;

(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;

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

(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.

[G 1] Non si ritengono necessarie ulteriori spiegazioni.

Articolo 4. Modifiche significative

Articolo 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] Nel caso in cui non vi sia una norma nazionale notificata, la responsabilità della decisione è del proponente. L'entità della modifica si basa su un parere esperto. Per esempio, se la modifica desiderata in un sistema esistente è complessa, può essere valutata come significativa se il rischio di influire su funzioni esistenti[6] del sistema è elevato, sebbene la modifica in sé non abbia necessariamente un nesso molto stretto con la sicurezza.

Articolo 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

(4) *OJ L 235, 17.9.1996, p. 6.*

(5) *OJ L 110 , 20.4.2001, p. 1.*

(6) *Poiché le funzioni di un sistema non sempre sono indipendenti, la modifica di talune funzioni può anche influire su altre funzioni del sistema anche se quest'ultime potrebbero non sembrare interessate dalla modifica.*

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

significant.

The proposer shall keep adequate documentation to justify his decision.

[G 1] **Esempio di modifiche di scarsa entità:** dopo la messa in servizio del sistema, aumentare per una volta la velocità massima della linea di 5 km/h potrebbe non essere significativo. Ad ogni modo, se si continua ad aumentare la velocità massima della linea, ogni volta di 5 km/h, la somma delle modifiche successive (valutate singolarmente come modifiche non significative) potrebbe diventare una modifica significativa rispetto ai requisiti di sicurezza del sistema iniziali.

[G 2] Al fine di valutare se una serie di diverse modifiche successive (non significative) è significativa quando viene considerata nell'insieme, si devono valutare tutti gli eventi pericolosi e i rischi connessi a ciascuna modifica. La serie di modifiche presa in considerazione può essere considerata non significativa se il rischio risultante è ampiamente accettabile.

[G 3] Dal lavoro svolto dall'Agenzia sulle modifiche significative è emerso che:

(a) non è possibile identificare soglie o norme armonizzate partendo dalle quali, per una determinata modifica, si può prendere la decisione sull'entità della stessa e;
(b) non è possibile fornire un elenco esaustivo di modifiche significative;
(c) la decisione non può essere valida per tutti i proponenti e tutte le condizioni tecniche, operative, organizzative ed ambientali

È quindi essenziale lasciare la responsabilità della decisione ai proponenti che sono responsabili, ai sensi dell'articolo 4, paragrafo 3, della direttiva sulla sicurezza delle ferrovie {Ref. 1}, del funzionamento sicuro e del controllo dei rischi relativi alla parte del sistema di cui si occupano.

[G 4] Per aiutare il proponente, nella sezione C.2. dell'appendice C è illustrato un esempio di "valutazione ed uso di criteri".

[G 5] Il metodo comune di sicurezza non si deve applicare se una modifica che interessa la sicurezza non è considerata significativa. Ciò, però, non significa che non si debba fare niente. Il proponente deve comunque eseguire un qualche tipo di analisi (preliminare) dei rischi per decidere se la modifica è significativa o meno. Tali analisi dei rischi, nonché qualsiasi giustificazione e argomentazione, devono essere documentate al fine di consentire alla NSA di eseguire i dovuti controlli. L'organismo di valutazione non deve eseguire la valutazione indipendente dell'entità di una modifica e della decisione che considera una modifica come non significativa.

Articolo 5. Procedimento di gestione dei rischi

Articolo 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.

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] Non si ritengono necessarie ulteriori spiegazioni.

Articolo 5 (2)

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

[G 1] Non si ritengono necessarie ulteriori spiegazioni.

Articolo 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] Non si ritengono necessarie ulteriori spiegazioni.

Articolo 6. Valutazione indipendente

Articolo 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] Il livello di indipendenza richiesto, necessario all'organismo di valutazione, dipende dal livello di sicurezza richiesto per il sistema sottoposto a valutazione. In attesa dell'armonizzazione di questo argomento, le buona pratica in materia si possono trovare nella norma IEC61508-1:2001 Clausola 8 o nella sezione 5.3.9. della norma EN 50 129 {Ref. 7}. Il livello di indipendenza dipende sia dalla gravità delle conseguenze dell'evento pericoloso sull'apparecchiatura sia dalla sua novità. La sezione 9.7.2 della norma EN 50 126-2 e la norma EN 50129 definiscono il livello di indipendenza per i sistemi di segnalamento. In linea di massima, queste indicazioni potrebbero essere utilizzate anche per altri sistemi.

[G 2] L'Agenzia sta ancora lavorando alla definizione dei ruoli e delle responsabilità dei diversi organismi di valutazione (NSA, ON ed ISA) nonché ai punti d'interazione necessarie fra loro. In questo modo si definirà (se possibile) quale di questi organismi di valutazione dovrà eseguire determinati compiti, quali compiti dovrà eseguire e secondo quali modalità. Alla fine sarà quindi possibile definire come:

(a) verificare, in base alle prove fornite, che la gestione del rischio e i procedimenti di valutazione del rischio previsti dal metodo comune di sicurezza siano applicati correttamente e;
(b) sostenere il proponente nella sua decisione di accettare la modifica significativa all'interno del sistema sottoposto a valutazione.

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

Articolo 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] Il lavoro svolto dall'agenzia sui ruoli e sulle responsabilità degli organismi di valutazione fornirà ulteriori informazioni.

Articolo 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] Non si ritengono necessarie ulteriori spiegazioni.

Articolo 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] Non si ritengono necessarie ulteriori spiegazioni.

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

Articolo 7. Relazioni di valutazione della sicurezza

Articolo 7 (1)

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

[G 1] Non si ritengono necessarie ulteriori spiegazioni.

Articolo 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] Non si ritengono necessarie ulteriori spiegazioni.

Articolo 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] Non si ritengono necessarie ulteriori spiegazioni.

Articolo 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] Questo principio di reciproco riconoscimento è già accettato dalle norme CENELEC: cfr. la sezione 5.5.2 della norma EN 50 129 e la sezione 5.9 della norma EN 50 126-2. Nelle norme CENELEC, il riconoscimento transnazionale o principio del reciproco riconoscimento è applicato dai proponenti o dai valutatori indipendenti della sicurezza a prodotti e applicazioni generici(7), a condizione che la valutazione e la dimostrazione di sicurezza siano eseguite conformemente ai requisiti delle norme CENELEC.

(7) *Consultare il punto [G 5] della sezione 1.1.5 e le note (9) e (10) a pagina 31, nonché la, di questo documento, per un'ulteriore spiegazione della definizione di "prodotto generico e applicazione generica" e principi inerenti.*

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] Il reciproco riconoscimento deve essere applicato anche per l'accettazione di sistemi nuovi o modificati, se la loro valutazione del rischio e la dimostrazione di conformità del sistema ai requisiti di sicurezza vengono effettuate in linea con le disposizioni del regolamento sul metodo comune di sicurezza {Ref. 3}

Articolo 8. Gestione della riduzione dei rischi/controlli interni ed esterni

Articolo 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] Non si ritengono necessarie ulteriori spiegazioni.

Articolo 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] Non si ritengono necessarie ulteriori spiegazioni.

Articolo 9. Feedback e progresso tecnico

Articolo 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] Non si ritengono necessarie ulteriori spiegazioni.

Articolo 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] Non si ritengono necessarie ulteriori spiegazioni.

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

Articolo 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] Non si ritengono necessarie ulteriori spiegazioni.

Articolo 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 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] Non si ritengono necessarie ulteriori spiegazioni.

Articolo 10. Entrata in vigore

Articolo 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] Non si ritengono necessarie ulteriori spiegazioni.

Articolo 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] Non si ritengono necessarie ulteriori spiegazioni.

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

ALLEGATO I – SPIEGAZIONE DEL PROCEDIMENTO NEL REGOLAMENTO SUL METODO COMUNE DI SICUREZZA

1. PRINCIPI GENERALI DEL PROCEDIMENTO DI GESTIONE DEI RISCHI

1.1. Principi e obblighi generali

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 2] Il grafico di gestione del rischio per il metodo comune di sicurezza e il relativo procedimento di valutazione del rischio sono illustrati nella Figura 1. Nei casi ritenuti necessari, ogni casella/attività di questa figura è descritto più dettagliatamente in una specifica sezione di questo documento.

[G 3] Il CENELEC consiglia di descrivere i procedimenti di gestione e valutazione del rischio in un piano di sicurezza. Se, però, questa soluzione non dovesse essere pratica per il progetto, la descrizione in questione può essere acclusa a un qualsiasi altro documento pertinente. Cfr. la sezione 1.1.6.

[G 4] Il procedimento di valutazione del rischio inizia con una definizione preliminare del sistema. Durante lo sviluppo del progetto, la definizione preliminare del sistema viene aggiornata progressivamente per poi essere sostituita dalla definizione del sistema. Nel caso non vi sia una definizione preliminare del sistema, per realizzare la valutazione del rischio si usa la definizione ufficiale del sistema. In questo caso, però, è utile che tutti gli operatori interessati dalla modifica significativa si riuniscano all'inizio del progetto al fine di:

(a) concordare i principi globali del sistema, le sue funzioni ecc. In linea di massima, tutto ciò si potrebbe descrivere in una definizione preliminare del sistema;
(b) concordare l'organizzazione del progetto;
(c) concordare la condivisione dei ruoli e delle responsabilità fra i diversi operatori già coinvolti, compresi NSA, ON ed ISA, ove opportuno.

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

Un coordinamento di questo tipo, durante la definizione preliminare del sistema, offre al proponente, ai subappaltatori, alla NSA, agli ON e agli ISA, se opportuno, la possibilità di concordare in una fase iniziale i codici di buona pratica o i sistemi di riferimento accettabili da poter utilizzare nell'ambito del progetto

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

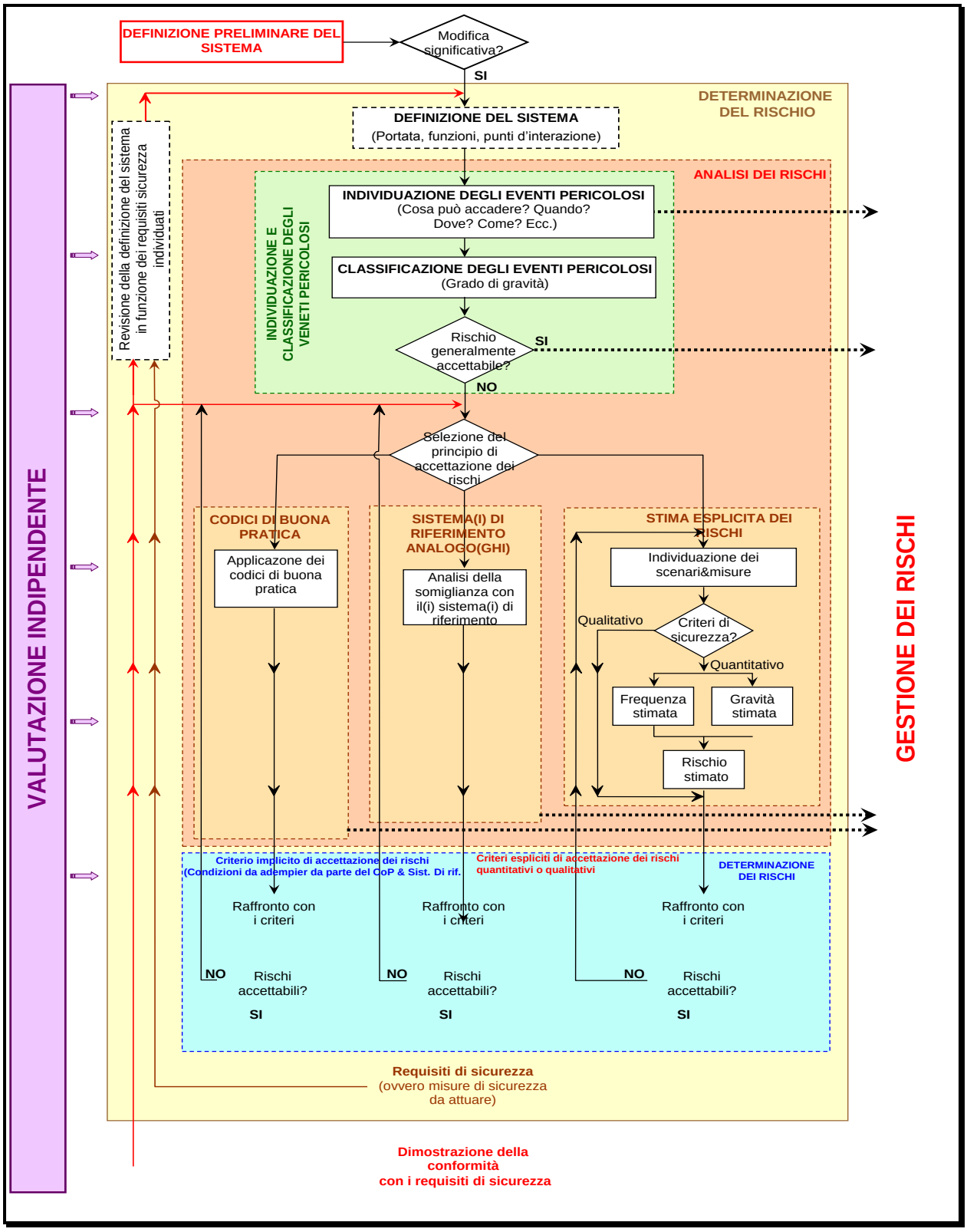

Figura 1 : Quadro di gestione del rischio nel regolamento sul metodo comune di sicurezza {Ref. 3}.

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

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] Il sistema di gestione della sicurezza (SMS) dell'impresa ferroviaria e del gestore dell'infrastruttura illustra il procedimento e le procedure che:

(a) controllano che il sistema continui ad essere sicuro durante l'intero ciclo di vita (p.es. durante il funzionamento e la manutenzione);
(b) garantiscono lo smantellamento sicuro o la sostituzione del sistema in questione.

Questo procedimento non fa parte del metodo comune di sicurezza sulla valutazione del rischio

[G 2] Per applicare il metodo comune di sicurezza è necessario che tutte le parti coinvolte siano competenti (vale a dire che abbiano l'abilità, la conoscenza e l'esperienza adeguate). All'interno delle imprese del settore ferroviario vi è un costante bisogno di gestire la competenza:

(a) per i gestori dell'infrastruttura e le imprese ferroviarie questo aspetto è coperto dal loro sistema di gestione della sicurezza (SMS) in virtù dell'allegato III, paragrafo 2, lettera e, della direttiva sulla sicurezza delle ferrovie {Ref. 1};
(b) per quanto riguarda gli altri operatori le cui attività possono avere ripercussioni sul sistema ferroviario, sebbene il sistema di gestione della sicurezza non sia obbligatorio, in generale, per lo meno a livello di progetto (cfr. punto [G 1] nella sezione 5.1.), dispongono di un procedimento di gestione della qualità (QMP) e/o di un procedimento di gestione della sicurezza (SMP) che copre questo requisito.

[G 3] Le seguenti sezioni della norma CENELEC EN 50 126-1 {Ref. 8} illustrano delle linee guide sulla competenza:

(a) ai sensi del paragrafo 5.3.5., lettera b: *"tutto il personale con responsabilità all'interno del" "procedimento di gestione"* del rischio deve essere *"competente per adempiere a tali responsabilità"*;
(b) § 5.3.5., lettera d: i requisiti della gestione e della valutazione del rischio devono essere *"attuati all'interno di processi aziendali sostenuti da un sistema di gestione della qualità (QMS) conforme ai requisiti EN ISO 9001, EN ISO 9002 o EN ISO 9003 adatti al sistema sottoposto a* valutazione*"*. Un esempio di aspetti controllati dal sistema di gestione della qualità è illustrato nella sezione 5.2. della norma EN 50 129 {Ref. 7}.

Esse contemplano le attività di assicurazione di qualità, nonché la competenza e la formazione per il personale/le persone, necessarie per sostenere il procedimento previsto dal metodo comune di sicurezza.

[G 4] Molto spesso il procedimento di valutazione del rischio è seguito da un organismo di valutazione fin dall'inizio del progetto, ma a meno che non sia imposto da una legge nazionale dello Stato membro in questione, il coinvolgimento dell'organismo di valutazione in una fase così iniziale non è obbligatorio, sebbene sia consigliabile. Il parere dell'organismo di valutazione indipendente potrebbe essere utile prima di passare da una fase all'altra della valutazione del rischio. Consultare l'Articolo 6 per maggiori dettagli sulla valutazione indipendente

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

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

[G 1] Non si ritengono necessarie ulteriori spiegazioni.

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 rappresenta il rapporto fra il metodo comune di sicurezza e i "sistemi di gestione della sicurezza e i procedimenti di valutazione del rischio".

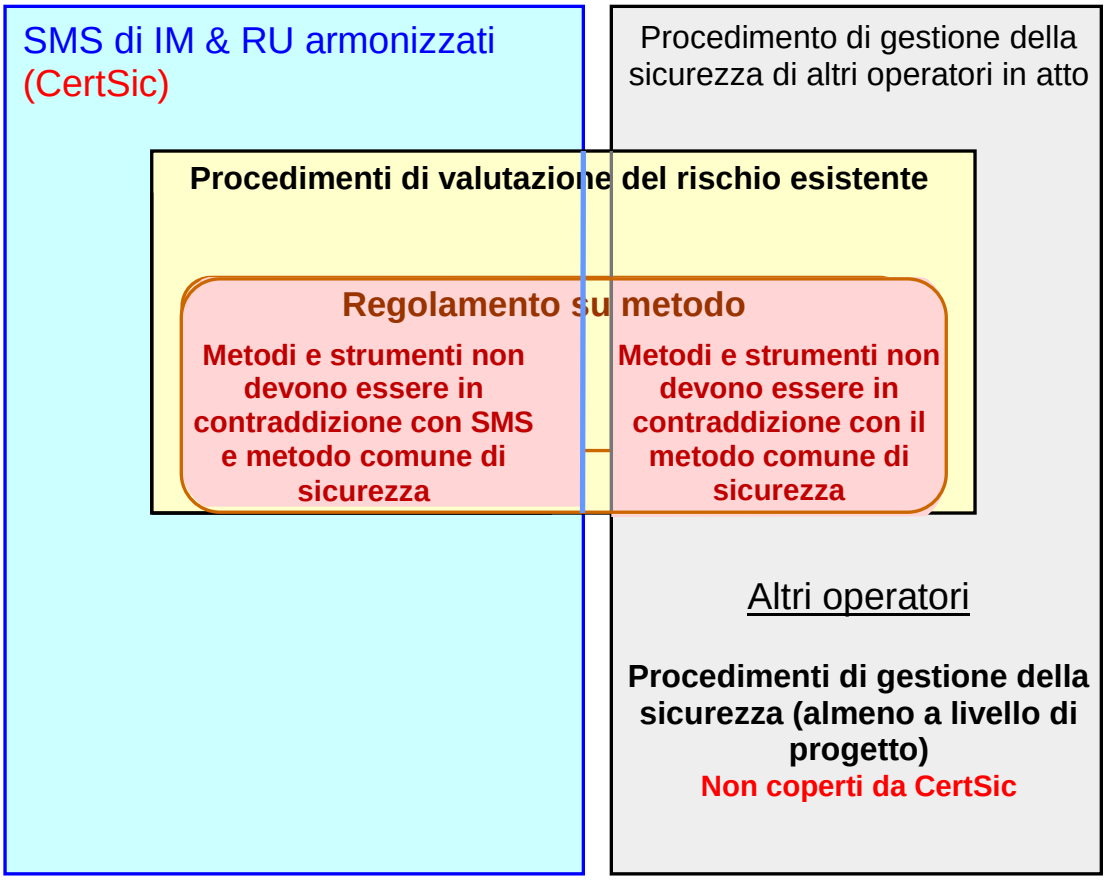

Figura 2 : SMS e metodo comune di sicurezza armonizzati.

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] Se il proponente è un gestore dell'infrastruttura o un'impresa ferroviaria, talvolta può essere necessario coinvolgere altri attori nel procedimento[8] (cfr. la sezione 1.2.1). In alcuni casi, il gestore dell'infrastruttura o l'impresa ferroviaria potrebbero subappaltare, parzialmente o integralmente, le attività di valutazione del rischio. Generalmente, i ruoli e le responsabilità di ciascun operatore sono concordati fra gli operatori interessati in una fase iniziale del progetto.

[G 2] È importante notare che il proponente resta comunque responsabile dell'applicazione del metodo comune di sicurezza, dell'accettazione del rischio e quindi della sicurezza del sistema. Egli dovrà anche fare in modo che:

(a) vi sia piena collaborazione fra gli operatori interessati in modo tale che vengano fornite tutte le informazioni necessarie, e;
(b) che sia chiaro chi deve soddisfare i particolari requisiti del metodo comune di sicurezza (per esempio l'esecuzione dell'analisi del rischio o la gestione del registro degli eventi pericolosi).

In caso di disaccordo fra i diversi operatori sui requisiti di sicurezza che ciascuno deve soddisfare, si potrebbe chiedere il parere della NSA. Ad ogni modo, la responsabilità di trovare una soluzione resta del proponente e non può essere trasferita alla NSA: cfr. anche la sezione 0.2.2.

[G 3] Qualora il compito fosse subappaltato, il subappaltatore non ha l'obbligo di disporre di un proprio organismo responsabile della sicurezza se non si tratta di un gestore dell'infrastruttura o di un'impresa ferroviaria o, in particolare, se la sua struttura/le sue dimensioni sono ridotte o il se il suo contributo al sistema complessivo è limitato. La responsabilità della gestione del rischio, comprese le attività di valutazione del rischio e gestione degli eventi pericolosi, può continuare ad essere dell'impresa di livello superiore (vale a dire del cliente del subappaltatore). Ad ogni modo, il subappaltatore è sempre responsabile di fornire le giuste informazioni relative alle proprie attività e necessarie all'impresa di livello superiore per creare la documentazione sulla gestione del rischio.
Le imprese che collaborano possono anche concordare di creare un organismo comune responsabile della sicurezza, per esempio per ottimizzare i costi. In questo caso, un solo organismo gestirà le attività di sicurezza di tutte le imprese coinvolte. La responsabilità dell'accuratezza delle informazioni (p.es. eventi pericolosi, rischi e misure di sicurezza), nonché la gestione dell'attuazione delle misure di sicurezza, resta dell'impresa incaricata di controllare gli eventi pericolosi ai quali sono connesse queste misure di sicurezza.

[G 4] Di norma, il proponente indica i "livelli di sicurezza" ed i "requisiti di sicurezza" assegnati agli operatori che partecipano al progetto e ai diversi sottosistemi e apparecchiature degli stessi:

(a) nei contratti stipulati fra il proponente e i rispettivi operatori (subappaltatori);

(8) *Conformemente all'appendice A.4 della 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

(b) in un piano di sicurezza o in qualsiasi altro documento pertinente con la stessa finalità, con la descrizione dell'organizzazione complessiva del progetto e le responsabilità di ogni operatore, comprese quelle del proponente: cfr. la sezione 1.1.6 ;
(c) nel(i) registro(i) degli eventi pericolosi del proponente: cfr. la sezione 4.1.1.

Quest'assegnazione dei "livelli di sicurezza" e dei "requisiti di sicurezza" del sistema ai sottosistemi e alle apparecchiature soggiacenti, e quindi ai rispettivi operatori compreso lo stesso proponente, si può perfezionare/ampliare durante la "fase di dimostrazione della conformità del sistema ai requisiti di sicurezza": cfr. Figura 1. Rispetto al ciclo a V delle norme CENELEC (cfr. la sezione 2.1.1 e la a pagina 38), quest'attività corrisponde alla Fase 5 che tratta della "ripartizione di requisiti di sicurezza" ai diversi sottosistemi e componenti

[G 5] L'Articolo 5 (2) consente che altri operatori, a parte l'impresa ferroviaria e il gestore dell'infrastruttura, si assumano la responsabilità complessiva della conformità al metodo comune di sicurezza, a seconda delle proprie esigenze. Per quanto riguarda i prodotti generici o le applicazioni generiche[9] per esempio, il produttore può eseguire la valutazione del rischio sulla base di una "definizione generica del sistema" per specificare i livelli e i requisiti di sicurezza imposti ai prodotti generici e alle applicazioni generiche.

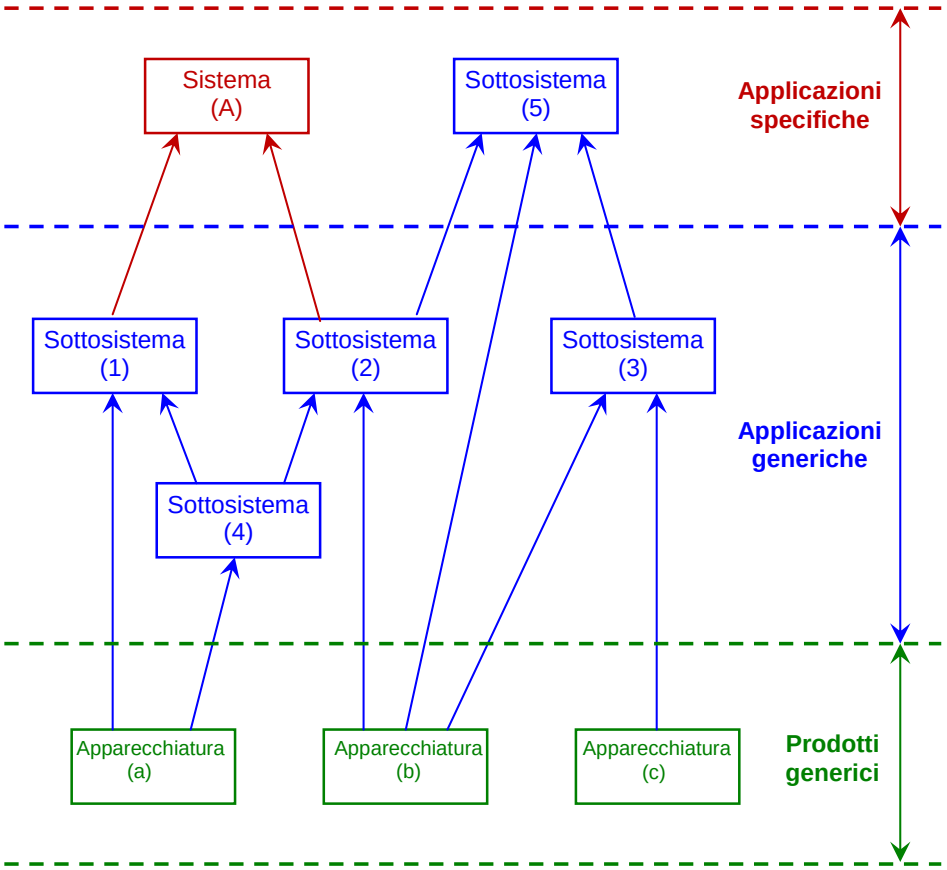

Figura 3 : Esempi di interdipendenza fra "safety case" (tratto dalla Figura 9 della norma EN 50 129).

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] Il CENELEC consiglia al produttore di fornire le prove documentate della valutazione del rischio nei *safety case* su prodotti generici (o applicazioni generiche[9]) e nei registri degli eventi pericolosi. Questi *safety case* e registri degli eventi pericolosi contengono tutte le ipotesi[10] e le "restrizioni d'uso" identificate (cioè le condizioni di applicazione relative alla sicurezza) applicabili ai prodotti generici (rispettivamente alle applicazioni generiche) in questione. Di conseguenza, ogniqualvolta un prodotto generico o un'applicazione generica vengono utilizzati in funzionamento in una specifica applicazione, la conformità a tutte queste ipotesi[10] e "restrizioni d'uso" (o condizioni di applicazione relative alla sicurezza) deve essere dimostrata in ogni specifica applicazione.

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.

[G 1] Molto spesso, a meno che diversamente concordato nei contratti all'inizio del progetto, ogni progetto ha un documento che descrive le attività di gestione del rischio. Tale documento è

---

(9) *I termini "safety case" su "applicazioni generiche" e su "prodotti generici" vengono riutilizzati dal CENELEC quando si possono prendere in considerazione tre diverse categorie di safety case : esempi di dipendenze tra safety cases (tratto dalla figura 3 in EN 50129 standard)*

(a) ***Safety case su prodotti generici*** *(indipendente dall'applicazione). Un prodotto generico può essere riutilizzato per diverse applicazioni indipendenti;*

(b) ***Safety case su applicazioni generiche*** *(per una categoria di applicazioni). Un'applicazione generica può essere riutilizzata per una categoria/un tipo di applicazione con funzioni comuni;*

(c) ***Safety case su applicazioni specifiche*** *(per un'applicazione specifica). Un'applicazione specifica viene utilizzata soltanto per un impianto particolare.*

Per maggiori informazioni sulla loro interdipendenza, cfr. la sezione 9.4 e la Figura 9.1 della guida CENELEC 50 126-2 {Ref. 9}.

(10) *Queste ipotesi e restrizioni d'uso determinano i limiti e la validità delle "valutazioni di sicurezza" e delle "analisi di sicurezza" connesse ai "safety case" dei relativi prodotti generici e applicazioni generiche. Qualora non vengano soddisfatte dall'applicazione specifica presa in considerazione, occorre aggiornare o sostituire le relative "valutazioni di sicurezza" e "analisi di sicurezza" (p.es. analisi causale) con delle valutazioni e analisi nuove.*

> *Ciò è in linea con il seguente principio di sicurezza generale: "Ogniqualvolta il progetto di uno specifico (sotto)sistema si basi su applicazioni generiche e prodotti generici, si deve dimostrare che tale specifico (sotto)sistema è conforme a tutte le ipotesi e le restrizioni d'uso (altrimenti dette nelle norme CENELEC 'condizioni di applicazione relative alla sicurezza') esportate nei corrispondenti 'safety case' su applicazioni generiche e prodotti generici (cfr. figura 3)"*

Se, per un'applicazione specifica, non è possibile ottenere la conformità ad alcune ipotesi e restrizioni d'uso a livello di sottosistema (p.es. nel caso di requisiti di sicurezza operativi), le ipotesi e restrizioni d'uso in questione possono essere trasferite ad un livello superiore (cioè, generalmente a livello di sistema). Queste ipotesi e restrizioni d'uso sono quindi chiaramente identificate nel "safety case su applicazioni specifiche" del sottosistema in questione. Ciò è essenziale per garantire, in esempi d'interdipendenza di questo tipo, che le condizioni di applicazione relative alla sicurezza di ogni 'safety case' vengano soddisfatte nel 'safety case' del livello superiore, oppure trasferite alle condizioni di applicazione relative alla sicurezza del 'safety case' del livello più alto (cioè il 'safety case' 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

aggiornato e revisionato ogniqualvolta vengono apportate modifiche significative al sistema originale.

[G 2] Questo documento descrive la struttura organizzativa, le responsabilità assegnate al personale, i procedimenti, le procedure e le attività che, tutte insieme, garantiscono che il sistema sottoposto a valutazione soddisfi i livelli e i requisiti di sicurezza specificati. Il documento deve essere conforme al metodo comune di sicurezza dal momento che viene utilizzato come strumento di riferimento e orientamento dall'organismo di valutazione. Le norme CENELEC consigliano di inserire questo tipo di informazioni in un piano di sicurezza, oppure in un altro documento con una parte dedicata a questi argomenti.

[G 3] Il piano di sicurezza del proponente in particolare, o qualsiasi altro documento pertinente, presenta l'organizzazione complessiva del progetto. Esso descrive le modalità di condivisione dei diversi ruoli e responsabilità fra gli operatori che partecipano al progetto. Per informazioni più dettagliate si possono consultare i piani di sicurezza o gli organismi di sicurezza dei diversi operatori coinvolti. Generalmente, la condivisione di responsabilità fra i diversi operatori viene discussa e concordata durante la definizione preliminare del sistema (cioè all'inizio del progetto), ove ve ne fosse una.

[G 4] Il piano di sicurezza è un documento dinamico aggiornato all'occorrenza nell'arco della durata del progetto.

[G 5] Per maggiori dettagli consultare la norma EN 50 126-1 {Ref. 8} e la guida connessa 50 126-2 {Ref. 9} sul contenuto di un piano di sicurezza.

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] Non si ritengono necessarie ulteriori spiegazioni.

1.2. Gestione dei punti d'interazione

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] Per esempio, se per ragioni operative un'impresa ferroviaria ha bisogno di un gestore dell'infrastruttura per realizzare determinate modifiche all'infrastruttura, ai sensi delle disposizioni dell'allegato III, paragrafo 2, lettera g, della direttiva sulla sicurezza delle ferrovie {Ref. 1}, anche l'impresa ferroviaria controlla il lavoro complessivo al fine di garantire che le modifiche attese siano eseguite correttamente. Ad ogni modo, la direzione dell'impresa ferroviaria non esonera il relativo gestore dell'infrastruttura dalla propria responsabilità di informare le altre imprese ferroviarie se anch'esse sono interessate dalla modifica dell'infrastruttura in questione. Il gestore dell'infrastruttura può anche dover eseguire 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

valutazione del rischio, conformemente al metodo comune di sicurezza, se a suo parere la modifica in questione è significativa.

[G 2] Eventuali trasferimenti di responsabilità fra i diversi operatori sono possibili e, in qualche circostanza, persino necessari. Tuttavia, quando diversi operatori sono coinvolti in un sistema, molto spesso un operatore è indicato come il responsabile della totalità del sistema. Ci sono sempre interdipendenze fra sottosistemi e operazioni particolarmente difficili da identificare. Occorre quindi che qualcuno si assuma la responsabilità complessiva delle analisi di sicurezza ed abbia anche libero accesso a tutta la relativa documentazione. Ovviamente, il proponente che intende introdurre la modifica significativa di solito ha la piena responsabilità della sistematicità e della completezza della valutazione del rischio.

[G 3] I principali criteri da concordare per la gestione di un punto d'interazione fra gli operatori interessati sono:

(a) la direzione delle attività, che solitamente è garantita dal proponente che intende introdurre la modifica significativa;
(b) gli input necessari;
(c) i metodi per l'individuazione degli eventi pericolosi e la valutazione del rischio;
(d) i partecipanti necessari con la competenza necessaria (cioè un insieme di conoscenza, abilità ed esperienza pratica nel settore –cfr. anche la definizione di "competenza del personale" al punto [G 2], paragrafo b, dell'articolo 3 in {Ref. 4});
(e) i risultati attesi.

Questi criteri sono descritti nei piani di sicurezza (o in qualsiasi altro documento pertinente) delle imprese che operano con i punti d'interazione interessati.

[G 4] La sezione C.3. dell'appendice C offre esempi di punti d'interazione insieme ad un esempio dell'applicazione dei principali criteri per la gestione dei punti d'interazione fra un produttore di treni ed un gestore dell'infrastruttura o un'impresa ferroviaria.

[G 5] La gestione dei punti d'interazione deve anche prendere in esame i rischi che potrebbero sorgere nei punti d'interazione con operatori umani (durante il funzionamento e la manutenzione) per la progettazione di tali punti d'interazione.

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] Il procedimento di trasferimento degli eventi pericolosi e delle misure di sicurezza connesse fra operatori è applicabile anche a livelli inferiori del ciclo a "V" delle norme CENELEC illustrato nella Figura 5 a pagina 38. Si può infatti applicare, per esempio, ogniqualvolta è necessario lo scambio di tali informazioni fra un operatore e i suoi subappaltatori. La differenza con lo stesso processo a livello di sistema è che il proponente non deve essere necessariamente informato di tutti i trasferimenti di eventi pericolosi e misure di sicurezza connesse a livello di sottosistemi. Il proponente viene informato soltanto quando gli eventi pericolosi trasferiti e le misure di sicurezza connesse riguardano punti d'interazione ad alto livello (cioè quando riguardano un punto d'interazione con il 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] Il sistema di gestione della sicurezza (SMS) dell'impresa ferroviaria e del gestore dell'infrastruttura contempla gli accordi e le procedure per garantire che eventuali non conformità o inadeguatezze delle misure di sicurezza siano gestite correttamente. Di conseguenza, tali accordi e procedure non fanno parte del metodo comune di sicurezza.

[G 2] Analogamente, accordi e procedure[(11)] che altri operatori[(12)] devono attuare per garantire che eventuali non conformità o inadeguatezze delle misure di sicurezza siano gestite correttamente e, all'occorrenza, che le misure di sicurezza siano trasferite agli operatori pertinenti, sono concordati fra gli attori in questione all'inizio del progetto e descritti dettagliatamente nel loro piano di sicurezza: cfr. la sezione 0.2.

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] In questo modo sarà possibile gestire eventuali non conformità o inadeguatezze delle misure di sicurezza all'interno del sistema sottoposto a valutazione o all'interno di sistemi simili che utilizzano le stesse misure.

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] Non si ritengono necessarie ulteriori spiegazioni.

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] Non si ritengono necessarie ulteriori spiegazioni.

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] Non si ritengono necessarie ulteriori spiegazioni.

---

(11) *In linea di massima, tali accordi e procedure sono contemplati nel processo di gestione della qualità e/o della sicurezza di questi operatori, indicato per lo meno a livello di progetto (cfr. anche la Figura 2).*

(12) *Il termine "altri operatori" designa tutti gli altri operatori interessati tranne IM ed RU.*

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

2. DESCRIZIONE DEL PROCEDIMENTO DI VALUTAZIONE DEI RISCHI

2.1. Descrizione generale – Corrispondenza fra il procedimento di valutazione del rischio del metodo comune di sicurezza e il ciclo a "V" delle norme 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] Il procedimento di gestione del rischio contemplato dal metodo comune di sicurezza può essere rappresentato all'interno di un ciclo a "V" che inizia con la definizione (preliminare) del sistema e che termina con l'accettazione del sistema: cfr. Figura 4. Questo ciclo a "V" semplificato può essere quindi elaborato sulla scia del ciclo a "V" classico illustrato nella Figura 10 della norma EN 50 126-1 {Ref. 8}. Al fine di mostrare la corrispondenza del procedimento di gestione del rischio del metodo comune di sicurezza illustrato nella Figura 1, il ciclo a "V" delle norme CENELEC illustrato nella Figura 10 è richiamato nella Figura 5:

(a) la "definizione preliminare del sistema" del metodo comune di sicurezza nella Figura 1 corrisponde alla Fase 1 nel ciclo a "V" delle norme CENELEC, cioè alla definizione del "concetto" di sistema (cfr. QUADRO 1 nella Figura 5);

(b) la "valutazione del rischio" del metodo comune di sicurezza nella Figura 1 comprende le seguenti fasi del ciclo a "V" delle norme CENELEC (cfr. QUADRO 2 nella Figura 5):

(1) Fase 2 nella Figura 5: "definizione del sistema e condizioni di applicazione";

(2) Fase 3 nella Figura 5: "analisi dei rischi";

(3) Fase 4 nella Figura 5: "requisiti di sistema";

(4) Fase 5 nella Figura 5: "ripartizione di requisiti di sistema" ai diversi sottosistemi e componenti.

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

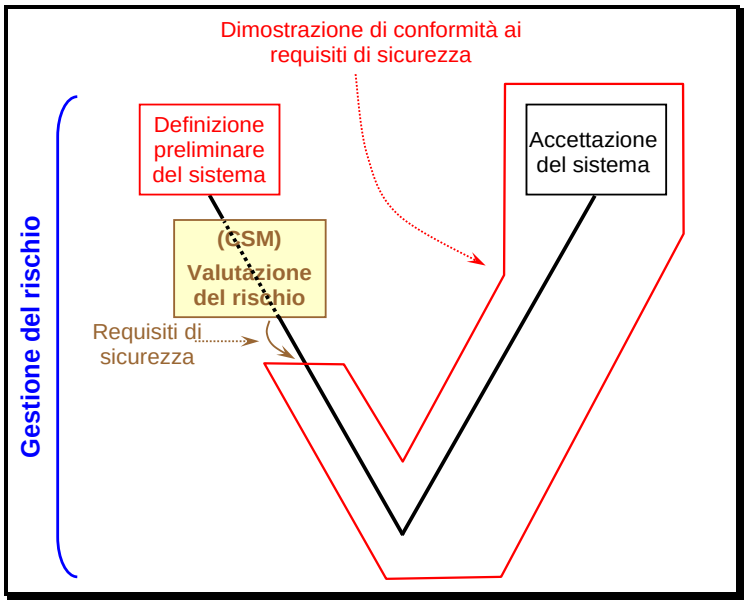

Figura 4 : Ciclo a "V" semplificato della Figura 10 della norma EN 50 126.

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

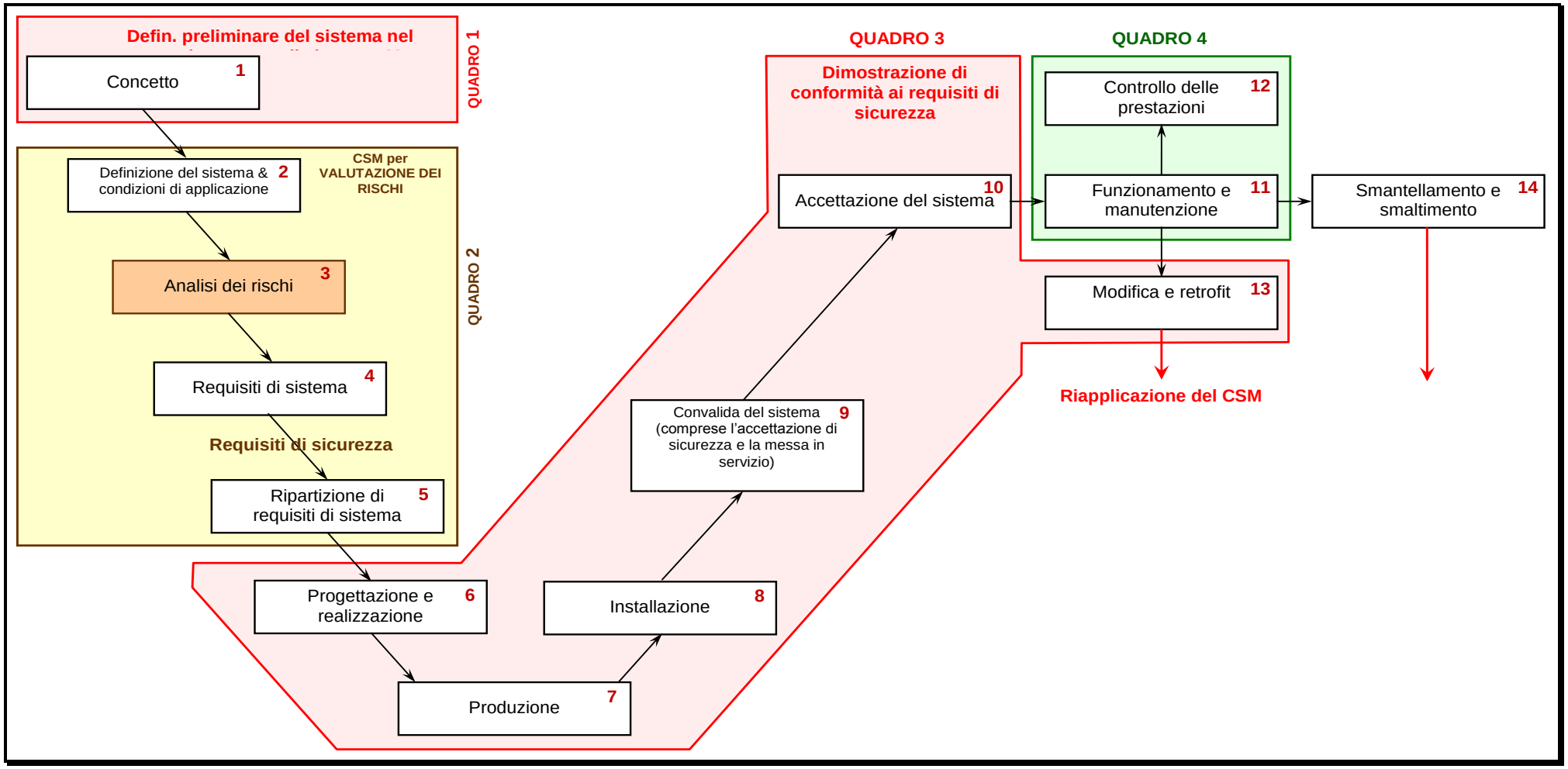

Figura 5 : Figura 10 del ciclo a "V" della norma EN 50 126 (ciclo di vita del sistema CENELEC).

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] I risultati del procedimento di valutazione del rischio previsto dal metodo comune di sicurezza sono (dopo alcune ripetizioni – cfr. Figura 1):

(a) la “definizione del sistema” aggiornata con i "requisiti di sicurezza" derivanti dalle attività di “analisi” e “valutazione del rischio” (cfr. la sezione 2.1.6);
(b) la "ripartizione di requisiti di sistema" ai diversi sottosistemi e componenti (Fase 5 nella Figura 5);
(c) il "registro degli eventi pericolosi" che riporta:

(1) tutti gli eventi pericolosi identificati e le misure di sicurezza connesse;
(2) i conseguenti requisiti di sicurezza;
(3) le ipotesi di cui si è tenuto conto per il sistema e che determinano i limiti e la validità della valutazione del rischio (cfr. punto (g) nella sezione 2.1.2);

(d) e, in generale, tutte le prove derivanti dall’applicazione del metodo comune di sicurezza: cfr. la sezione 5.

Questi risultati della valutazione del rischio del metodo comune di sicurezza corrispondono ai risultati relativi alla sicurezza della Fase 4 del ciclo a “V” delle norme CENELEC, cioè alle specifiche di requisiti di sistema della Figura 5.

[G 3] La definizione del sistema aggiornata con i risultati della valutazione del rischio e il registro degli eventi pericolosi costituiscono gli input rispetto ai quali il sistema viene progettato e accettato. La "dimostrazione della conformità del sistema ai requisiti di sicurezza" del metodo comune di sicurezza corrisponde alle seguenti fasi del ciclo a “V” delle norme CENELEC (cfr. QUADRO 3 nella Figura 5):

(a) Fase 6 nella Figura 5: "progettazione e realizzazione";
(b) Fase 7 nella Figura 5: "produzione";
(c) Fase 8 nella Figura 5: "installazione";
(d) Fase 9 nella Figura 5: "validazione del sistema (comprese l’accettazione della sicurezza e la messa in servizio)";
(e) Fase 10 nella Figura 5: "accettazione del sistema".

[G 4] La dimostrazione della conformità del sistema ai requisiti di sicurezza dipende dalla natura tecnica, operativa od organizzativa della modifica significativa. Pertanto, le diverse fasi del ciclo a “V” delle norme CENELEC illustrate nella Figura 5 possono non essere adatte a tutte le modifiche significative di un determinato tipo. Il ciclo a “V” della Figura 5 deve essere considerato di conseguenza, ed utilizzato valutando opportunamente ciò che si adatta a ciascuna applicazione specifica (p.es. per modifiche operative ed organizzative non vi è una fase di produzione).

[G 5] Ciò significa che la "dimostrazione della conformità del sistema ai requisiti di sicurezza" nel metodo comune di sicurezza non comprende soltanto le attività di "verifica e validazione" mediante test o simulazioni. In pratica, essa comprende tutte le fasi "dalla 6 alla 10" (vedi elenco di cui sopra e la Figura 5) del ciclo a “V” delle norme CENELEC. Fra queste vi sono le attività di progettazione, produzione, installazione, verifica e validazione, nonché le attività RAMS e l’accettazione del sistema.

[G 6] Durante la "dimostrazione della conformità del sistema ai requisiti di sicurezza", il principio generale è quello di concentrare la valutazione del rischio esclusivamente sulle funzioni che interessano la sicurezza e sui punti d’interazione del sistema. Ciò significa che, ogniqualvolta una delle fasi del ciclo a “V” delle norme CENELEC illustrato Figura 5, si concentra su:

(a) le funzioni relative alla sicurezza e i punti d’interazione;

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

(b) i sottosistemi e/o i componenti coinvolti nell'ottenimento delle funzioni connesse alla sicurezza e/o i punti d'interazione valutati durante le attività di valutazione del rischio di livello superiore.

[G 7] Dal confronto con il classico ciclo a "V" delle norme CENELEC illustrato nella Figura 5 emerge che:

(a) il metodo comune di sicurezza copre le fasi "da 1 a 10" e "13" di questo ciclo a "V". Esse comprendono le attività necessarie affinché il sistema sottoposto a valutazione sia accettato;

(b) il metodo comune di sicurezza non copre le fasi "11", "12" e "14" del ciclo di vita del sistema:

(1) le fasi "11" e "12" riguardano, rispettivamente, "funzionamento e manutenzione" e "controllo delle prestazioni" del sistema dopo l'accettazione dello stesso sulla base del metodo comune di sicurezza. Queste due fasi sono invece coperte dal sistema di gestione della sicurezza (SMS) dell'impresa ferroviaria e del gestore dell'infrastruttura – (Cfr. QUADRO 4 nella Figura 5. Tuttavia, qualora durante il funzionamento, la manutenzione o il controllo delle prestazioni del sistema sembri necessario modificare e aggiornare il sistema (Fase 13 nella Figura 5), sebbene sia già in funzione, si applica nuovamente il metodo comune di sicurezza alle nuove modifiche, conformemente all'Articolo 2. Di conseguenza, se la modifica è significativa:

(i) vi si applicano i procedimenti di gestione e valutazione del rischio previsti nel metodo comune di sicurezza;
(ii) occorre l'accettazione di queste nuove modifiche conformemente all'Articolo 6;

(2) anche lo "smantellamento e lo smaltimento" di un sistema già in funzione (Fase 14) potrebbero essere ritenuti una modifica significativa e, di conseguenza, si potrebbe applicare nuovamente il metodo comune di sicurezza, conformemente all'Articolo 2 per la fase 14 della Figura 5.

Per maggiori informazioni sull'ambito di applicazione di ogni fase o attività del ciclo a "V" delle norme CENELEC richiamate nella Figura 5, consultare la sezione 6. della norma EN 50 126-1 {Ref. 8}

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] Non si ritengono necessarie ulteriori spiegazioni.

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

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

[G 1] Non si ritengono necessarie ulteriori spiegazioni.

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:

(a) the application of codes of practice (section 2.3);
(b) a comparison with similar systems (section 2.4);
(c) 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] In generale, il proponente decide quale principio di accettabilità dei rischi è più adatto a controllare gli eventi pericolosi identificati sulla base dei requisiti specifici del progetto, nonché sull'esperienza del proponente stesso con i tre principi.

[G 2] Non sempre è possibile valutare l'accettabilità dei rischi a livello di sistema mediante l'uso di uno solo dei tre principi di accettazione dei rischi. L'accettabilità dei rischi spesso si baserà su una combinazione di tali principi. Se per un evento pericoloso significativo occorre applicare più di un principio di accettabilità del rischio per controllare il rischio connesso, l'evento pericoloso in questione deve essere suddiviso in eventi secondari, in modo tale che ogni singolo evento pericoloso secondario sia controllato adeguatamente da un solo principio di accettabilità del rischio.

[G 3] La decisione di controllare un evento pericoloso mediante un principio di accettabilità dei rischi deve tener conto dell'evento pericoloso e delle cause dell'evento pericoloso già identificate durante la fase di individuazione degli eventi pericolosi. Pertanto, se due cause diverse e indipendenti sono legate allo stesso evento pericoloso, quest'ultimo deve essere suddiviso in due diversi eventi pericolosi secondari. Ogni evento pericoloso secondario sarà quindi controllato da un unico principio di accettazione del rischio. I due eventi pericolosi secondari devono essere annotati e gestiti nel registro degli eventi pericolosi. Per esempio, se l'evento pericoloso è causato da un errore di progettazione può essere gestito mediante l'applicazione di un codice di buona pratica, mentre se la causa dell'evento pericoloso è un errore di manutenzione, il codice di buona pratica da solo può non essere sufficiente e può essere necessaria l'applicazione di un altro principio di accettazione dei rischi.

[G 4] La riduzione del rischio ad un livello accettabile potrebbe richiedere diverse ripetizioni fra la fase di analisi e quella di valutazione del rischio fino a che non si identificano misure di sicurezza opportune.

[G 5] L'attuale rischio residuo derivante dall'esperienza sul campo per i sistemi esistenti e per i sistemi basati sull'applicazione di codici di buona pratica, è considerato accettabile. Il rischio derivante dalla stima esplicita del rischio si basa su un parere esperto e su diverse ipotesi fatte dall'esperto durante l'analisi, oppure su database di esperienze di incidenti o esperienze operative. Di conseguenza, il rischio residuo derivante dalla stima esplicita del rischio non può essere confermato immediatamente dal feedback sul campo. Una dimostrazione di questo tipo richiede tempo per operare, controllare ed ottenere un'esperienza rappresentativa del(i) sistema(i) in questione. In generale, l'applicazione di

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

codici di buona pratica e il confronto con sistemi di riferimento simili hanno il vantaggio di evitare un'eccessiva specificazione di requisiti di sicurezza inutilmente rigorosi che possono derivare da ipotesi (di sicurezza) eccessivamente conservatrici nelle stime esplicite del rischio. Ad ogni modo, potrebbe accadere che alcuni requisiti di sicurezza derivanti da codici di buona pratica o da sistemi di riferimento simili non debbano essere soddisfatti dal sistema sottoposto a valutazione. In tal caso, l'applicazione della stima esplicita del rischio avrebbe il vantaggio di evitare un inutile eccesso di progettazione del sistema sottoposto a valutazione e consentirebbe di offrire un progetto più conveniente mai provato prima.

[G 6] Se gli eventi pericolosi identificati e il(i) rischio(i) connesso(i) del sistema sottoposto a valutazione non possono essere controllati mediante l'applicazione di codici di buona pratica o di sistemi di riferimento simili, si esegue una stima esplicita del rischio basata su analisi quantitative o qualitative di eventi pericolosi. Questa situazione sorge quando il sistema sottoposto a valutazione è completamente nuovo (o il progetto è innovativo) oppure quando il sistema si discosta da un codice di buona pratica o da un sistema di riferimento. La stima esplicita del rischio valuterà quindi se il rischio è accettabile (cioè se non è necessaria un'ulteriore analisi) o se sono necessarie misure di sicurezza supplementari per ridurre ulteriormente il rischio.

[G 7] Orientamenti sulla riduzione e l'accettazione del rischio si possono trovare anche nella sezione 8 della guida EN 50 126-2 {Ref. 9}.

[G 8] Il principio di accettazione del rischio utilizzato e la sua applicazione devono essere valutati dall'organismo di valutazione.

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] Per esempio, se per il software di un componente viene specificata come requisito di sicurezza l'applicazione del processo di sviluppo SIL 4 della norma EN 50 128, la dimostrazione dovrà appunto indicare che il processo raccomandato dalla norma è soddisfatto. Ciò comprende, per esempio, la dimostrazione che:

(a) i requisiti di indipendenza nell'organizzazione del progetto, nella verifica e nella validazione del software sono soddisfatti;
(b) sono applicati i metodi corretti della norma EN 50 128 per il livello d'integrità della sicurezza SIL 4;
(c) ecc.

[G 2] Per esempio, se si deve utilizzare un codice di buona pratica dedicato per la produzione di elettrovalvole per freni d'emergenza, la dimostrazione dovrà provare che tutti i requisiti del codice di buona pratica sono soddisfatti durante il processo di produzione.

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

2.1.6. 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] Si possono individuare due tipi di misure di sicurezza:

(a) "misure di sicurezza preventive" che evitano l'insorgenza di eventi pericolosi o delle loro cause, e;
(b) "misure di sicurezza mitigative" che evitano che gli eventi pericolosi evolvano in incidenti o che riducono le conseguenze degli incidenti dopo che questi si sono verificati (misure di protezione)

Ai fini della fattibilità, generalmente la prevenzione delle cause è più efficiente.

[G 2] Il proponente considererà come misure di sicurezza più opportune quelle che offrono il miglior compromesso fra il costo per ottenere la riduzione del rischio e il livello del rischio residuo. Le misure di sicurezza scelte diventano i requisiti di sicurezza per il sistema sottoposto a valutazione.

[G 3] È importante controllare che le misure di sicurezza selezionate per controllare un pericolo non siano in conflitto con altri eventi pericolosi. Come rappresentato nella Figura 6, possono presentarsi, per esempio, i due seguenti casi [(13)]:

(a) CASO 1: se la stessa misura di sicurezza (misura A sulla Figura 6) può controllare diversi eventi pericolosi senza creare conflitti fra loro, ed è economicamente giustificata, si potrebbe scegliere la misura di sicurezza in questione da sola come "requisito di sicurezza" associato. Il numero totale di requisiti di sicurezza da soddisfare è inferiore rispetto all'implementazione delle misure sia B che C;

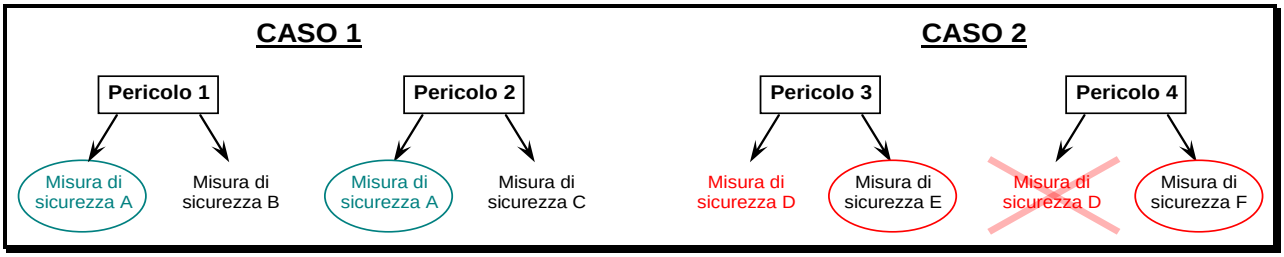

Figura 6 : Selezione di adeguate misure di sicurezza per controllare i rischi.

(b) CASO 2: al contrario, se una misura di sicurezza può controllare un evento pericoloso ma crea un conflitto con un altro evento pericoloso (misura D sulla Figura 6), non può essere scelta come "requisito di sicurezza". Le altre misure di sicurezza per l'evento pericoloso considerato devono essere utilizzate (misure E ed F sulla Figura 6):

(1) Un tipico esempio nel sistema di controllo-comando è l'uso della posizione del treno sul binario o per controllare l'azionamento dei freni o per autorizzare l'accelerazione

(13) *Si tenga presente che la guida non elenca tutte le situazioni in cui le misure di sicurezza potrebbero entrare in conflitto con altri eventi pericolosi identificati. Vengono forniti soltanto alcuni esempi illustrativi.*

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

del treno. L'uso della testa del treno (o della coda del treno) come posizione del treno non è sicuro in tutte le situazioni:

(i) quando il sistema di controllo-comando ETCS deve azionare i freni di emergenza in condizioni di sicurezza, utilizza la MASSIMA SICUREZZA ALLA TESTA DEL TRENO per garantire che la testa del treno si arresti effettivamente prima di raggiungere il Punto Protetto (Danger Point);

(ii) viceversa, quando il treno è autorizzato ad accelerare dopo un limite di velocità, per esempio, il sistema di controllo-comando ETCS usa la MINIMA SICUREZZA ALLA CODA DEL TRENO;

(2) Un altro esempio è una misura di sicurezza che potrebbe essere valida per arrestare un treno in quasi tutte le circostanze affinché entri in uno stato di arresto in condizioni di sicurezza, eccetto nel caso di una galleria o di un ponte. In ques'ultimo caso, non si deve adottare la misura D del CASO 2 della 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] A seconda, per esempio, delle scelte tecniche per la progettazione di un sistema, dei suoi sotto-sistemi e delle apparecchiature, si potrebbero identificare nuovi eventi pericolosi durante la "dimostrazione di conformità ai requisiti di sicurezza" (p.es. l'uso di una determinata vernice potrebbe determinare la formazione di gas tossici in caso d'incendio). Questi nuovi eventi pericolosi e i rischi connessi devono essere considerati come nuovi input per un nuovo ciclo del procedimento di valutazione iterativa del rischio. L'appendice A.4.3 della norma EN 50 129 offre altri esempi in cui potrebbero essere introdotti nuovi eventi pericolosi da dover controllare.

2.2. Individuazione degli eventi pericolosi

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] Gli eventi pericolosi sono esplicitati il più possibile allo stesso livello di dettaglio. Può accadere, durante le analisi preliminari degli eventi pericolosi, che si identifichino eventi pericolosi di diversi livelli di dettaglio (p.es. perché nell'analisi HAZOP confluiscono persone con esperienze diverse).
Il livello di dettaglio dipende anche dal principio di accettazione del rischio selezionato per l'(gli) evento(i) pericoloso(i) identificato(i). Per esempio, se un evento pericoloso è controllato completamente da un codice di buona pratica o ad un sistema di riferimento simile, non occorrerà un'individuazione degli eventi pericolosi più dettagliata.

[G 2] Tutti gli eventi pericolosi identificati durante il procedimento di valutazione del rischio (compresi quelli connessi a rischi ampiamente accettabili), le misure di sicurezza e i rischi connessi, devono essere annotati nel registro degli eventi pericolosi.

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] A seconda della natura del sistema da analizzare, si possono utilizzare diversi metodi per l'individuazione degli eventi pericolosi:

(a) l'individuazione empirica degli eventi pericolosi può essere utilizzata sfruttando l'esperienza già acquisita (p.es. utilizzando liste di controllo o elenchi generici di eventi pericolosi);
(b) l'individuazione creativa di eventi pericolosi può essere utilizzata per nuovi settori di interesse (previsioni proattive, p.es. studi "WHAT-IF" strutturati come le analisi FMEA o HAZOP).

[G 4] I metodi empirico e creativo per l'individuazione di eventi pericolosi possono essere utilizzati insieme per integrarsi, garantendo che l'elenco di potenziali eventi pericolosi e misure di sicurezza, ove opportuno, sia esaustivo.

[G 5] Come fase preliminare, l'individuazione degli eventi pericolosi potrebbe iniziare con un team di brainstorming in cui sono presenti esperti con diverse competenze che abbracciano tutti gli aspetti della modifica significativa. Quando la commissione di esperti lo ritiene necessario, si possono utilizzare metodi empirici per analizzare una specifica funzione o modalità operativa.

[G 6] I metodi usati per l'individuazione degli eventi pericolosi dipendono dalla definizione del sistema. Alcuni esempi sono illustrati nell'appendice B.

[G 7] Maggiori informazioni sulle tecniche di individuazione degli eventi pericolosi figurano nell'allegato A.2 & E della guida EN 50 126-2 {Ref. 9}.

[G 8] Un esempio di elenco di eventi pericolosi generici è illustrato nella sezione C.17. dell'appendice C.

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] Per aiutare il procedimento di valutazione dei rischi, gli eventi pericolosi significativi possono essere raggruppati ulteriormente in diverse categorie. Per esempio, possono essere classificati o catalogati in base alla gravità del rischio prevista e alla frequenza del loro verificarsi. Le norme CENELEC offrono una guida per esercizi di questo tipo: cfr. sezione A.2. dell'appendice A.

[G 2] L'analisi e la valutazione dei rischi descritte nella sezione 2.1.4 vengono applicate su una base di priorità, cominciando dagli eventi pericolosi che si trovano ai primi posti nella classifica.

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

2.2.3. 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] Per esempio, un rischio connesso a un evento pericoloso può essere considerato ampiamente accettabile:

(a) se il rischio è inferiore ad una determinata percentuale (p.es. x%) del Rischio Massimo Tollerabile per questo tipo di eventi pericolosi. Il valore di x% si potrebbe basare sul meglio derivato dalla pratica e dall'esperienza con diversi approcci di analisi del rischio, p.es. il rapporto fra classificazioni dei rischi ampiamente accettabili e dei rischi intollerabili nelle curve FN o in matrici di rischio. Questa situazione si può rappresentare come illustrato nella Figura 7;

(b) oppure, se la perdita legata al rischio è così ridotta da non giustificare l'applicazione di alcuna contromisura di sicurezza.

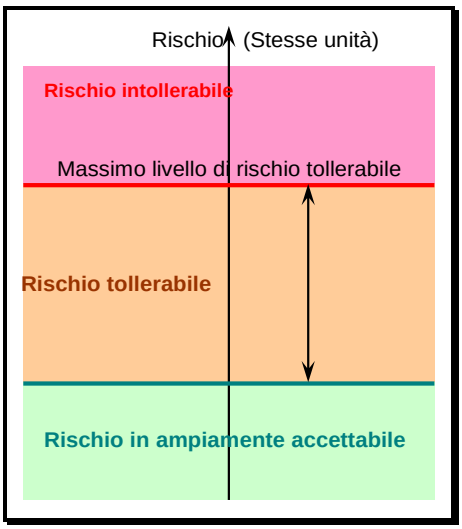

Figura 7 : Rischi ampiamente accettabili

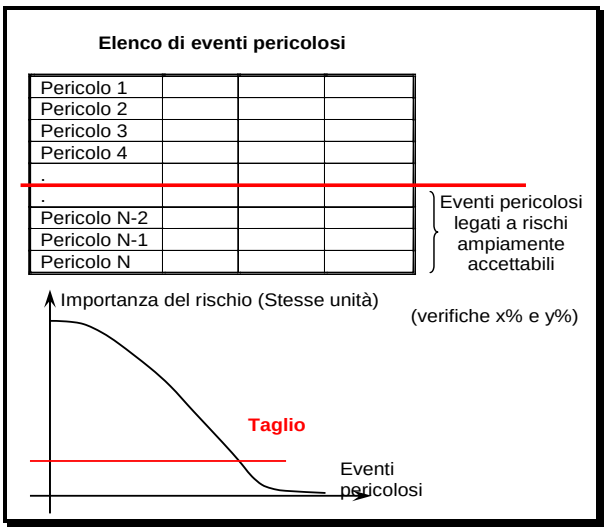

Figura 8 : Filtraggio di eventi pericolosi legati a rischi ampiamente accettabili.

[G 2] Inoltre, se si identificano eventi pericolosi con diversi livelli di dettaglio (cioè eventi pericolosi ad alto livello da una parte ed eventi pericolosi secondari di maggior dettaglio dall'altra), occorre prendere delle precauzioni per evitare una classificazione erronea fra gli eventi pericolosi legati a rischi ampiamente accettabili. Il contributo di tutti gli eventi pericolosi legati a rischi ampiamente accettabili non può superare una determinata proporzione (p.es. y%) del rischio complessivo a livello di sistema. Questa verifica è necessaria per evitare che il principio sia svuotato di contenuto suddividendo gli eventi pericolosi in molti eventi pericolosi secondari di basso livello. Se un evento pericoloso, infatti, è espresso sotto forma di molti diversi eventi pericolosi secondari "più piccoli", ciascuno di questi può essere facilmente classificato come evento pericoloso legato a rischi ampiamente accettabili, se si effettua una valutazione separata, ma se gli eventi pericolosi vengono valutati tutti insieme, l'evento pericoloso complessivo può essere considerato legato a un rischio significativo (cioè come un evento pericoloso di alto livello). Il valore della proporzione (p.es. y%) dipende dai criteri di accettazione del rischio applicabili a livello di sistema. Esso può basarsi su una stima derivante dall'esperienza operativa di sistemi di riferimento simili.

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] Le due verifiche di cui sopra (cioè rispetto alle percentuali x % e y %) consente di concentrare la valutazione dei rischi sugli eventi pericolosi più importanti, nonché di garantire che qualsiasi rischio significativo sia controllato (cfr. Figura 8).
Fatti salvi i requisiti di legge di un determinato Stato membro, il proponente è responsabile di definire, in base al parere degli esperti, i valori di x % ed y % e di farli valutare separatamente dall'organismo di valutazione. Un esempio di ordini di grandezza può essere x = 1% ed y = 10%, se questa situazione è considerata accettabile dal parere degli esperti

[G 4] La sezione 2.2.2. dispone che un organismo di valutazione faccia una valutazione indipendente della classificazione in "rischi(o) ampiamente accettabile(i.

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] Lo scopo principale dell'attività è l'individuazione di eventi pericolosi legati alla modifica. Se sono state già identificate misure di sicurezza, esse devono essere annotate nel registro degli eventi pericolosi. La natura delle misure dipende dalla modifica, che può essere procedurale, tecnica, operativa o organizzativa.

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] Anche se un rischio è controllato ad un livello accettabile, il proponente può comunque decidere che occorre un'individuazione degli eventi pericolosi più dettagliata. Uno dei motivi di questa decisione potrebbe essere che è probabile trovare misure efficaci di controllo del rischio più convenienti se si effettua un'individuazione degli eventi pericolosi più dettagliata.

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:

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

[G 1] Non si ritengono necessarie ulteriori spiegazioni.

2.3. Utilizzo di codici di buona pratica e determinazione dei rischi

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] Non si ritengono necessarie ulteriori spiegazioni.

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

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

(a) 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;
(b) be relevant for the control of the considered hazards in the system under assessment;
(c) be publicly available for all actors who want to use them.

[G 1] Non si ritengono necessarie ulteriori spiegazioni.

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] Non si ritengono necessarie ulteriori spiegazioni.

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] Non si ritengono necessarie ulteriori spiegazioni.

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:

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

[G 1] Non si ritengono necessarie ulteriori spiegazioni.

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] Non si ritengono necessarie ulteriori spiegazioni.

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

2.3.7. 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] Non si ritengono necessarie ulteriori spiegazioni.

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

(a) The hazard identification in accordance with section 2.2.6;
(b) The registration of the use of the codes of practice in the hazard record in accordance with section 2.3.5;
(c) The documentation of the application of the risk management process in accordance with section 5;
(d) An independent assessment in accordance with Article 6.

[G 1] Non si ritengono necessarie ulteriori spiegazioni.

2.4. Uso del sistema di riferimento e determinazione dei rischi

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] Maggiori informazioni su questi principi si possono trovare nella sezione 8 della guida EN 50 126-2 {Ref. 9}.

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

(a) 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;
(b) it has similar functions and interfaces as the system under assessment;
(c) it is used under similar operational conditions as the system under assessment;
(d) it is used under similar environmental conditions as the system under assessment.

[G 1] Per esempio, un sistema di controllo-comando obsoleto che, in uso, ha dimostrato di avere un livello accettabile di sicurezza, potrebbe essere sostituito da un altro sistema con una tecnologia più recente e migliori prestazioni in termini di sicurezza. È quindi pertinente verificare, ogniqualvolta si applica un sistema di riferimento, se il sistema sottoposto a valutazione continua ad essere accettabile.

[G 2] Per esempio, poiché certi aspetti di sicurezza in galleria o la sicurezza del trasporto di merci pericolose potrebbero essere specifici e potrebbero dipendere da condizioni operative ed ambientali, per ogni progetto occorre verificare che il sistema sarà utilizzato nelle stesse condizioni.

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

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

(a) the risks associated with the hazards covered by the reference system shall be considered as acceptable;
(b) 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;
(c) these safety requirements shall be registered in the hazard record as safety requirements for the relevant hazards.

[G 1] Non si ritengono necessarie ulteriori spiegazioni.

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] Maggiori informazioni su analisi di similarità si possono trovare nella sezione 8.1.3 della guida EN 50 126-2 {Ref. 9}.

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] Non si ritengono necessarie ulteriori spiegazioni.

2.5. Stima e determinazione accurata dei rischi

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] Non si ritengono necessarie ulteriori spiegazioni.

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

2.5.2. 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] Al fine di valutare se i rischi del sistema sottoposto a valutazione sono accettabili o meno, occorrono dei criteri di accettabilità del rischio (cfr. quadri sulla "valutazione dei rischi" della Figura 1). I criteri di accettabilità dei rischi possono essere o impliciti o espliciti:

(a) criteri di accettabilità del rischio impliciti: in base alle sezioni 2.3.5 e 2.4.3., i rischi coperti dall'applicazione di codici di buona pratica e dal confronto con sistemi di riferimento sono considerati implicitamente accettabili a condizione che, rispettivamente, (cfr. cerchio tratteggiato nella Figura 1):

(1) siano soddisfatte le condizioni di applicazione di codici di buona pratica indicate nella sezione 2.3.2;
(2) siano soddisfatte le condizioni per l'uso di un sistema di riferimento indicate nella sezione 2.4.2;

(b) criteri di accettabilità del rischio espliciti: al fine di valutare se il(i) rischio(i) controllato(i) dall'applicazione di una stima esplicita del rischio è(sono) accettabile(i) o meno, occorrono dei criteri espliciti di accettabilità dei rischi (cfr. il cerchio a linea continua nella Figura 1 per il terzo principio). Tali criteri si possono definire a diversi livelli di un sistema ferroviario. Possono essere infatti considerati come una "piramide di criteri" (cfr. Figura 9) cominciando dai criteri di accettabilità dei rischi di alto livello (definiti per esempio come rischi per la società o per i singoli), per scendere ai sottosistemi ed ai componenti (per coprire i sistemi tecnici) e includere gli operatori umani durante il funzionamento e gli interventi di manutenzione del sistema e dei sottosistemi. Sebbene i criteri di accettabilità del rischio contribuiscano ad ottenere il livello di sicurezza del sistema, e siano quindi legati agli obiettivi comuni di sicurezza (CST) ed ai valori di riferimento nazionali (NRV), è molto difficile creare fra loro un modello matematico: cfr. {Ref. 12} per maggiori dettagli.
Il livello in cui sono definiti i criteri espliciti di accettabilità dei rischi deve coincidere con l'importanza e la complessità della modifica significativa. Per esempio, non è necessario valutare il rischio complessivo del sistema ferroviario quando si modifica un tipo di asse del materiale rotabile. La definizione dei criteri di accettabilità del rischio può concentrarsi sulla sicurezza del materiale rotabile. Viceversa, grandi modifiche o aggiunte ad un sistema ferroviario esistente non devono essere valutate esclusivamente sulla base dei livelli di sicurezza di singole funzioni o modifiche aggiunte. Si deve verificare anche a livello del sistema ferroviario se la modifica è accettabile nel suo insieme.

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

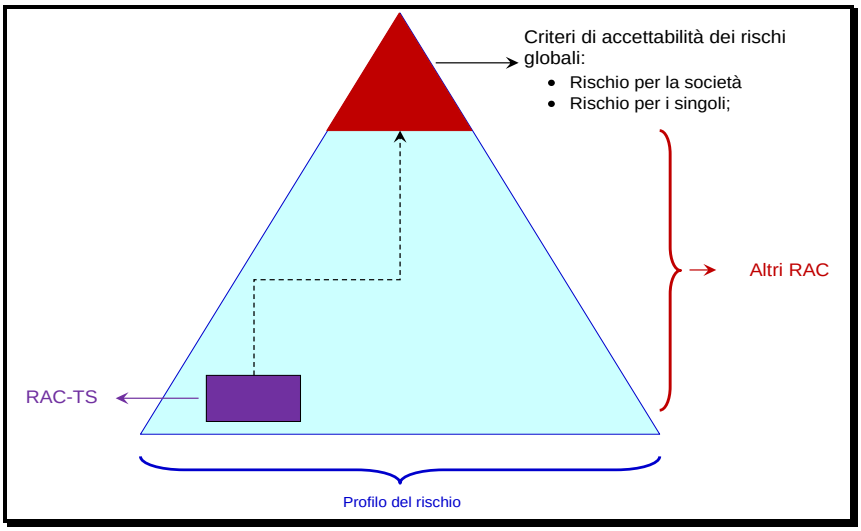

Figura 9 : Piramide dei criteri di accettabilità dei rischi (RAC).

[G 2] I criteri espliciti di accettabilità dei rischi necessari per sostenere il reciproco riconoscimento saranno armonizzati fra gli Stati membri dal lavoro che l'Agenzia sta realizzando sui criteri di accettabilità del rischio. Ove disponibili, informazioni supplementari saranno accluse a questo documento.

[G 3] Nel frattempo, i rischi si possono valutare utilizzando, per esempio, la matrice di rischio che si può trovare nella sezione 4.6 della norma EN 50 126-1 {Ref. 8}. Si possono usare anche altri tipi di criteri idonei, dal momento che si ritiene che tali criteri offrano un livello di sicurezza accettabile nel caso in questione.

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] Non si ritengono necessarie ulteriori spiegazioni.

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] Ulteriori dettagli sul RAC-TS, nonché la specifica degli aspetti e delle funzioni del sistema tecnico ai quali si applica il criterio, sono forniti con una comunicazione separata dell'Agenzia correlata al presente documento: cfr. la sezione A.3. dell'appendice A e il documento di riferimento {Ref. 11}.

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

2.5.5. 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] Non si ritengono necessarie ulteriori spiegazioni.

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] Non si ritengono necessarie ulteriori spiegazioni.

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

(a) the methods used for explicit risk estimation shall reflect correctly the system under assessment and its parameters (including all operational modes);
(b) 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] Non si ritengono necessarie ulteriori spiegazioni.

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. DIMOSTRAZIONE DELLA CONFORMITÀ AI REQUISITI DI SICUREZZA

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] Come spiegato ai punti da [G 3] a [G 6] della sezione 2.1.1, la "dimostrazione della conformità del sistema ai requisiti di sicurezza" comprende le fasi da “6 a 10” del ciclo a “V” delle norme CENELEC (cfr. QUADRO 3 nella Figura 5). Cfr. il punto [G 3] della sezione 2.1.1.

[G 2] Cfr. anche il punto [G 4] della sezione 2.1.1 di questo 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 esempio di valutazioni ed analisi di sicurezza da poter realizzare a livello di sotto-sistemi è rappresentato dalle analisi causali: cfr. Figura 10. Ma si può utilizzare qualsiasi altro metodo per dimostrare la conformità dei sottosistemi ai requisiti di sicurezza stabiliti.

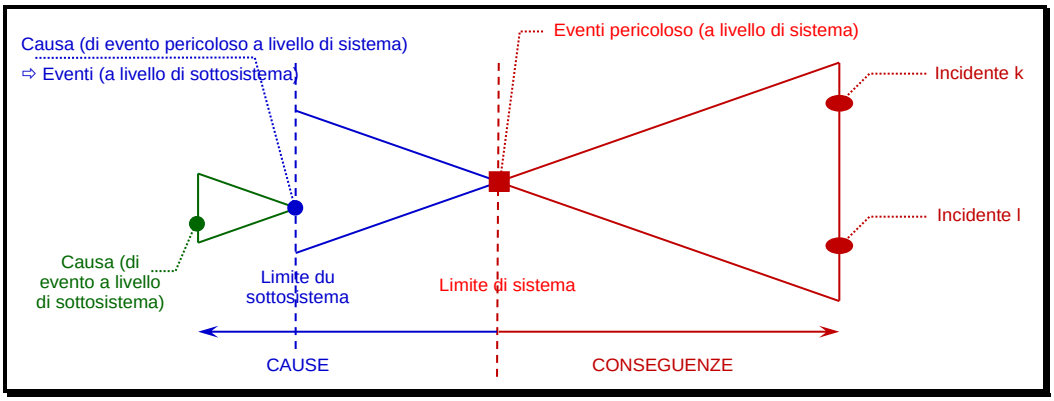

Figura 10 : Figura A.4 della norma EN 50 129: Definizione di eventi pericolosi rispetto al limite del sistema.

[G 2] La strutturazione gerarchica di eventi pericolosi e cause, rispetto a sistemi e sottosistemi, può essere ripetuta per ogni fase di livello inferiore del ciclo a “V” delle norme CENELEC illustrato nella Figura 5. Anche l’individuazione degli eventi pericolosi e le attività di analisi causale (o qualsiasi metodo pertinente), nonché l’uso di codici di buona pratica, sistemi di riferimento simili e analisi e valutazioni esplicite, possono essere ripetuti per ogni fase del ciclo di sviluppo del sistema al fine di ricavare, dalle misure di sicurezza identificate a livello di sottosistema, i requisiti di sicurezza da soddisfare nella fase successiva. Cfr. l’illustrazione della Figura 11.

[G 3] Cfr. anche il punto [G 4] della sezione 2.1.1 di questo 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

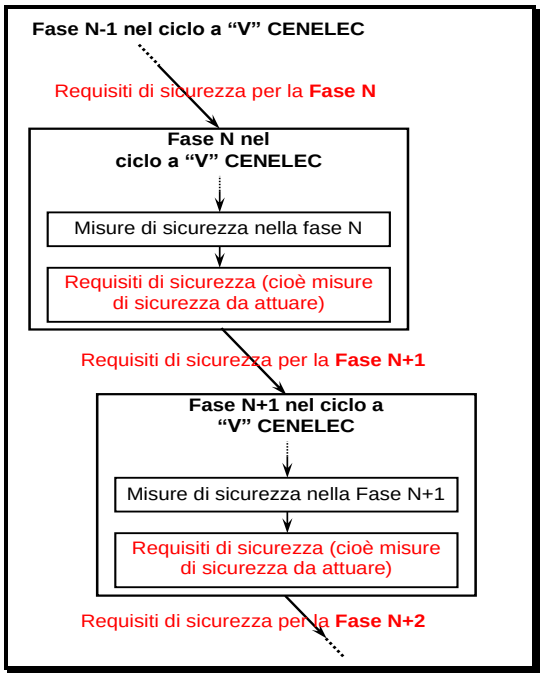

Figura 11 : Deduzione dei requisiti di sicurezza per le fasi di livello inferiore.

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] Tutte le attività rappresentate nel QUADRO 3[(14)] del ciclo a "V" delle norme CENELEC illustrato nella Figura 5 vengono quindi anche sottoposte a valutazione indipendente.

[G 2] Il tipo e il livello di dettaglio per la valutazione indipendente realizzata dagli organismi di valutazione (cioè la valutazione dettagliata o macroscopica) sono spiegati nell'Articolo 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.*

[G 1] Ad esempio, la modalità di estinzione di un incendio potrebbe portare a un nuovo evento pericoloso (soffocamento) che imporrà nuovi requisiti di sicurezza (p.es. una procedura specifica per l'evacuazione dei passeggeri). Un altro esempio è l'uso di vetro temperato per evitare che i finestrini si rompano in caso d'incidente e che i passeggeri siano feriti dal vetro o addirittura sbalzati fuori. Il nuovo evento pericoloso indotto è quindi che l'evacuazione di

(14) *La corrispondenza di attività fra i metodi comuni di sicurezza e la Figura 5 (cioè la Figura 10 del ciclo a "V" della norma CENELEC 50 126) è descritta nella sezione* ***2.1.1****. In particolare, il punto [G 3] della sezione* ***2.1.1*** *elenca quali attività CENELEC sono incluse nella fase del metodo comune di sicurezza denominata "dimostrazione della conformità del sistema ai requisiti di sicurezza".*

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

emergenza dai vagoni attraverso i finestrini è molto più difficile, il che può determinare dei requisiti di sicurezza in base ai quali certi finestrini devono essere appositamente progettati per consentire l'evacuazione.

[G 2] Esempio di una modifica operativa: è vietato a tutti i trasporti di merci pericolose transitare su una linea che attraversa zone densamente popolate. Questo tipo di trasporti deve quindi circolare seguendo un itinerario alternativo con gallerie, creando così diversi tipi di eventi pericolosi.

[G 3] Altri esempi di nuovi eventi pericolosi che potrebbero essere identificati durante la dimostrazione della conformità del sistema ai requisiti di sicurezza si possono trovare nell'appendice A.4.3 della 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

4. GESTIONE DEGLI EVENTI PERICOLOSI

4.1. Procedimento di gestione degli eventi pericolosi

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] L'uso di un registro degli eventi pericolosi per annotare, gestire e controllare informazioni di sicurezza importanti è consigliato anche dalle norme CENELEC 50 126-1 {Ref. 8} e 50 129 {Ref. 7}.

[G 2] Per esempio, a seconda della complessità del sistema, un operatore potrebbe avere uno o più registri degli eventi pericolosi. In entrambi i casi, il(i) registro(i) degli eventi pericolosi e(sono) soggetto(i) alla valutazione indipendente di un organismo/organismi di valutazione Per esempio, una possibile soluzione potrebbe essere quella di avere:

(a) un "registro interno degli eventi pericolosi" per la gestione di tutti i requisiti di sicurezza interni applicabili al sottosistema di cui l'operatore è responsabile. Le dimensioni e il volume di lavoro di gestione dipendono dalla sua struttura e, ovviamente, dalla complessità del sottosistema. Tuttavia, poiché viene usato a scopo di gestione interna, il registro degli eventi pericolosi non deve essere comunicato ad altri operatori. Il registro interno degli eventi pericolosi contiene tutti gli eventi pericolosi identificati che sono controllati, nonché le misure di sicurezza connesse che sono validate;
(b) un "registro esterno degli eventi pericolosi" per trasferire ad altri operatori eventi pericolosi e misure di sicurezza correlate (che l'operatore non è in grado di attuare pienamente da solo), conformemente alla sezione 1.2.2. Generalmente, questo secondo registro degli eventi pericolosi è più piccolo e richiede un volume di lavoro di gestione inferiore (cfr. l'esempio illustrato nella sezione C.16.4. dell'appendice C).

[G 3] Se gestire diversi registri degli eventi pericolosi sembra complicato, un'altra soluzione possibile è gestire tutti gli eventi pericolosi e le misure di sicurezza correlate contemplate dai punti (a) e (b) di cui sopra in un unico registro degli eventi pericolosi, ma con la possibilità di elaborare due relazioni diverse (cfr. l'esempio illustrato nella sezione C.16.3. dell'appendice C):

(a) una relazione del registro degli eventi pericolosi interno, che potrebbe persino non essere necessaria se il registro degli eventi pericolosi è ben strutturato, in modo da consentire una valutazione indipendente;
(b) una relazione del registro degli eventi pericolosi esterno per trasferire gli eventi pericolosi e le misure di sicurezza correlate ad altri operatori.

[G 4] Come spiegato nella sezione 4.2, al termine del progetto quando il sistema è omologato:

(a) tutti gli eventi pericolosi trasferiti ad altri operatori sono controllati nel registro degli eventi pericolosi esterno dell'operatore che li trasferisce. Poiché sono importati e gestiti nei registri degli eventi pericolosi interni degli altri attori, non devono essere gestiti ulteriormente dall'operatore interessato durante il ciclo di vita del (sotto)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

(b) ad ogni modo, tutte le misure di sicurezza correlate non devono essere validate nel registro degli eventi pericolosi per le ragioni spiegate al punto [G 9] della sezione 4.2. È anzi utile che l'impresa che esporta le restrizioni d'uso indichi chiaramente nel proprio registro degli eventi pericolosi che le misure di sicurezza correlate non sono state validate.

[G 5] Viceversa, tutti i registri interni degli eventi pericolosi vengono conservati per l'intero ciclo di vita del (sotto)sistema. Ciò consente di tenere traccia dell'andamento del controllo dei rischi legati agli eventi pericolosi identificati durante il funzionamento e la manutenzione del (sotto)sistema, cioè anche dopo la sua messa in servizio: cfr. QUADRO 4 del ciclo a "V" delle norme CENELEC illustrato nella 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] Le informazioni sugli eventi pericolosi e sulle misure di sicurezza correlate ricevute da altri operatori (cfr. la sezione 1.2.2) comprendono anche tutte le ipotesi(15) e le restrizioni d'uso(15) (altrimenti dette condizioni di applicazione relative alla sicurezza) applicabili ai vari sottosistemi, i *safety case* sulle applicazioni generiche e sui prodotti generici dei vari produttori, ove opportuno.

[G 2] Un possibile esempio di struttura per il registro degli eventi pericolosi è descritto nella sezione C.16. dell'appendice C.

4.2. Scambio di informazioni

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] Per esempio, per il sottosistema odometrico delle apparecchiature ETCS a bordo, il fabbricante può validare in laboratorio gli algoritmi simulando i segnali teorici che potrebbero essere generati dai corrispondenti odometri di rilevamento. Tuttavia, la validazione completa del sottosistema odometrico richiede l'ausilio dell'impresa ferroviaria e del gestore dell'infrastruttura per effettuare la validazione utilizzando un treno vero e il vero contatto ruota del treno-rotaia.

(15) *Consultare il punto [G 5] nella sezione 1.1.5 e le note (9) e (10) a pagina 31 di questo documento per un'ulteriore spiegazione della definizione di safety case di "prodotti generici e applicazioni generiche", "ipotesi e restrizioni d'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

[G 2] Altri esempi potrebbero essere i trasferimenti dai produttori alle imprese ferroviarie di misure di sicurezza operative o di manutenzione per apparecchiature tecniche. Tali misure di sicurezza dovranno essere messe in atto dall'impresa ferroviaria.

[G 3] Al fine di consentire che questi eventi pericolosi, le misure di sicurezza e i rischi correlati siano valutati una seconda volta congiuntamente dalle imprese coinvolte, è utile che l'impresa che li ha identificati fornisca tutte le spiegazioni necessarie per comprendere chiaramente il problema. Potrebbe darsi che la formulazione iniziale degli eventi pericolosi, delle misure di sicurezza e dei rischi debba essere modificata per renderli comprensibili senza doverne discutere di nuovo congiuntamente. La nuova valutazione congiunta degli eventi pericolosi potrebbe portare a identificare nuove misure di sicurezza.

[G 4] L'operatore ricevente, responsabile dell'attuazione, della verifica e della validazione delle misure di sicurezza ricevute o nuove, annota nel proprio registro degli eventi pericolosi tutti gli eventi pericolosi relativi alle misure di sicurezza connesse (sia quelle importate sia quelle identificate congiuntamente).

[G 5] Quando una misura di sicurezza non viene validata pienamente, occorre elaborare e annotare nel registro degli eventi pericolosi una chiara restrizione d'uso (p.es. misure di riduzione operativa). È possibile, infatti, che misure di sicurezza tecniche/progettuali:

(a) non siano attuate correttamente, oppure;
(b) non siano attuate completamente, oppure;
(c) non siano attuate intenzionalmente, per esempio perché sono messe in atto misure di sicurezza diverse da quelle annotate nel registro degli eventi pericolosi (p.es. per motivi di costi). Poiché non sono validate, tali misure di sicurezza devono essere identificate chiaramente nel registro degli eventi pericolosi. E occorre dimostrare/giustificare il motivo per cui le misure di sicurezza attuate al posto di quelle registrate[16] sono adeguate; è altresì necessario dimostrare che, con le misure di sicurezza sostitutive, il sistema è conforme ai requisiti di sicurezza;
(d) ecc.

In questi casi le relative misure di sicurezza tecniche/progettuali non possono essere verificate e validate nel processo di gestione degli eventi pericolosi. I relativi eventi pericolosi e misure di sicurezza devono quindi restare aperti nel registro degli eventi pericolosi al fine di evitare l'uso improprio delle misure di sicurezza per altri sistemi mediante l'applicazione del principio di accettazione del rischio del "sistema di riferimento simile"

[G 6] Generalmente, le misure di sicurezza messe in atto "non correttamente" e/o "non completamente" sono individuate in una fase iniziale del ciclo di vita del sistema e vengono corrette prima dell'accettazione del sistema. Tuttavia, qualora siano individuate troppo tardi per poterle mettere in atto tecnicamente in modo corretto e completo, l'impresa responsabile dell'attuazione e della gestione deve identificare e annotare nel registro degli eventi pericolosi chiare restrizioni d'uso per il sistema sottoposto a valutazione. Tali restrizioni d'uso sono spesso limitazioni di applicazioni operative per il sistema sottoposto a valutazione.

[G 7] Potrebbe anche essere utile annotare nel registro degli eventi pericolosi se le misure di sicurezza connesse saranno attuate correttamente in una fase successiva del ciclo di vita del sistema o se il sistema continuerà ad essere utilizzato con le restrizioni d'uso identificate. Potrebbe anche essere utile annotare nel registro degli eventi pericolosi la giustificazione per

(16) *Se sono state già messe in atto misure di sicurezza diverse da quelle specificate inizialmente, anch'esse devono essere annotate nel registro degli eventi pericolosi.*

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

non aver messo in atto correttamente/completamente le relative misure di sicurezza tecniche.

[G 8] L'operatore che riceve le restrizioni d'uso:

(a) le importa tutte nel proprio registro degli eventi pericolosi;
(b) garantisce che le condizioni d'uso del sistema sottoposto a valutazione siano conformi a tutte le restrizioni d'uso ricevute;
(a) verifica e valida che il sistema sottoposto a valutazione sia conforme a tali restrizioni d'uso

[G 9] A seconda delle decisioni prese dalle imprese interessate:

(a) o le misure tecniche di sicurezza connesse vengono messe in atto correttamente nella progettazione in una fase successiva; in questo caso l'impresa che esporta le restrizioni d'uso continua a tener traccia della corretta attuazione delle misure di sicurezza connesse. Di conseguenza, le relative misure di sicurezza non possono essere validate e gli eventi pericolosi ad esse correlati non possono essere controllati nel registro degli eventi pericolosi di tale impresa fintantoché le corrispondenti misure tecniche di sicurezza non vengono messe in atto pienamente. Questo punto deve essere garantito anche se, nel frattempo, vengono messe in atto le restrizioni d'uso esportate.

(b) oppure le misure tecniche di sicurezza connesse non saranno messe in atto nella progettazione in una fase successiva; in questo caso il sistema continuerà ad essere utilizzato per tutto il suo ciclo di vita con le relative restrizioni d'uso. In una situazione come questa si può procedere come segue:

(1) l'impresa che esporta le restrizioni d'uso non annota le misure di sicurezza connesse come "validate" nel proprio registro degli eventi pericolosi. In questo modo, quando si utilizza il sistema in questione come sistema di riferimento in altri progetti, non si trascureranno i relativi rapporti di sicurezza. Così, anche se un altro operatore accetta di gestire i rischi correlati in modo diverso, è utile che l'impresa che esporta le restrizioni d'uso indichi chiaramente nel proprio registro degli eventi pericolosi che le misure di sicurezza correlate non sono state validate, oppure.

(2) si può modificare la descrizione del sistema per includere le restrizioni d'uso nell'ambito di applicazione del sistema (cioè nelle ipotesi per il sistema) e nei requisiti di sicurezza. In questo modo sarà possibile controllare gli eventi pericolosi. Pertanto, se si utilizza il sistema come sistema di riferimento in un'altra applicazione:

(i) il nuovo sistema dovrà essere usato nelle stesse condizioni (cioè dovrà rispettare le restrizioni d'uso connesse a tali ipotesi), oppure;
(ii) il proponente dovrà eseguire un'ulteriore valutazione del rischio per le deviazioni da tali ipotesi.

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. PROVE OGGETTIVE DERIVANTI DALL'APPLICAZIONE DEL PROCEDIMENTO DI GESTIONE DEI RISCHI

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] Il sistema di gestione della sicurezza (SMS) del gestore dell'infrastruttura e dell'impresa ferroviaria contempla già questi requisiti. Per quanto riguarda gli altri operatori del settore ferroviario che sono interessati dalla modifica significativa, sebbene il sistema di gestione della sicurezza non sia obbligatorio, in generale, per lo meno a livello di progetto essi dispongono di un procedimento di gestione della qualità (QMP) e/o di un procedimento di gestione della sicurezza (SMP). Entrambi questi procedimenti si basano su una gerarchia di documentazione strutturata o all'interno dell'impresa o come minimo all'interno del progetto. Essi si occupano anche delle esigenze documentarie della gestione delle tecniche RAMS. Una documentazione di questo tipo strutturata può essere composta essenzialmente da (cfr. anche la Figura 12):

(a) **Piani di progetto** elaborati per descrivere l'organizzazione da porre in essere per gestire un'attività all'interno di un progetto.

(b) **Procedure di progetto** elaborate per descrivere in dettaglio la modalità per realizzare un compito dedicato. Generalmente, le procedure e le istruzioni esistono all'interno dell'impresa e sono utilizzate come tali. Nuove procedure di progetto vengono elaborate soltanto se è necessario descrivere un compito specifico all'interno del progetto preso in esame.

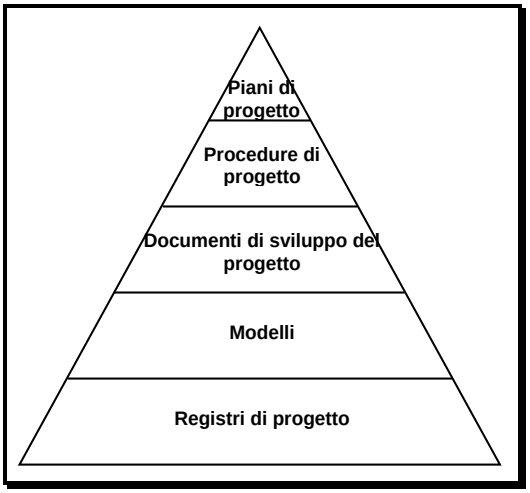

Figura 12: Gerarchia di documentazione strutturata.

(c) **Documenti di sviluppo del progetto** elaborati nel corso del ciclo di vita del sistema rappresentato nella Figura 5.

(d) **Modelli a livello d'impresa o per lo meno di progetto** esistono per i diversi tipi di documenti da produrre.

(e) **Registri di progetto** elaborati nel corso del progetto e necessari per dimostrare la conformità ai procedimenti di gestione della qualità e della sicurezza dell'impresa.

Questo è uno dei modi per soddisfare la necessità di una prova documentata. Ce ne possono però essere degli altri nella misura in cui soddisfano i criteri del metodo comune di sicurezza.

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] Le norme CENELEC consigliano di dimostrare la conformità del sistema ai requisiti funzionali e di sicurezza in un *safety case* (o una relazione sulla sicurezza). Sebbene non sia obbligatorio, l'uso di un *safety case* offre in un documento strutturato a giustificazione della sicurezza:

(a) la prova della gestione della qualità;
(b) la prova della gestione della sicurezza;
(c) la prova della sicurezza funzionale e tecnica;

Al tempo stesso, ha il vantaggio di sostenere e guidare l'organismo/gli organismi di valutazione nella valutazione indipendente della corretta applicazione del metodo comune di sicurezza.

[G 3] Il *safety case* descrive e sintetizza come i documenti del progetto derivanti dall'applicazione dei procedimenti di gestione della qualità e/o della sicurezza dell'impresa o del progetto sono collegati all'interno del procedimento di sviluppo del sistema per dimostrare la sicurezza dello stesso. Generalmente, il *safety case* non comprende grandi quantità di prove dettagliate e di documentazione di supporto, ma offre precisi riferimenti a questo tipo di documenti.

[G 4] ***Safety case* per sistemi tecnici:** Le norme CENELEC si possono usare come linee guida per la redazione e/o per la struttura di *safety case*:

(a) cfr. la norma EN 50 129 {Ref. 7} per "Applicazioni ferroviarie – "Sistemi di comunicazione, segnalamento ed elaborazione & sistemi elettronici di segnalamento relativi alla sicurezza"; l'appendice H.2 della guida EN 50 126-2 {Ref. 9} propone anche una struttura per il *safety case* di sistemi di segnalamento;
(b) cfr. l'appendice H.1 della guida EN 50 126-2 {Ref. 9} sulla struttura del *safety case* per materiale rotabile;
(c) cfr. l'appendice H.3 della guida EN 50 126-2 {Ref. 9} sulla struttura del *safety case* per infrastrutture

Come appare in questi documenti di riferimento, la struttura del *safety case* per sistemi tecnici, nonché il suo contenuto, dipendono dal sistema per il quale si deve fornire la dimostrazione di conformità in materia di sicurezza.

Il *safety case* descritto a grandi linee nell'appendice Appendix H della guida EN 50 126-2 {Ref. 9} fornisce soltanto degli esempi e può non essere adatto a tutti i sistemi del tipo indicato. Di conseguenza, lo schema deve essere utilizzato valutando opportunamente ciò che è adatto ad ogni specifica applicazione.

[G 5] ***Safety case* per aspetti organizzativi ed operativi in sistemi ferroviari:**

Attualmente non esiste alcuna norma specifica sulla struttura, sul contenuto e sulla redazione di *safety case* per aspetti organizzativi ed operativi di un sistema ferroviario. Tuttavia, poiché il *safety case* punta a dimostrare in modo strutturato la conformità del sistema ai suoi requisiti di sicurezza, può essere utilizzata lo stesso tipo di struttura di *safety case* in uso per i sistemi tecnici. Infatti, i riferimenti del punto [G 4] sezione 5.1. danno dei suggerimenti ed una lista di controllo di elementi di cui occuparsi a prescindere dal tipo del sistema sottoposto a valutazione. La gestione di modifiche organizzative ed operative richiede lo stesso tipo di procedimenti di gestione della qualità e della sicurezza delle modifiche tecniche, con una dimostrazione della conformità del sistema ai requisiti di sicurezza specificati. I requisiti delle norme CENELEC non applicabili ad aspetti organizzativi ed operativi sono quelli meramente legati alle strutture di progettazione del sistema tecnico, come ad esempio i principi di "sicurezza propria dell'hardware", la compatibilità elettromagnetica (EMC) ecc.

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] A seconda della complessità del sistema, queste prove possono essere raggruppate in uno o più *safety case*. Cfr. rispettivamente i punti [G 4] e [G 5] della sezione 5.1 per la struttura del *safety case* per sistemi tecnici e per gli aspetti operativi ed organizzativi.

[G 2] Consultare anche la sezione A.4. dell'appendice A su possibili esempi di prove.

[G 3] Generalmente, la vita utile di sistemi tecnici e sotto-sistemi nel settore ferroviario si stima intorno ai 30 anni. Nel corso di questo lungo periodo di tempo è plausibile aspettarsi diverse modifiche significative ai sistemi. Si potrebbero quindi eseguire ulteriori valutazioni del rischio per questi sistemi e per i loro punti d'interazione, con documentazione di accompagnamento che dovrà essere revisionata, integrata e trasferita fra diversi operatori ed imprese che utilizzino registri degli eventi pericolosi. Ciò comporta requisiti piuttosto rigorosi sul controllo della documentazione e sulla gestione della configurazione.

[G 4] È quindi utile che l'impresa che archivia tutte le informazioni sulla valutazione e la gestione dei rischi garantisca che i risultati/le informazioni siano conservate su un supporto fisico leggibile/accessibile durante tutto il ciclo di vita del sistema (p.es. per 30 anni).

[G 5] Le ragioni principali di questo requisito sono, fra l'altro:

(a) garantire che tutte le analisi e i registri di sicurezza del sistema sottoposto a valutazione siano accessibili durante tutto il ciclo di vita del sistema. Così:

(1) in caso di ulteriori modifiche significative allo stesso sistema, sarà disponibile la documentazione più recente;

(2) nel caso in cui sorga un problema durante il ciclo di vita del sistema, è utile poter consultare le relative analisi e i registri di sicurezza;

(b) garantire che le analisi e i registri di sicurezza del sistema sottoposto a valutazione siano accessibili qualora quest'ultimo sia utilizzato in un'altra applicazione come sistema di riferimento simile.

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

ALLEGATO II AL REGOLAMENTO SUL METODO COMUNE DI SICUREZZA

Criteri cui devono conformarsi gli organismi di valutazione

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] Non si ritengono necessarie ulteriori spiegazioni.

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

APPENDICE A: CHIARIMENTI AGGIUNTIVI

A.1. Introduzione

A.1.1. Lo scopo di quest'appendice è quello di facilitare la lettura del presente documento. Invece di fornire grandi quantità di informazioni all'interno del documento, gli argomenti più complessi sono spiegati più a fondo nella presente appendice.

A.2. Classificazione degli eventi pericolosi

A.2.1. La sezione 4.6.3. della norma EN 50 126-1 {Ref. 8}, nonché l'appendice B.2 della guida EN 50 126-2 {Ref. 9} forniscono istruzioni per la catalogazione/classificazione degli eventi pericolosi.

A.3. Criterio di accettabilità del rischio per sistemi tecnici (RAC-TS)

A.3.1. Limite superiore di accettabilità del rischio per sistemi tecnici

A.3.1.1. Il RAC-TS è descritto nella sezione 2.5.4. del documento {Ref. 4}.

A.3.1.2. Lo scopo del RAC-TS è quello di specificare un limite superiore di accettabilità del rischio per sistemi tecnici per i quali i requisiti di sicurezza non possono essere ricavati né mediante l'applicazione di codici di buona pratica né mediante il confronto con sistemi di riferimento simili. Di conseguenza, esso definisce un punto di riferimento a partire dal quale si possono calibrare i metodi di analisi del rischio per i sistemi tecnici. Come descritto nella sezione A.3.6. dell'appendice A del presente documento, questo punto di riferimento o limite superiore di accettabilità del rischio potrebbe essere anche utilizzato per determinare i criteri di accettazione del rischio per altri guasti funzionali di sistemi tecnici, che non hanno una diretta e verosimile potenzialità di provocare conseguenze catastrofiche (cioè altre situazioni gravi). Ma il RAC-TS non è un metodo di analisi del rischio.

A.3.1.3. Il RAC-TS è un criterio semi-quantitativo. Esso riguarda sia i guasti casuali dell'hardware sia i guasti/gli errori sistematici del sistema tecnico. In questo modo sono coperti i guasti/gli errori sistematici del sistema tecnico derivanti, potenzialmente, da errori umani durante il procedimento di sviluppo del sistema tecnico (cioè specifiche, progettazione, implementazione e validazione). Ma gli errori umani durante il funzionamento e la manutenzione dei sistemi tecnici non sono coperti dal RAC-TS.

A.3.1.4. Secondo le appendici A.3 ed A.4 della norma CENELEC 50 129, i guasti/gli errori sistematici non sono quantificabili e quindi l'obiettivo quantitativo deve essere dimostrato soltanto per i guasti casuali dell'hardware, mentre i guasti/gli errori sistematici sono affrontati con metodi qualitativi[17]. *"Poiché non è possibile valutare l'integrità dei guasti sistematici mediante*

(17) *Secondo le norme CENELEC 50 126, 50 128 e 50 129, la cifra quantitativa che riguarda i guasti casuali all'hardware deve essere sempre legata ad un livello d'integrità della sicurezza per gestire i guasti/gli errori sistematici. Di conseguenza, la cifra 10^{-9} h^{-1} del RAC-TS richiede anche la messa in atto di un processo adeguato per gestire correttamente anche i guasti/gli errori sistematici. Ma per facilitare la lettura della nota, spesso si riferisce soltanto ai guasti casuali dell'hardware del sistema tecnico.*

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

metodi quantitativi, i livelli d'integrità di sicurezza sono utilizzati per raggruppare metodi, strumenti e tecniche che, se usati efficacemente, si ritiene offrano un adeguato livello di confidenza nella realizzazione di un sistema con un livello d'integrità specificato."

A.3.1.5. Analogamente, in base alle norme CENELEC, l'integrità del software di sistemi tecnici non è quantificabile. La norma CENELEC 50 128 offre una guida per il procedimento di sviluppo di software connesso con la sicurezza in funzione del livello d'integrità di sicurezza necessario. Ciò comprende i processi di progettazione, verifica, validazione e assicurazione di qualità per il software.
In base alla norma CENELEC 50 128, per un sistema di controllo elettronico programmabile che mette in atto funzioni di sicurezza, il livello d'integrità di sicurezza più alto possibile per il procedimento di sviluppo del software è il SIL 4, che corrisponde ad un indice di pericolo tollerabile quantitativo di $10^{-9}\ h^{-1}$.

A.3.1.6. Di conseguenza, poiché i guasti/gli errori sistematici non possono essere quantificati, devono essere gestiti qualitativamente mettendo in atto un procedimento di qualità e sicurezza compatibile con il livello d'integrità di sicurezza necessario per il sistema sottoposto a valutazione.

a lo scopo del procedimento di qualità è quello di *"ridurre al minimo l'incidenza di errori umani in ogni fase del ciclo di vita del sistema, riducendo così il rischio di guasti sistematici nel sistema stesso"*;

b lo scopo del procedimento di sicurezza è quello di *"ridurre ulteriormente l'incidenza di errori umani connessi con la sicurezza nel corso dell'intero ciclo di vita del sistema, riducendo così al minimo il rischio residuo di guasti sistematici che interessano la sicurezza."*

A.3.1.7. Nelle norme seguenti sono fornite le istruzioni per la gestione dell'incidenza di guasti/errori sistematici, nonché le istruzioni per le possibili misure progettuali al fine di proteggere il sistema tecnico contro guasti per causa/di modo comune (CCF/CMF) e garantire che il sistema entri in uno stato di arresto in condizioni di sicurezza nel caso in cui si verifichino tali guasti/errori:

a) la norma CENELEC 50 126-1 {Ref. 8} e la sua guida 50 126-2 {Ref. 9} elencano le disposizioni CENELEC 50 129 e la loro applicabilità per prove documentate di sistemi diversi da quelli di segnalamento: cfr. la Tabella 9.1 nella guida 50 126-2 {Ref. 9}. Questo elenco fa riferimento alla guida su come affrontare sia i guasti derivanti dal sistema stesso sia gli effetti dell'ambiente sul sistema sottoposto a valutazione;

Per esempio, tecniche/misure per caratteristiche progettuali sono indicate nella *"Tabella E.5: Caratteristiche progettuali (menzionate nel paragrafo 5.4)"* della norma CENELEC 50 129 {Ref. 7}, *"per evitare e controllare i guasti causati da:*

(1) *"qualsiasi guasto di progettazione residuo";*
(2) *"condizioni ambientali";*
(3) *"uso improprio o errori operativi";*
(4) *"qualsiasi guasto residuo nel software";*
(5) *"fattori umani";*

Le appendici D ed E della norma CENELEC 50 129 {Ref. 7} indicano tecniche e misure per evitare i guasti sistematici e per controllare i guasti/gli errori casuali dell'hardware e i guasti/gli errori sistematici per sistemi elettronici connessi alla sicurezza nell'ambito del segnalamento. Molte di queste tecniche e misure possono essere estese a sistemi diversi da quello di segnalamento facendo riferimento alle indicazioni della Tabella 9.1 della guida 50 126-2 {Ref. 9}.

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

b) La norma CENELEC 50 128 offre una guida per il procedimento di sviluppo di software legato alla sicurezza in funzione del livello d'integrità di sicurezza (da SIL 0 a SIL 4) necessario per il software del sistema sottoposto a valutazione.

A.3.1.8. Il RAC-TS rappresenta anche il livello più alto d'integrità che può essere richiesto in base sia alle norme CENELEC sia alle norme IEC. Per facilitarne la consultazione, si citano i requisiti delle norme IEC 61508-1 e CENELEC 50 129:

a) IEC 61508-1: *"Questa norma fissa un limite inferiore alle misure di guasto target, in un modalità di guasto pericolosa, che possono essere richieste. Esse sono specificate come i limiti inferiori per il livello 4 d'integrità di sicurezza. È possibile realizzare progetti di sistemi legati alla sicurezza con valori inferiori per le misure di guasto target di sistemi non complessi, ma si ritiene che i valori indicati nella tabella rappresentino il limite di ciò che si può ottenere attualmente per sistemi relativamente complessi (per esempio sistemi elettronici programmabili legati alla sicurezza."*

b) EN 50129: *"Una funzione che abbia requisiti quantitativi più esigenti di 10-9 h-1 deve essere trattata in uno dei seguenti modi*:

(1) *se è possibile dividere la funzione in sottofunzioni funzionalmente indipendenti, l'indice di pericolo tollerabile (THR) può essere suddiviso fra queste sottofunzioni e si può assegnare un SIL ad ogni sottofunzione;*
(2) *se la funzione non può essere separata, devono essere soddisfatti almeno le misure e i metodi richiesti per il SIL 4, e la funzione deve essere utilizzata in abbinamento con altre misure tecniche o operative al fine di raggiungere il THR necessario."*

A.3.1.9. Tutti i sistemi tecnici devono quindi limitare il requisito di sicurezza quantitativo a questa valore. Se è necessario un livello di protezione superiore, esso non si può ottenere con un solo sistema. Si deve quindi modificare l'architettura del sistema utilizzando, per esempio, due sistemi indipendenti in parallelo che si verificano a vicenda per generare risultati sicuri. Ma questa prassi aumenta decisamente i costi dello sviluppo del sistema tecnico.

Nota: se vi sono funzioni, p.es. sistemi totalmente meccanici che, sulla base dell'esperienza operativa, possono aver ottenuto un livello d'integrità superiore, allora i livelli di sicurezza possono essere descritti da uno specifico codice di buona pratica, oppure si possono stabilire i requisiti di sicurezza mediante un'analisi di similarità con il sistema esistente. Nell'ambito di applicazione del metodo comune di sicurezza, il RAC-TS deve essere applicato soltanto se non esiste alcun codice di buona pratica né sistema di riferimento.

A.3.1.10. Si può sintetizzare quanto segue:

a secondo le norme CENELEC 50 126, 50 128 e 50 129, i guasti/gli errori sistematici nello sviluppo non sono quantificabili;

b l'incidenza di guasti/errori sistematici, nonché il loro rischio residuo, devono essere controllati e gestiti mediante l'applicazione di opportuni procedimenti di qualità e sicurezza compatibili con il livello d'integrità di sicurezza inadeguato al sistema sottoposto a valutazione;

c il livello raggiungibile più elevato d'integrità di sicurezza è il SIL 4, sia per i guasti casuali dell'hardware sia per i guasti/gli errori sistematici di sistemi tecnici;

d questo limite del livello SIL4 d'integrità di sicurezza comporta che anche l'indice massimo di evento pericoloso tollerabile (THR) (cioè l'indice massimo di guasti) per sistemi tecnici sia limitato a 10^{-9} h^{-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

A.3.1.11. Un indice di evento pericoloso tollerabile di $10^{-9}\,h^{-1}$ si può ottenere mediante o una "architettura di sicurezza" (che per definizione raggiunge un tale livello di sicurezza) oppure mediante una "architettura ridondante" (p.es. due canali di elaborazione indipendenti che si verificano reciprocamente).

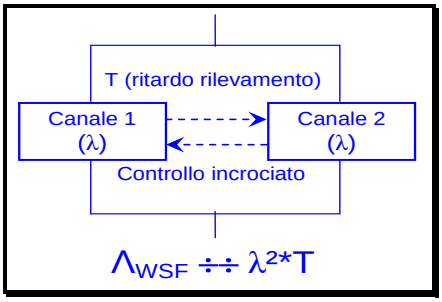

Figura 13: Architettura ridondante per un sistema tecnico.

Per quanto riguarda l'architettura ridondante, si può dimostrare che il guasto completo del sistema tecnico contrario alla sicurezza (Λ_{WSF}) è proporzionale a λ^2*T, dove:

a λ^2 rappresenta il quadrato dell'indice di guasto contrario alla sicurezza di un canale;

b T rappresenta il tempo necessario affinché un canale rilevi il(i) guasto(i) contrario(i) alla sicurezza dell'altro canale. Generalmente è un multiplo del tempo/ciclo di elaborazione di un canale. Di solito T è molto inferiore a 1 secondo.

A.3.1.12. Sulla base di questa formula (λ^2*T), teoricamente si può dimostrare (considerando soltanto i guasti casuali dell'hardware del sistema tecnico – cfr. anche il punto A.3.1.13. dell'appendice A) che è possibile raggiungere un requisito quantitativo di $10^{-9}\,h^{-1}$ per il RAC-TS. I guasti/gli errori sistematici devono essere gestiti da un processo: consultare il punto A.3.1.6. dell'appendice A. Per esempio:

a con un MTBF di 10 000 ore per il valore di affidabilità di un canale, e l'ipotesi conservativa che qualsiasi guasto di canale non è sicuro, il guasto contrario alla sicurezza del canale è $10^{-4}\,h^{-1}$;

b anche con un tempo di 10 minuti (cioè $\approx 2*10^{-3}$ ore) per rilevare il(i) guasto(i) contrario(i) alla sicurezza dell'altro canale, che è anch'essa un'ipotesi conservativa;

Il guasto completo contrario alla sicurezza $\Lambda_{WSF} \approx 2 * 10^{-10}\,h^{-1}$

A.3.1.13. In pratica, per un'architettura ridondante di questo tipo la valutazione dei guasti completi quantitativi dell'hardware contrari alla sicurezza deve tener conto delle misure progettuali adottate al fine di proteggere il sistema tecnico contro guasti per causa/di modo comune (CCF/CMF) e garantire che il sistema entri in uno stato di arresto in condizioni di sicurezza nel caso in cui si verifichino tali guasti/errori. Questa valutazione del guasto completo contrario alla sicurezza (Λ_{WSF}) deve pertanto considerare anche:

a i componenti comuni a tutti i canali, p.es. input singoli o input comuni a tutti i canali, l'alimentazione comune, comparatori, voter ecc.;

b il tempo necessario per rilevare i guasti latenti. Per sistemi tecnici complessi, questo lasso di tempo può essere superiore di diversi ordini di grandezza a 1 secondo;

c l'impatto dei guasti per causa/di modo comune (CCF/CMF).

Una guida su questi argomenti si può trovare nelle norme richiamate nel punto A.3.1.7. dell'appendice A di questo documento.

A.3.2. Diagramma di flusso per il test di applicabilità del RAC-TS

A.3.2.1. La modalità di applicazione del RAC-TS agli eventi pericolosi che derivano da guasti di sistemi tecnici può essere rappresentata come illustrato nella Figura 14.

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.3.2.2. L'applicazione di quel diagramma di flusso su un esempio è illustrata nella sezione C.15. dell'appendice C.

A.3.3. Definizione di un sistema tecnico derivante dal metodo comune di sicurezza

A.3.3.1. Il RAC-TS riguarda esclusivamente sistemi tecnici. Il testo riportato di seguito è la definizione di "sistema tecnico" data dall'Articolo 3(22) del regolamento sul metodo comune di sicurezza:

'sistema tecnico' significa un prodotto o un insieme di prodotti ivi comprese progettazione, implementazione e documentazione di supporto. Lo sviluppo di un sistema tecnico inizia con le sue specifiche di requisiti e finisce con la sua accettazione. Sebbene si tenga conto, nella progettazione, dei rilevanti punti di interazione con il comportamento umano, non sono considerati in un sistema tecnico gli operatori umani e le loro azioni,. Il procedimento di manutenzione è descritto nei relativi manuali ma di fatto non fa parte del sistema tecnico.

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

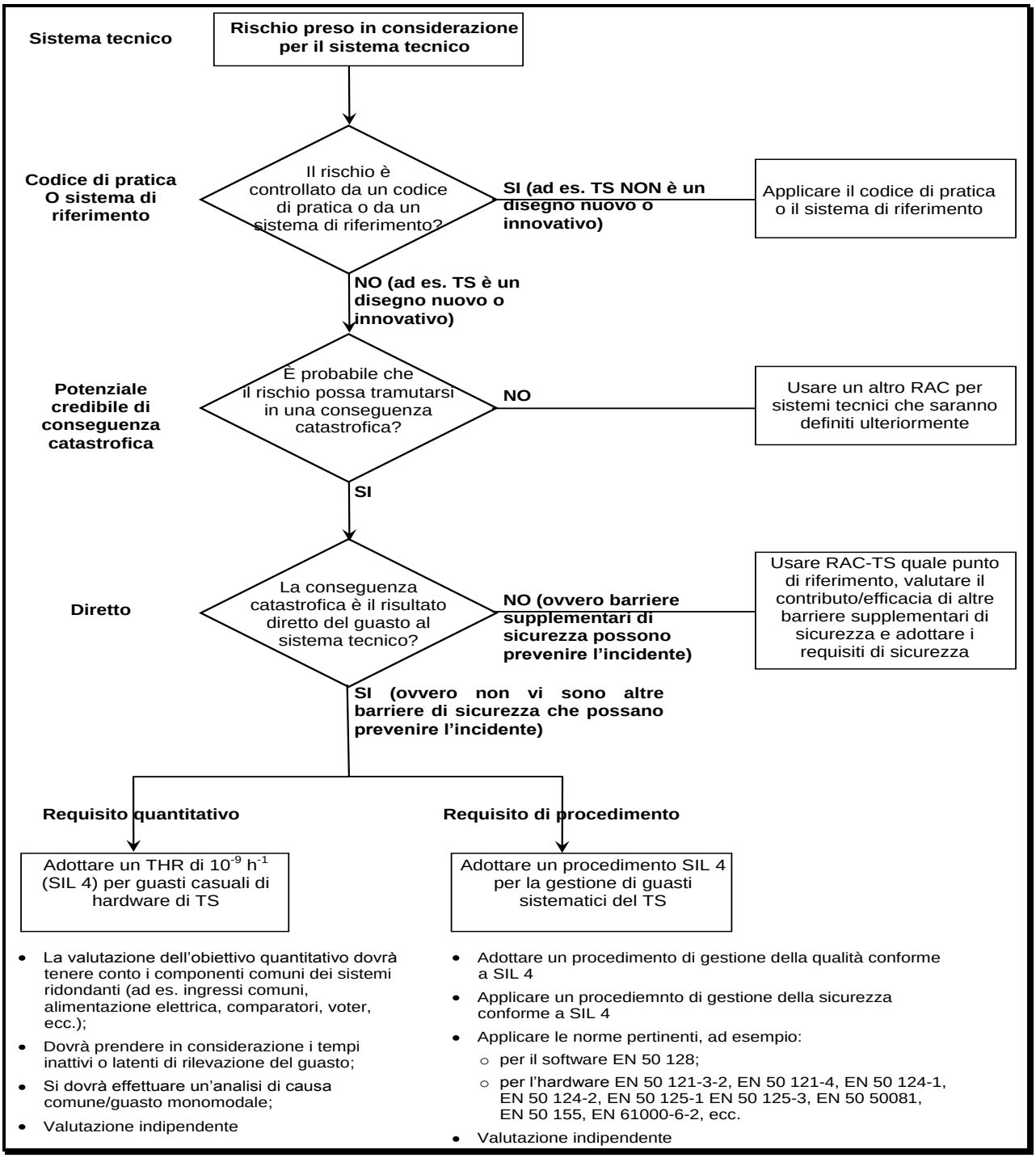

Figura 14 : Diagramma di flusso per il test di applicabilità del RAC-TS.

A.3.4. Spiegazione della definizione di "sistema tecnico"

A.3.4.1. Questa definizione di sistema tecnico descrive portatali campo di applicazione del sistema tecnico: *"sistema tecnico significa un prodotto o un insieme di prodotti ivi comprese*

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

progettazione, implementazione e documentazione di supporto." Di conseguenza, esso comprende e consiste dei seguenti elementi:

a le parti fisiche che costituiscono il sistema tecnico;

b il software correlato (se presente);

c la progettazione e l'implementazione del sistema tecnico comprese, ove opportuno, la configurazione o la parametrizzazione di un prodotto generico rispetto a requisiti specifici della specifica applicazione;

d la documentazione di supporto necessaria per:

(1) lo sviluppo del sistema tecnico;
(2) il funzionamento e la manutenzione del sistema tecnico;

A.3.4.2. Le note connesse a questa definizione specificano ulteriormente il campo di applicazione del sistema tecnico:

a "*Lo sviluppo di un sistema tecnico inizia con le sue specifiche di requisiti e finisce con la sua accettazione di sicurezza*". Esso comprende le fasi da 1 a 10 del ciclo a "V" rappresentato nella Figura 10 della norma CENELEC 50 126-1 {Ref. 8};

b *"Deve tener conto della progettazione di opportuni punti d'interazione con il comportamento umano. Tuttavia, gli operatori umani e le loro azioni non sono inclusi in un sistema tecnico."* Sebbene gli errori umani durante il funzionamento e la manutenzione del sistema tecnico non facciano parte del sistema tecnico in sé, la progettazione dei punti d'interazione con gli operatori umani deve tenerne conto. Lo scopo è quello di ridurre al minimo la probabilità di errori umani dovuti ad un'architettura fragile dei relativi punti d'interazione con gli operatori umani;

c *"La manutenzione non è compresa nella definizione, bensì figura negli appositi manuali."* Ciò significa che il RAC-TS non deve essere applicato al funzionamento e alla manutenzione del sistema tecnico; essi, infatti, dipendono molto da processi ed azioni ad opera di personale umano.
Tuttavia, a supporto della manutenzione di sistemi tecnici, la definizione di sistema tecnico deve comprendere qualsiasi requisito pertinente (p.es. manutenzione periodica preventiva oppure manutenzione correttiva in caso di guasti), con un congruo livello di dettaglio. Ciò che però non fa parte della definizione di sistema tecnico bensì è incluso nei manuali di manutenzione è il modo in cui deve essere organizzata e realizzata la manutenzione sul sistema tecnico in questione.

A.3.4.3. Cfr. anche la sezione A.3.1. dell'appendice A.

A.3.5. Funzioni dei sistemi tecnici ai quali si applica il RAC-TS

A.3.5.1. In base alla definizione del RAC-TS, esso si applica ai guasti contrari alla sicurezza delle funzioni che il sistema tecnico deve assolvere se tali guasti hanno un *"un verosimile* ***diretto*** *potenziale di provocare conseguenze catastrofiche"*: cfr. la sezione 2.5.4. nel documento {Ref. 4}.

A.3.5.2. Il RAC-TS può essere applicato anche a funzioni che riguardano sistemi tecnici ma i cui guasti **non hanno una "potenzialità diretta** *di provocare conseguenze catastrofiche"*. In questo caso, il RAC-TS deve essere applicato come target complessivo per la serie di eventi che portano a conseguenze catastrofiche. A partire da questo target complessivo, l'effettivo

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

contributo di ogni evento, e quindi dei guasti funzionali del sistema tecnico coinvolto nello scenario analizzato, deve esser ricavato in base alla sezione A.3.6. dell'appendice A.
Un tale uso del RAC-TS deve ancora essere discusso e approvato con il gruppo di lavoro sul metodo comune di sicurezza.

A.3.5.3. A quali funzioni del sistema tecnico si applica il RAC-TS? Secondo la norma IEC 61226:2005:

a una funzione è definita in questo contesto come uno "*specifico scopo o obiettivo da raggiungere che può essere specificato o descritto senza fare riferimento ai mezzi materiali per raggiungerlo";*

b una funzione (considerata come una scatola nera) trasferisce parametri di input (p.es. materiale, energia, informazioni) in parametri di output connessi all'obiettivo (p.es. materiale, energia, informazioni);

c l'analisi della funzione è indipendente dalla sua realizzazione tecnica.

A.3.5.4. Il RAC-TS è applicabile ai seguenti tipi di funzioni:

a esempi per il sottosistema di bordo ETCS:

(1) "fornire al macchinista le informazioni necessarie affinché possa guidare il treno in condizioni di sicurezza e frenare in caso di eccesso di velocità". Sulla base delle informazioni ricevute dagli impianti a terra (velocità ammessa) e sul calcolo della velocità del treno fatto dall'ETCS di bordo, il macchinista e l'ETCS di bordo sono in grado di controllare che il treno non superi il limite di velocità consentita. Il RAC-TS si applica alla valutazione della velocità del treno fatta da bordo del treno poiché:

(i) non vi sono barriere supplementari (dirette) laddove anche l'informazione fornita al macchinista è sottostimata;
(ii) l'eccesso di velocità del treno potrebbe provocare il deragliamento, che è un incidente con potenziali conseguenze catastrofiche;

(2) "fornire al macchinista le informazioni necessarie affinché possa guidare il treno in condizioni di sicurezza e frenare in caso di violazione dell'autorizzazione al movimento consentita";

b esempio per un circuito di binario: "rilevare l'occupazione del tratto di binario". Il RAC-TS sarà applicabile come tale a questa funzione soltanto se non è implementata una funzione di "monitoraggio sequenziale" nel sistema di interlocking;
c esempio per un deviatoio: "controllare la posizione del deviatoio";

A.3.5.5. Alcune norme definiscono anche funzioni alle quali si potrebbe applicare il RAC-TS. Per esempio:

a la norma prEN 0015380-4 {Ref. 13} (ModTrain Work) definisce nella sua parte normativa tre livelli gerarchici di funzione (ampliati fino a cinque livelli in allegati informativi). In totale, la norma prEN 0015380-4 definisce diverse centinaia di funzioni correlate ai treni;
b in linea di massima, si raccomanda di selezionare le funzioni dai primi tre livelli della prEN 0015380-4 (ma non al di sotto), tenendo anche conto della struttura di scomposizione del prodotto;
c per le funzioni che non rientrano nell'ambito di applicazione della prEN 0015380-4, il livello funzionale adeguato deve essere deciso per confronto, utilizzando un parere esperto.

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

Questi esempi di funzioni della prEN 0015380-4 devono essere ancora approfonditi dall'Agenzia nell'ambito del lavoro che sta svolgendo sui rischi ampiamente accettabili e sui criteri di accettazione del rischio.

A.3.5.6. Il RAC-TS è applicabile anche, per esempio, alla seguente funzione della prEN 0015380-4: *"controllo dell'inclinazione"* (codice = CLB). Questa funzione si potrebbe usare a livello di sistema nei due modi indicati di seguito:

primo caso: il treno deve inclinarsi in curva per la comodità dei passeggeri e deve controllare la conformità dello scartamento del treno all'infrastruttura a terra;

d secondo caso: il treno deve inclinarsi in curva solo per la comodità dei passeggeri ma non deve controllare la conformità dello scartamento del treno all'infrastruttura a terra;

Il RAC-TS sarà applicato nel primo caso ma non nel secondo in quanto il guasto della funzione d'inclinazione non ha conseguenze catastrofiche.

A.3.5.7. L'esempio (b) del punto A.3.5.4. e gli esempi del punto A.3.5.6. dell'appendice A mostrano chiaramente che non sarà fattibile creare un elenco predefinito di funzioni a cui il RAC-TS si applica in tutti i casi. Questo, infatti, dipenderà sempre da come il sistema utilizzerà queste funzioni di sottosistema.

A.3.5.8. Un esempio di applicazione del RAC-TS è illustrato nella sezione C.15. dell'appendice C.

A.3.6. Esempi di applicazione del RAC-TS

A.3.6.1. Introduzione

a questo capitolo mostra esempi di come determinare l'indice di guasti per gli altri livelli di gravità degli eventi pericolosi e come si possono ricavare requisiti di sicurezza inferiori a $10^{-9}\,h^{-1}$. Questo documento non predilige né impone alcun metodo in particolare. Esso mostra semplicemente a titolo informativo come si può usare il RAC-TS per calibrare alcuni metodi ampiamente utilizzati. Questo aspetto deve essere sviluppato ulteriormente dall'Agenzia nel lavoro che sta svolgendo sui rischi ampiamente accettabili e sui criteri di accettazione del rischio.

b effettivamente, il RAC-TS si può applicare in modo diretto soltanto in un ridotto numero di casi, poiché in pratica non molti guasti funzionali di sistemi tecnici provocano direttamente incidenti con conseguenze potenzialmente catastrofiche. Di conseguenza, al fine di applicare il criterio agli eventi pericolosi con conseguenze non catastrofiche e di determinare l'indice di guasti target, è possibile operare dei trade-off (p.es. calibrando una matrice di rischio con questo criterio) fra parametri diversi, p.es. gravità rispetto a frequenza.

A.3.6.2. Esempio 1: Trade-off per rischi diretti

a il RAC-TS può essere applicato facilmente a scenari che differiscono soltanto di qualche parametro indipendente dalle condizioni di riferimento definite nel RAC-TS della sezione 2.5.4. del regolamento sul metodo comune di sicurezza {Ref. 3};

b supponiamo che per un particolare parametro p il rapporto con il rischio sia moltiplicativo. Supponiamo che nella condizione di riferimento è presente p* mentre nello scenario alternativo sia applicabile p'. In questo caso soltanto il rapporto p*/p' è importante e l'indice di occorrenza può essere ridotto. Questa procedura può essere ripetuta se i parametri sono indipendenti.

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 Esempio:

(1) supponiamo che il potenziale reale delle conseguenze catastrofiche sia stato stimato da un parere esperto in dieci volte inferiore al potenziale nelle condizioni di riferimento della sezione 2.5.4 del regolamento sul metodo comune di sicurezza. Il requisito sarebbe quindi $10^{-8}\,h^{-1}$ invece di $10^{-9}\,h^{-1}$.

(2) supponiamo la presenza di una barriera di sicurezza supplementare mediante un altro sistema tecnico (indipendente dalle conseguenze) che è efficace nel 50% dei casi, se identificato;

(3) il requisito di sicurezza sarebbe quindi $5*10^{-7}\,h^{-1}$ (cioè $0,5*10^{-8}\,h^{-1}$) invece di $10^{-9}\,h^{-1}$.

A.3.6.3. Esempio 2: Calibratura di una matrice di rischio

a al fine di utilizzare correttamente il RAC-TS in una matrice di rischio, la matrice deve riferirsi al livello di sistema corretto (paragonabile a quello fornito nella sezione A.3.5. dell'appendice A).

b il RAC-TS definisce accettabile un campo che corrisponde alla coordinata gravità catastrofica (frequenza $10^{-9}\,h^{-1}$): cfr. campo rosso nella Tabella 5. Tutti i campi che si riferiscono ad una frequenza maggiore devono essere etichettati come "inaccettabili". È da notare che soltanto in caso di verosimile diretta potenzialità di conseguenze catastrofiche, la frequenza di incidenti è uguale alla frequenza di guasti funzionali.

c poi si può compilare il resto della matrice, ma si deve tener conto di effetti quali l'avversione al rischio o la scalatura delle classificazioni. Nel più semplice dei casi di scalatura lineare per decine (come illustrato nella Tabella 5 dalla freccia) il campo etichettato come "accettabile" dal RAC-TS è estrapolato linearmente al resto della matrice. Ciò significa che tutti i campi nella stessa diagonale (o al di sotto della diagonale) sono etichettati come "accettabili". Anche i campi al di sotto possono essere etichettati come "accettabili".

Tabella 5: Esempio tipico di una matrice di rischio calibrata.

Frequenza di un incidente (causato da un evento pericoloso	**Livelli di rischio**			
Frequente (10^{-4} /ora)	**Intollerabile**	**Intollerabile**	**Intollerabile**	**Intollerabile**
Probabile (10^{-5} /ora)	**Intollerabile**	**Intollerabile**	**Intollerabile**	**Intollerabile**
Occasionale (10^{-6} /ora)	**Accettabile**	**Intollerabile**	**Intollerabile**	**Intollerabile**
Remoto (10^{-7} /ora)	**Accettabile**	**Accettabile**	**Intollerabile**	**Intollerabile**
Improbabile (10^{-8} /ora)	**Accettabile**	**Accettabile**	**Accettabile**	**Intollerabile**
Inverosimile (10^{-9} /ora)	**Accettabile**	**Accettabile**	**Accettabile**	**Accettabile**
	Insignificante	Marginale	Critico	Catastrofico
	Livelli di gravità di conseguenze di eventi pericolosi (cioè incidenti)			

d una volta compilata la matrice, questa può essere applicata anche a eventi pericolosi non catastrofici. Se, per esempio, la gravità di un altro guasto funzionale è classificata come "critica", con la matrice di rischio calibrata la frequenza di incidenti tollerabile deve essere inferiore a "improbabile" (o persino di meno).

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

e si tenga presente che l'uso della matrice di rischio può portare a risultati eccessivamente prudenti, quando si applica a frequenze di guasti funzionali (cioè per guasti funzionali che non provocano direttamente incidenti).

A.3.6.4. Principio per la calibrazione di altri metodi di analisi del rischio

Altri metodi di analisi del rischio, per esempio lo schema proposto dell'indice RPN o il grafico del rischio della norma VDV 331 o della IEC 61508 possono anch'essi essere calibrati mediante una procedura simile a quella descritta per la matrice di rischio:

a) primo passo: classificare il valore di riferimento del RAC-TS come tollerabile e i punti con maggiore frequenza o maggiore gravità come intollerabili.

b) secondo passo: utilizzare i meccanismi di trade-off del particolare metodo per estrapolare la tollerabilità del rischio a eventi pericolosi non catastrofici (utilizzando il trade-off del rischio lineare come punto di partenza).

c) terzo passo: per eventi pericolosi non catastrofici, quindi, si può ricavare il RAC-TS dal metodo di analisi calibrata del rischio, comparando la coordinata (frequenza; gravità) alla curva FN così ottenuta.

A.3.7. Conclusioni per il RAC-TS

A.3.7.1. Nel quadro generale di valutazione del rischio proposto dal metodo comune di sicurezza, i criteri di accettazione del rischio sono necessari per determinare quando il livello residuo di rischio diventa accettabile e, di conseguenza, quando sospendere la stima esplicita del rischio.

A.3.7.2. Il RAC-TS è un target di progettazione (10^{-9} h^{-1}) per sistemi tecnici.

A.3.7.3. Gli scopi principali del RAC-TS sono:

a specificare un limite superiore di accettabilità del rischio e, di conseguenza, un valore di riferimento a partire dal quale si possono calibrare i metodi di analisi del rischio per i sistemi tecnici.
b consentire il reciproco riconoscimento di sistemi tecnici poiché il rischio connesso e le valutazioni della sicurezza saranno valutate utilizzando lo stesso criterio di accettazione del rischio in tutti gli Stati Membri;
c risparmiare sui costi in quanto non richiede requisiti di sicurezza quantitativi inutilmente elevati;
d facilitare la concorrenza fra diversi produttori. L'uso di diversi criteri di accettazione del rischio a seconda del proponente o dello Stato Membro porterebbe l'industria a realizzare un gran numero di dimostrazioni diverse sugli stessi sistemi tecnici. In questo modo si pregiudicherebbe la competitività dei produttori e si rincarerebbero inutilmente i prodotti.

A.3.7.4. Il requisito semi-quantitativo contenuto nel RAC-TS non sempre deve essere dimostrato per i sistemi tecnici. Infatti, nell'ambito del metodo comune di sicurezza, il RAC-TS deve essere applicato soltanto a sistemi tecnici per i quali gli eventi pericolosi identificati non possono essere adeguatamente controllati né mediante l'uso di codici di buona pratica né mediante il confronto con sistemi di riferimento simili. In questo modo si possono indicare requisiti di sicurezza inferiori, a condizione che si possa mantenere il livello di sicurezza complessivo.

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.3.7.5. Soltanto quando non esistono né codici di buona pratica né sistemi di riferimento, occorre un criterio semi-quantitativo di accettazione del rischio armonizzato per sistemi tecnici.

A.3.7.6. Poiché il livello d'integrità di sicurezza per guasti/errori sistematici si limita al SIL 4, anche il livello d'integrità di sicurezza per i guasti casuali dell'hardware di sistemi tecnici deve essere limitato al SIL 4, il che corrisponde a un indice massimo di evento pericoloso tollerabile (THR) di $10^{-9}\,h^{-1}$ (cioè l'indice massimo di guasti). Secondo la norma CENELEC 50 129, se sono necessari requisiti di sicurezza più esigenti, essi non possono essere soddisfatti soltanto con un sistema; si deve quindi modificare l'architettura del sistema utilizzando per esempio due sistemi, cosa che inevitabilmente aumenta i costi del sistema tecnico in modo drastico. Per maggiori dettagli, consultare la sezione A.3.1. dell'appendice A.

A.3.7.7. Infine, la sezione A.3.6. dell'appendice A descrive come si può utilizzare il RAC-TS come punto di riferimento per calibrare particolari metodi di analisi del rischio quando i sistemi tecnici hanno una potenzialità di conseguenze meno gravi di quelle catastrofiche.

A.4. Prova della valutazione della sicurezza

A.4.1. Questa sezione fornisce una guida sulle prove che generalmente vengono fornite ad un organismo di valutazione per consentire la valutazione indipendente ed ottenere l'accettazione della sicurezza, senza però pregiudicare i requisiti nazionali di un determinato Stato Membro. Può essere utilizzata come lista di controllo per verificare che tutti gli aspetti correlati siano coperti e documentati, ove opportuno, durante l'applicazione del metodo comune di sicurezza.

A.4.2. Piano di sicurezza: Il CENELEC consiglia di elaborare un piano di sicurezza all'inizio del progetto oppure, se per il progetto in questione non è una soluzione pratica, di inserirne la descrizione in qualsiasi altro documento pertinente. Se all'inizio del progetto vengono nominati degli organismi di valutazione, il piano di sicurezza può anche essere presentato loro per un parere. In linea di massima il piano di sicurezza descrive:

a l'organizzazione posta in essere e la competenza delle persone coinvolte nello sviluppo e nella valutazione del rischio;
b tutte le attività relative alla sicurezza, pianificate nel corso delle varie fasi del progetto, nonché i risultati attesi;

A.4.3. Prove richieste dalla fase di definizione del sistema:

a descrizione del sistema:
   (1) definizione delle dimensioni/limiti del sistema;
   (2) descrizione delle funzioni;
   (3) descrizione della struttura del sistema;
   (4) descrizione di condizioni operative ed ambientali;
b descrizione di punti d'interazione esterni;
c descrizione di punti d'interazione interni;
d descrizione delle fasi del ciclo di vita;
e descrizione di principi di sicurezza;
f descrizione delle ipotesi che definiscono i limiti per la valutazione del rischio;

A.4.4. Al fine di consentire la realizzazione della valutazione del rischio, la definizione del sistema tiene conto del contesto della modifica che si vuole adottare:

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 se la modifica voluta è una modifica di un sistema esistente, la definizione del sistema descrive sia il sistema prima della modifica sia la modifica prevista:
b se la modifica voluta è la costruzione di un nuovo sistema, la descrizione si limita alla definizione del sistema, in quanto non vi è la descrizione di un sistema esistente.

A.4.5. Prove richieste dalla fase di individuazione degli eventi pericolosi:

a descrizione e giustificazione (comprese le limitazioni) di metodi e strumenti per l'individuazione di eventi pericolosi (metodo top-down, bottom-up, HAZOP ecc.);
b risultati:

(1) elenchi di eventi pericolosi:
(2) evento pericoloso rispetto al limite del sistema;
(3) evento pericoloso dei sottosistemi;
(4) eventi pericolosi per i punti d'interazione;
(5) le misure di sicurezza che potrebbero essere individuate durante questa fase;

A.4.6. Dalla fase di analisi del rischio si richiedono anche le seguenti prove:

a quando per controllare gli eventi pericolosi si usano codici di buona pratica, la dimostrazione che il sistema sottoposto a valutazione soddisfa tutti i pertinenti requisiti dei codici di buona pratica. Ciò comprende la dimostrazione della corretta applicazione dei codici di buona pratica in questione;

b quando per controllare gli eventi pericolosi si usano sistemi di riferimento simili:

(1) definizione, per il sistema sottoposto a valutazione, dei requisiti di sicurezza a partire dagli opportuni sistemi di riferimento;
(2) dimostrazione che il sistema sottoposto a valutazione viene utilizzato in condizioni operative ed ambientali simili a quelle del relativo sistema di riferimento. Se ciò non è possibile, la dimostrazione che le deviazioni dal sistema di riferimento vengono valutate correttamente;
(3) la dimostrazione che i requisiti di sicurezza di sistemi di riferimento sono applicati correttamente nel sistema sottoposto a valutazione;

c quando per controllare gli eventi pericolosi si usa la stima esplicita del rischio:

(1) descrizione e giustificazione (comprese le limitazioni) di metodi e strumenti per l'analisi del rischio (analisi qualitativa, quantitativa, semi-quantitativa, di non regressione,…);
(2) individuazione di misure di sicurezza esistenti e fattori di riduzione del rischio per ogni evento pericoloso (compresi gli aspetti del fattore umano);
(3) valutazione e classificazione del rischio per ogni evento pericoloso:

(i) stima delle conseguenze dell'evento pericoloso e relativa giustificazione (con ipotesi e condizioni);
(ii) stima della frequenza dell'evento pericoloso e relativa giustificazione (con ipotesi e condizioni);
(iii) classificazione degli eventi pericolosi in base alla loro rilevanza e frequenza;

(4) individuazione di opportune misure di sicurezza supplementari che portano a rischi accettabili per ogni evento pericoloso (procedimento iterativo dopo la fase di valutazione del rischio);

A.4.7. Prove richieste della valutazione del rischio:

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 quando si realizza la stima esplicita del rischio:

(1) definizione e giustificazione di criteri di valutazione del rischio per ogni evento pericoloso;
(2) dimostrazione/giustificazione che le misure di sicurezza e i requisiti di sicurezza coprono ogni evento pericoloso ad un livello accettabile (secondo il criterio di valutazione del rischio di cui sopra);

b ai sensi delle sezioni 2.3.5 e 2.4.3 del regolamento sul metodo comune di sicurezza i rischi coperti dall'applicazione di codici di buona pratica e dal confronto con sistemi di riferimento, sono considerati implicitamente accettabili a condizione che, rispettivamente, (cfr. cerchio tratteggiato nella Figura 1):

(1) siano soddisfatte le condizioni di applicazione di codici di buona pratica indicate nella sezione 2.3.2;
(2) siano soddisfatte le condizioni per l'uso di un sistema di riferimento indicate nella sezione 2.4.2;

I criteri di accettazione del rischio sono impliciti per questi due principi di accettazione del rischio.

A.4.8. Prove della gestione degli eventi pericolosi:

a annotazione di tutti gli eventi pericolosi in un apposito registro contenente i seguenti elementi:

(1) evento pericoloso identificato;
(2) misure di sicurezza che evitano il verificarsi dell'evento pericoloso o ne attenuano le conseguenze;
(3) requisiti di sicurezza sulle misure;
(4) parte interessata del sistema;
(5) operatore responsabile delle misure di sicurezza;
(6) stato dell'evento pericoloso (p.es. aperto, risolto, eliminato, trasferito, controllato ecc.);
(7) data di registrazione, revisione e controllo di ogni evento pericoloso;

b descrizione di come gli eventi pericolosi saranno gestiti efficacemente durante l'intero ciclo di vita;
c descrizione dello scambio di informazioni fra le parti per gli eventi pericolosi nei punti d'interazione e per l'assegnazione di responsabilità.

A.4.9. Prove relative alla qualità del procedimento di valutazione del rischio e valutazione:

a descrizione delle persone coinvolte nel procedimento e della loro competenza;
b per le stime esplicite del rischio, descrizione di informazioni, dati ed altre statistiche utilizzate nel procedimento, e giustificazione della loro idoneità (p.es. studio di sensibilità sui dati utilizzati).

A.4.10. Prove di conformità a requisiti di sicurezza:

a elenco di norme utilizzate;
b descrizione di principi progettuali e operativi;
c prove dell'applicazione di un buon sistema di gestione della qualità e della sicurezza per il progetto: cfr. il punto [G 3] della sezione 1.1.2;
d sintesi di relazioni di analisi sulla sicurezza (p.es. analisi delle cause di eventi pericolosi) che dimostri il soddisfacimento dei requisiti di sicurezza;

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

e descrizione e giustificazione di metodi e strumenti (FMECA, FTA, …) utilizzati per l'analisi delle cause degli eventi pericolosi;
f sintesi di test di verifica e validazione della sicurezza.

A.4.11. Safety case: Il CENELEC consiglia di raggruppare e sintetizzare tutte le prove menzionate in precedenza in un unico documento da presentare all'organismo di valutazione: cfr. i punti [G 4] e [G 5] della sezione 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

APPENDICE B: ESEMPI DI TECNICHE E STRUMENTI A SUPPORTO DEL PROCEDIMENTO DI VALUTAZIONE DEI RISCHI

B.1. Esempi di tecniche e strumenti per la realizzazione delle attività di valutazione dei rischi previste dal metodo comune di sicurezza si possono trovare nell'allegato E della guida EN 50126-2 {Ref. 9}. Una sintesi di tecniche e strumenti è illustrata nella Tabella E.1. È descritta ogni tecnica e, all'occorrenza, per maggiori informazioni è indicato un riferimento ad altre norme.

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

APPENDIX C: ESEMPI

C.1. Introduzione

C.1.1. Lo scopo di quest'appendice è quello di facilitare la lettura del presente documento. Essa riunisce tutti gli esempi raccolti allo scopo di facilitare l'applicazione del metodo comune di sicurezza.

C.1.2. Le valutazioni del rischio o della sicurezza degli esempi forniti in quest'appendice non derivano dall'applicazione del procedimento del metodo comune di sicurezza in quanto sono state effettuate prima dell'esistenza del regolamento sul metodo comune di sicurezza. Gli esempi possono essere classificati in:

a rispetto alla loro origine, esempi ricevuti da esperti del gruppo di lavoro sul metodo comune di sicurezza
b intenzionalmente senza riferimento alla loro origine, esempi anch'essi ricevuti da esperti del gruppo di lavoro sul metodo comune di sicurezza. Gli esperti in questione hanno chiesto di mantenere riservata l'origine degli esempi;
c esempi la cui origine non è menzionata e che sono stati prodotti da membri del personale dell'Agenzia sulla base della loro personale esperienza professionale precedente.

Per ogni esempio viene data tracciabilità del procedimento applicato e di quello richiesto dal metodo comune di sicurezza, nonché le argomentazioni e il valore aggiunto per fare gli ulteriori passi (se ve ne sono) richiesti dal metodo comune di sicurezza.

C.2. Esempi di applicazione di criteri per modifiche significative nell'Articolo 4 (2)

C.2.1. L'Agenzia sta lavorando alla definizione di ciò che può essere considerato come una "modifica significativa". Un esempio di questo lavoro è fornito in questa sezione su come applicare i criteri dell'Articolo 4 (2).

C.2.2. La modifica consiste nel cambiare, in un passaggio a livello manuale, il modo in cui gli operatori della circolazione comunicano le informazioni sulla direzione di un treno in arrivo all'operatore del passaggio a livello. La modifica è rappresentata nella Figura 15.

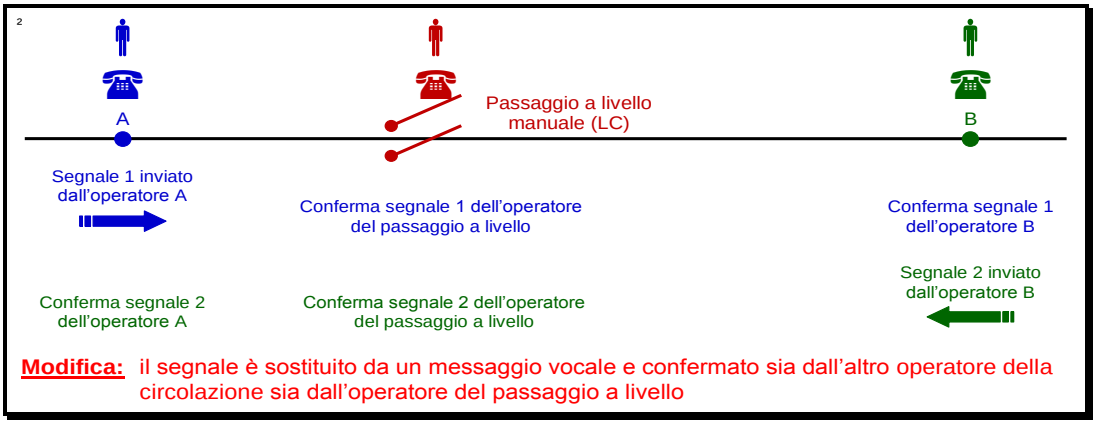

Figura 15 : Esempio di una modifica non significativa
Messaggio telefonico per controllare un passaggio a livello.

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 esistente: prima di realizzare la modifica desiderata, le informazioni sulla direzione di un treno in arrivo erano indicate automaticamente all'operatore del passaggio a livello mediante lo squillo del telefono. Il tono era diverso a seconda della provenienza della chiamata.

C.2.4. Modifica desiderata: poiché il vecchio sistema telefonico diventa obsoleto e deve essere sostituito da un nuovo sistema digitale, tecnicamente le informazioni in questione non possono più essere inserite nel tono. Il tono è esattamente lo stesso, indipendentemente dall'operatore della circolazione da cui proviene. Si decide quindi di ottenere la stessa funzione mediante una procedura operativa:

a alla partenza del treno, l'operatore della circolazione informa verbalmente l'operatore del passaggio a livello della direzione del treno in arrivo;
b l'informazione viene verificata con la tabella oraria e confermata sia dall'operatore del passaggio a livello sia dall'altro operatore della circolazione, al fine di evitare malintesi da parte dell'operatore.

La modifica desiderata e la procedura operativa connessa sono illustrate nella Figura 15.

C.2.5. Sebbene la modifica sembri avere un potenziale impatto sulla sicurezza (rischio di non chiudere in tempo la barriera del passaggio a livello), atri criteri dell'Articolo 4 (2), quali:

a scarsa complessità;
b mancanza d'innovazione; e
c facile monitoraggio;

possono indicare che la modifica desiderata non è una modifica significativa.

C.2.6. In questo esempio sono comunque necessarie alcune analisi o argomentazioni sulla sicurezza per dimostrare che, per questo compito di sicurezza essenziale, sostituire un vecchio sistema tecnico con una procedura operativa (con controllo incrociato eseguito dal personale) porterebbe ad un livello di sicurezza simile. La domanda è se ciò richiederebbe l'applicazione dell'intero procedimento del metodo comune di sicurezza, con registro degli eventi pericolosi, valutazione indipendente da parte di un organismo di valutazione ecc. In questo caso, è discutibile se ciò porterebbe del valore aggiunto, ed implica che una modifica di questo tipo non potrebbe quindi essere qualificata come significativa.

C.3. Esempi di punti d'interazione fra operatori del settore ferroviario

C.3.1. Di seguito sono riportati alcuni esempi di punti d'interazione e motivi di cooperazione fra operatori del settore ferroviario:

a Gestore Infrastruttura - Gestore Infrastruttura: per esempio, entrambe le infrastrutture devono prevedere misure di sicurezza per garantire un transito sicuro dei treni da un'infrastruttura all'altra;
b Gestore Infrastruttura - Impresa ferroviaria: per esempio, potrebbero esserci specifiche norme operative che dipendono dall'infrastruttura e che devono essere osservate dal macchinista;
c Gestore Infrastruttura – Produttore: per esempio, i sottosistemi del produttore potrebbero avere restrizioni d'uso che il gestore dell'infrastruttura deve rispettare;

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 Gestore Infrastruttura – Fornitore di servizi: per esempio, potrebbero esserci specifici vincoli di manutenzione per l'infrastruttura che il subappaltatore delle attività di manutenzione deve rispettare;

e Impresa ferroviaria – Produttore: per esempio, i sottosistemi del produttore potrebbero avere restrizioni d'uso che l'impresa ferroviaria deve rispettare;

f Impresa ferroviaria – Fornitore di servizi: per esempio, potrebbero esserci specifici vincoli di manutenzione per l'infrastruttura che il subappaltatore delle attività di manutenzione deve rispettare;

g Impresa ferroviaria – Addetti alla manutenzione: per esempio, per i veicoli potrebbero esserci restrizioni d'uso specifiche che l'impresa ferroviaria che li gestisce deve rispettare;

h Produttore – Produttore: per esempio, la gestione di punti d'interazione tecnici connessi alla sicurezza fra sottosistemi di due diversi produttori;

i Produttore – Fornitore di servizi: per esempio, la gestione da parte del produttore di un registro degli eventi pericolosi quando subappalta del lavoro ad un'impresa le cui dimensioni sono troppo piccole per avere un organismo responsabile della sicurezza per il progetto in questione;

j Fornitore di servizi – Fornitore di servizi: esempio simile a quello del punto (j) di cui sopra;

C.3.2. I fornitori di servizi si occupano di tutte le attività subappaltate dal gestore dell'infrastruttura, dall'impresa ferroviaria o dal produttore, quali ad esempio la manutenzione, l'emissione di biglietti, i servizi ingegneristici ecc.

C.3.3. Al fine di illustrare la gestione dei punti d'interazione e l'individuazione degli eventi pericolosi connessa, si illustra il seguente esempio. Si prende in considerazione un punto d'interazione fra un produttore di treni e un proponente (Impresa Ferroviaria). Si descrive poi come si potrebbero soddisfare i principali criteri richiesti al punto [G 3] della sezione 1.2.1:

a Direzione: il proponente (Impresa Ferroviaria);

b Input:

(1) elenco/elenchi di relativi pericoli di progetti simili;
(2) descrizione di tutti gli input ed output (I/O) per il punto d'interazione, comprese le caratteristiche delle prestazioni;

c Metodi: consultare l'appendice A.2 della guida EN 50 126-2 {Ref. 9};

d Partecipanti necessari:

(1) responsabile della garanzia della sicurezza del proponente (Impresa Ferroviaria);
(1) responsabile della garanzia della sicurezza del produttore di treni;
(2) autorità di progetto del proponente;
(3) autorità di progetto del produttore di treni;
(4) personale di manutenzione del proponente (che dipende parzialmente dall'analisi I/O);
(5) macchinisti (che dipende parzialmente dall'analisi I/O).

e Output:

(1) relazione condivisa ed approvata d'individuazione degli eventi pericolosi;
(2) misure di sicurezza per il registro degli eventi pericolosi con una chiara descrizione della responsabilità.

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. Esempi di metodi per determinare rischi ampiamente accettabili

C.4.1. Introduzione

C.4.1.1. I rischi ampiamente accettabili sono definiti nel regolamento sul metodo comune di sicurezza come rischi *"cosí esigui che non è ragionevole mettere in atto ulteriori misure di sicurezza (ridurre il rischio ulteriormente)"*. Nell'individuazione degli eventi pericolosi, classificare alcuni eventi pericolosi come connessi a rischi ampiamente accettabili consente di non analizzare ulteriormente tali eventi pericolosi nel procedimento di valutazione del rischio. La definizione di rischio ampiamente accettabili di cui sopra lascia un certo margine d'interpretazione. Ecco perché il regolamento indica che la decisione di classificare determinati eventi pericolosi con rischi ampiamente accettabili spetta a un parere esperto.

C.4.1.2. È infatti difficile definire comunemente, per rischi ampiamente accettabili, un criterio più esplicito che si applichi a tutti i vari livelli di sistema possibili in cui si potrebbero identificare tali eventi pericolosi, e che giustifichi i diversi fattori di avversione al rischio che possono prevalere per diverse applicazioni. Tuttavia, poiché è importante garantire che i pareri esperti siano facilmente compresi e rintracciabili, sono utili degli orientamenti su come definire i rischi come ampiamente accettabili. I criteri per definire rischi ampiamente accettabili possono essere quantitativi, qualitativi o semi-qualitativi. In basso vi sono alcuni esempi su come ricavare dei criteri che consentano la valutazione di rischi ampiamente accettabili in modo quantitativo o semi-quantitativo.

C.4.1.3. Gli esempi in basso illustrano questo principio. Sono stati estratti dal documento: *"Die Gefaehrdungseinstufung im ERA-Risikomanagementprozess", Kurz, Milius, Signal +Draht (100) 9/2008.*

C.4.2. Deduzione di criteri quantitativi

C.4.2.1. Si potrebbero definire i rischi ampiamente accettabili come quei rischi che sono molto più esigui dei rischi accettabili per una determinata categoria di eventi pericolosi. Usando dati statistici si potrebbe calcolare qual è il livello di rischio attuale per i sistemi ferroviari, e quindi dichiarare accettabile tale livello calcolato. Dividendo questo livello di rischio per il numero (N) di eventi pericolosi (per esempio si può supporre arbitrariamente che vi siano circa N = 100 categorie principali di eventi pericolosi nel sistema ferroviario), si ottiene un livello di rischio accettabile per categoria di evento pericoloso. Si potrebbe quindi affermare che un evento pericoloso con un rischio che è due ordini di grandezza inferiore rispetto al livello di rischio accettabile per evento pericoloso (parametro x% al punto [G 1] della sezione 2.2.3) sarebbe considerato come un rischio ampiamente accettabile.

C.4.2.2. Occorre comunque verificare che il contributo di tutti gli eventi pericolosi legati a rischi ampiamente accettabili non superari una determinata proporzione (p.es. y%) del rischio complessivo a livello di sistema: consultare la sezione 2.2.3 e la spiegazione al punto [G 2] della sezione 2.2.3.

C.4.3. Valutazione di rischi ampiamente accettabili

C.4.3.1. I valori limite per rischi ampiamente accettabili, ricavati negli esempi di cui sopra, possono essere usati per calibrare strumenti qualitativi, come ad esempio matrici di rischio, grafici di rischi o RPN, per aiutare l'esperto a prendere la decisione di classificare un rischio come ampiamente accettabile. È importante sottolineare che avere valori quantitativi come criteri

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

per rischi ampiamente accettabili, non significa che è necessario fare una stima o un'analisi precisa del rischio per decidere sull'accettabilità, ampia o meno, del rischio. È qui che entra in gioco il parere dell'esperto per fare questa stima approssimativa nella fase d'individuazione degli eventi pericolosi

C.4.3.2. È importante anche verificare che il contributo di tutti gli eventi pericolosi legati a rischi ampiamente accettabili non superi una determinata proporzione (p.es. y%) del rischio complessivo a livello di sistema: consultare la sezione 2.2.3 e la spiegazione al punto [G 2] della sezione 2.2.3.

C.5. Esempio di valutazione del rischio di una modifica organizzativa significativa

C.5.1. **Nota:** questo esempio di valutazione del rischio non è stato elaborato come conseguenza dell'applicazione del procedimento del metodo comune di sicurezza perché è precedente all'esistenza di quest'ultimo. Lo scopo dell'esempio è:

a identificare le somiglianze fra i metodi di valutazione del rischio esistenti e il procedimento del metodo comune di sicurezza;
b dare tracciabilità fra il procedimento esistente e quello richiesto dal metodo comune di sicurezza;
c fornire una giustificazione del valore aggiunto rappresentato dall'esecuzione delle fasi aggiuntive (se ve ne sono) richieste dal metodo comune di sicurezza.

Occorre sottolineare che questo esempio viene illustrato a titolo puramente informativo. Il suo scopo è quello di aiutare il lettore a comprendere il procedimento del metodo comune di sicurezza. Ma l'esempio in sé non deve essere applicato su un'altra modifica significativa né utilizzato come sistema di riferimento per quest'ultima. La valutazione del rischio deve essere effettuata per ogni modifica significativa, conformemente al regolamento sul metodo comune di sicurezza.

C.5.2. L'esempio riguarda una modifica alla struttura organizzativa. La modifica è stata considerata significativa dal relativo proponente. Per valutare la modifica è stato adottato un approccio basato sulla valutazione del rischio.

C.5.3. È stato necessario mettere in competizione con altre imprese dello stesso settore una divisione dell'impresa del gestore dell'infrastruttura che stava realizzando alcune attività di manutenzione (diverse dal segnalamento e dalla telematica). L'impatto diretto è stata la necessità di ridurre e ridistribuire il personale e i compiti all'interno della divisione distaccata dell'impresa del gestore dell'infrastruttura messa in competizione.

C.5.4. Questioni per il gestore dell'infrastruttura interessato:

a il personale dell'IM interessato dalla modifica era responsabile della manutenzione e delle riparazioni d'emergenza dovute a guasti improvvisi sull'infrastruttura. Il personale svolgeva anche alcune attività di manutenzione pianificate o previste dal progetto, come ad esempio rincalzo del binario, pulizia del pietrisco, controllo della vegetazione;
b questi compiti erano considerati fondamentali per la sicurezza e la puntualità del funzionamento. È stato quindi necessario analizzarli per trovare le giuste misure che garantissero che la situazione non peggiorasse, dal momento che molte persone responsabili delle questioni di sicurezza stavano lasciando l'impresa del Gestore dell'Infrastruttura.

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 lo stesso livello di sicurezza e puntualità dei treni deve essere mantenuto durante e dopo la modifica organizzativa.

C.5.5. Rispetto al procedimento del metodo comune di sicurezza, sono stati applicati i seguenti passi (cfr. anche la Figura 1):

a descrizione del sistema [sezione 2.1.2]:

(1) Descrizione dei compiti realizzati dall'impresa esistente (cioè dall'impresa del Gestore dell'Infrastruttura prima della modifica);
(2) descrizione delle modifiche pianificate all'interno dell'impresa del Gestore dell'Infrastruttura.
(3) è stato possibile descrivere, solo brevemente, i punti d'interazione della "divisione da distaccare" con altre imprese circostanti o con l'ambiente fisico. Non è stato possibile presentare chiaramente i limiti al 100 %;

b individuazione degli eventi pericolosi [sezione 2.2]:

(1) brainstorming di un gruppo di esperti:

(i) per trovare tutti gli eventi pericolosi con un'influenza rilevante sul rischio determinato dalla modifica aziendale desiderata;
(ii) per identificare possibili azioni volte a controllare il rischio;

(2) classificazione degli eventi pericolosi:

(i) in base alla gravità del rischio connesso: rischio alto, medio e basso;
(ii) in base all'impatto della modifica: rischio aumentato, inalterato, diminuito;

c uso di un sistema di riferimento [sezione 2.4]:

Il livello di sicurezza del sistema prima della modifica era considerato accettabile. È stato quindi usato come "sistema di riferimento" per ricavare i criteri di accettazione del rischio (RAC) per la modifica dell'azienda;

d stima e valutazione del rischio esplicite [sezione 2.5]:

Per ogni evento pericoloso con un rischio maggiore dovuto alla modifica della struttura organizzativa vengono identificate misure di riduzione del rischio. Il rischio residuo viene confrontato con il RAC del sistema di riferimento per verificare se occorre identificare ulteriori misure;

e dimostrazione della conformità del sistema ai requisiti di sicurezza [sezione 3]:

(1) l'analisi del rischio e il registro degli eventi pericolosi dimostrano che gli eventi pericolosi non possono essere controllati fino a che non vengono verificati e fino a che non si dimostra che sono stati applicati i requisiti di sicurezza (cioè le misure di sicurezza selezionate);
(2) l'analisi del rischio e il registro degli eventi pericolosi erano documenti dinamici. L'efficacia delle azioni decise è stata controllata con regolarità al fine di verificare se le condizioni fossero cambiate e se occorresse aggiornare l'analisi e la valutazione del rischio;
(3) se le misure messe in atto non erano abbastanza efficienti, l'analisi del rischio, la valutazione del rischio e il registro degli eventi pericolosi venivano aggiornati e controllati nuovamente;

f gestione degli eventi pericolosi [sezione 4.1]:

Gli eventi pericolosi identificati e le misure di sicurezza sono state registrate e gestite in un registro degli eventi pericolosi. Una delle conclusioni dell'esempio è stata di aggiornare costantemente l'analisi del rischio e il registro degli eventi pericolosi a mano

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 mano che si prendevano decisioni e azioni durante la modifica dell'organizzazione. Anche i rischi nei punti d'interazione con subappaltatori e imprenditori, per esempio, erano coperti dall'analisi del rischio.

La struttura e i campi utilizzati per il registro degli eventi pericolosi, nonché un estratto di alcune linee, sono riportati nella sezione C.16.2. dell'appendice C.

g valutazione indipendente [Articolo 6]:

È stata anche effettuata una valutazione indipendente da un terzo:

(1) per verificare che la gestione e la valutazione del rischio venissero effettuate correttamente;
(2) per verificare che la modifica aziendale fosse idonea e consentisse di mantenere lo stesso livello di sicurezza precedente alla modifica stessa.

C.5.6. L'esempio dimostra che i principi richiesti dal metodo di sicurezza comune sono metodi esistenti nel settore ferroviario e già applicati per valutare i rischi di modifiche aziendali. La valutazione del rischio nell'esempio soddisfa tutti i requisiti del metodo comune di sicurezza. Essa utilizza due dei tre principi di accettazione del rischio consentiti dall'approccio armonizzato del metodo comune di sicurezza:

a si applica un "sistema di riferimento" per determinare i criteri di accettazione del rischio necessari per valutare l'accettazione del rischio della modifica aziendale;
b "stima e valutazione del rischio esplicite":

(1) per analizzare le deviazioni della modifica dal sistema di riferimento;
(2) per identificare misure di riduzione del rischio per l'aumento del rischio dovuto alla modifica;
(3) per valutare se si ottiene un livello di rischio accettabile.

C.6. Esempio di valutazione del rischio di una modifica operativa significativa – Modifica delle ore di guida

C.6.1. **Nota:** questo esempio di valutazione del rischio non è stato elaborato come conseguenza dell'applicazione del procedimento del metodo comune di sicurezza perché è precedente all'esistenza di quest'ultimo. Lo scopo dell'esempio è:

a identificare le somiglianze fra i metodi di valutazione del rischio esistenti e il procedimento del metodo comune di sicurezza;
b dare tracciabilità fra il procedimento esistente e quello richiesto dal metodo comune di sicurezza;
c fornire una giustificazione del valore aggiunto rappresentato dall'esecuzione delle fasi aggiuntive (se ve ne sono) richieste dal metodo comune di sicurezza.

Occorre sottolineare che questo esempio viene illustrato a titolo puramente informativo. Il suo scopo è quello di aiutare il lettore a comprendere il procedimento del metodo comune di sicurezza. L'esempio in sé non deve essere però applicato su un'altra modifica significativa né utilizzato come sistema di riferimento per quest'ultima. La valutazione del rischio deve essere effettuata per ogni modifica significativa, conformemente al regolamento sul metodo comune di sicurezza.

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.6.2. L'esempio è una modifica operativa in cui l'impresa ferroviaria voleva assegnare nuovi itinerari e potenzialmente nuove ore di lavoro (compresi rotazione e schemi di turnazione) ai macchinisti.

C.6.3. Rispetto al procedimento del metodo comune di sicurezza, sono stati applicati i seguenti passi (cfr. anche la Figura 1):

a importanza della modifica [Articolo 4]:

L'impresa ferroviaria ha realizzato una valutazione del rischio preliminare dalla quale è emerso che la modifica operativa era significativa. Poiché i macchinisti dovevano percorrere nuovi itinerari, e probabilmente al di fuori delle loro ore di lavoro consuete, non si poteva ignorare la potenzialità di situazioni quali ad esempio superare i segnali disposti a via impedita, guidare in eccesso di velocità o ignorare i rallentamenti.

Quando è stata confrontata questa valutazione del rischio preliminare con i criteri dell'Articolo 4 (2) del regolamento sul metodo comune di sicurezza, è stato possibile catalogare la modifica come significativa in base ai seguenti criteri:

(1) importanza per la sicurezza: la modifica riguarda la sicurezza in quanto l'impatto della modifica del modo di lavorare dei macchinisti potrebbe essere catastrofico;
(2) conseguenze di guasti: gli errori dei macchinisti di cui sopra hanno la potenzialità di provocare conseguenze catastrofiche;
(3) novità: potenzialmente, l'impresa ferroviaria potrebbe introdurre nuove modalità di lavoro per i macchinisti;
(4) complessità della modifica: modificare le ore di guida potrebbe essere complesso in quanto potrebbe richiedere una valutazione e una modifica completa delle condizioni di lavoro esistenti;

b definizione del sistema [sezione 2.1.2]:

Inizialmente la definizione del sistema descriveva:

(1) condizioni di lavoro esistenti: orari di lavoro, schemi di turnazione ecc.;
(2) le modifiche delle ore lavorative;
(3) le questioni relative ai punti d'interazione (p.es. con il gestore dell'infrastruttura)

Durante le diverse iterazioni, la definizione del sistema è stata aggiornata con i requisiti di sicurezza derivanti dal procedimento di valutazione del rischio. Rappresentanti chiave del personale sono stati coinvolti in questo procedimento iterativo per l'individuazione di eventi pericolosi e l'aggiornamento della definizione del sistema.

c individuazione degli eventi pericolosi [sezione 2.2]:

Per i nuovi itinerari e le nuove turnazioni sono stati identificati gli eventi pericolosi e le possibili misure di sicurezza mediante il brainstorming di un gruppo di esperti, ivi compresi i rappresentati dei macchinisti. Sono stati esaminati i compiti dei macchinisti per le nuove condizioni al fine di valutare se queste ultime stessero incidendo sui macchinisti, per valutare il loro carico di lavoro, l'ambito geografico e l'orario dello schema di turnazione.
L'impresa ferroviaria ha anche consultato i sindacati dei lavoratori per vedere se questi ultimi potessero fornire informazioni supplementari e ha rivisto i livelli del rischio di affaticamento e di malattia che potevano essere indotti da un probabile aumento dello straordinario dovuto a viaggi prolungati su tragitti non noti.

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

Ad ogni evento pericoloso è stato assegnato un livello di gravità di rischio e di conseguenze (alto, medio, basso) ed è stato rivisto l'impatto della modifica proposta rispetto a questi valori (rischio aumentato, inalterato, ridotto).

d uso di codici di buona pratica [sezione2.3]:

Sono stati utilizzati codici di buona pratica relativi alle ore di lavoro e ai rischi di affaticamento umano per rivedere le condizioni di lavoro esistenti e per determinare i nuovi requisiti di sicurezza. Sono state scritte le necessarie norme operative in base ai codici di buona pratica per il nuovo sistema di turnazione. Tutte le parti necessarie sono state coinvolte nelle procedure operative riviste e nella decisione condivisa di portare avanti la modifica.

e dimostrazione della conformità del sistema ai requisiti di sicurezza [sezione 3]:

Le procedure operative riviste sono state introdotte nel sistema di gestione di sicurezza dell'impresa ferroviaria. Sono state controllate ed è stato messo in atto un processo di revisione per garantire che gli eventi pericolosi continuassero ad essere controllati correttamente durante il funzionamento del sistema ferroviario.

f gestione degli eventi pericolosi [sezione 4.1]:

Cfr. il punto cui sopra in quanto per le imprese ferroviarie il procedimento di gestione degli eventi pericolosi può fare parte del loro sistema di gestione della sicurezza per registrare e gestire i rischi. Gli eventi pericolosi identificati sono stati annotati in un registro degli eventi pericolosi con i requisiti di sicurezza (cioè facendo riferimento alle procedure operative riviste) che controllano il rischio connesso.
Le procedure revisionate sono state controllate, e all'occorrenza riviste, per garantire che gli eventi pericolosi identificati continuassero ad essere controllati correttamente durante il funzionamento del sistema ferroviario.

g valutazione indipendente [Articolo 6]:

Il procedimento di valutazione e gestione del rischio è stato valutato da una persona competente all'interno dell'impresa ferroviaria e indipendente dal procedimento di valutazione. La persona competente ha valutato sia il procedimento sia i risultati, cioè i requisiti di sicurezza identificati.

L'impresa ferroviaria ha basato la sua decisione di attuare il nuovo sistema sulla relazione di valutazione indipendente prodotta dalla persona competente.

C.6.4. L'esempio dimostra che i principi e il procedimento utilizzati dall'impresa ferroviaria sono il linea con il metodo di sicurezza comune. Il procedimento di gestione e valutazione del rischio ha soddisfatto tutti i requisiti del metodo comune di sicurezza.

C.7. Esempio di valutazione del rischio di una modifica tecnica significativa (CCS)

C.7.1. **Nota:** questo esempio di valutazione del rischio non è stato elaborato come conseguenza dell'applicazione del procedimento del metodo comune di sicurezza perché è precedente all'esistenza di quest'ultimo. Lo scopo dell'esempio è:

a identificare le somiglianze fra i metodi di valutazione del rischio esistenti e il procedimento del metodo comune di sicurezza;

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

b dare tracciabilità fra il procedimento esistente e quello richiesto dal metodo comune di sicurezza;
c fornire una giustificazione del valore aggiunto rappresentato dall'esecuzione delle fasi aggiuntive (se ve ne sono) richieste dal metodo comune di sicurezza.

Occorre sottolineare che questo esempio viene illustrato a titolo puramente informativo. Il suo scopo è quello di aiutare il lettore a comprendere il procedimento del metodo comune di sicurezza. L'esempio in sé non deve essere però applicato su un'altra modifica significativa né utilizzato come sistema di riferimento per quest'ultima. La valutazione del rischio deve essere effettuata per ogni modifica significativa, conformemente al regolamento sul metodo comune di sicurezza.

C.7.2. L'esempio riguarda una modifica tecnica al sistema di controllo-comando. La modifica è stata considerata significativa dal relativo produttore. Per valutare la modifica è stato adottato un approccio basato sulla valutazione del rischio.

C.7.3. Descrizione della modifica: la modifica consiste nel sostituire un loop a terra situato prima di un segnale con un sottosistema "radio infill + GSM " (cfr. Figura 16).

C.7.4. Questione: mantenere lo stesso livello di sicurezza del sistema dopo la modifica.

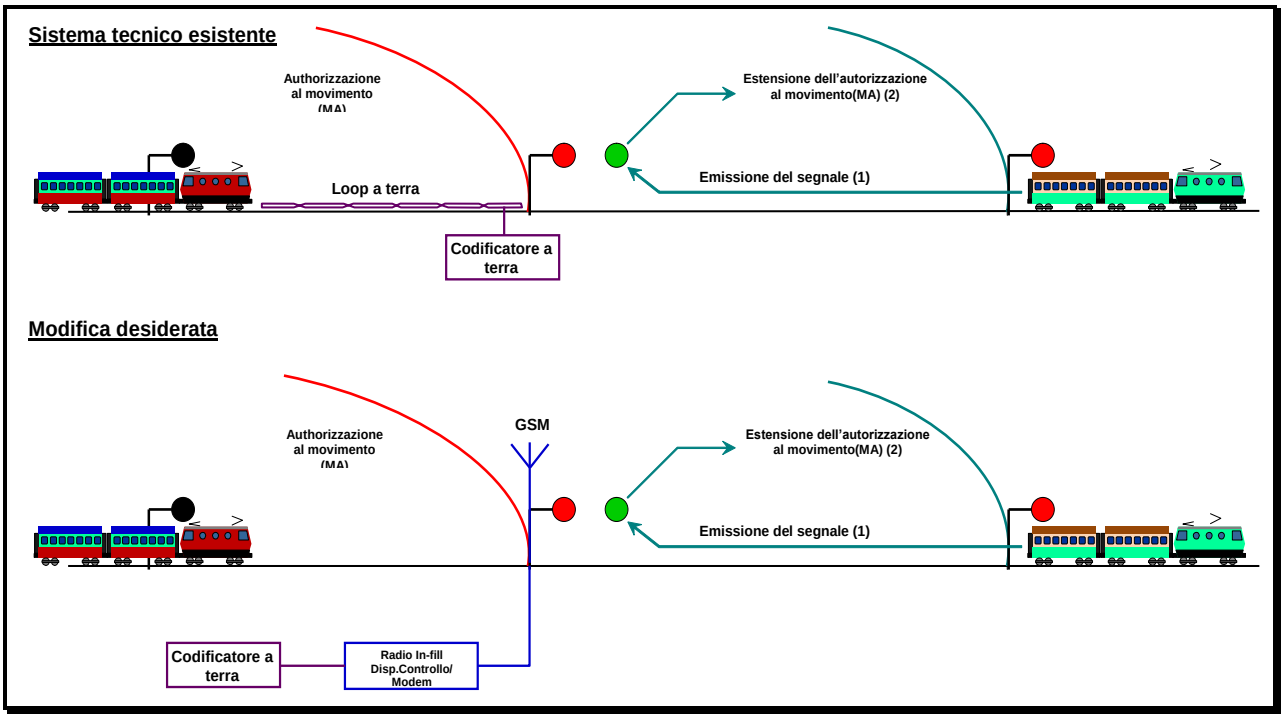

Figura 16 : Modifica di un loop a terra mediante un sottosistema radio infill.

C.7.5. Rispetto al procedimento del metodo comune di sicurezza, sono stati applicati i seguenti passi (cfr. anche la Figura 1):

a valutazione dell'importanza della modifica [Articolo 4]

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 criteri dell'Articolo 4 (2) sono utilizzati per valutare l'importanza di una modifica. Per decidere che la modifica è significativa sono state utilizzate principalmente la complessità e la novità.

b descrizione del sistema [sezione 2.1.2]:

(1) descrizione del sistema esistente: loop e sue funzioni nel sistema di controllo-comando;
(2) descrizione della modifica pianificata dal proponente e dal produttore;
(3) descrizione dei punti d'interazione funzionali e fisici del loop con il resto del sistema;

La funzione del "loop+codificatore" nel sistema esistente è quella di emettere il segnale all'avvicinarsi di un treno quando il tratto dietro al segnale (cioè di fronte al treno in avvicinamento) si libera: cfr. Figura 16.

c individuazione degli eventi pericolosi [sezione 2.2]:

Si applica il procedimento di valutazione iterativa del rischio e l'individuazione degli eventi pericolosi (cfr. sezione 2.1.1) sulla base di un brainstorming effettuato da un gruppo di esperti al fine di:

(1) identificare gli eventi pericolosi con un'influenza rilevante sul rischio determinato dalla modifica desiderata;
(2) identificare possibili azioni volte a controllare il rischio;

Poiché il loop, e quindi il radio infill, emette il segnale, c'è il rischio di dare un'autorizzazione al movimento non sicura al treno in avvicinamento, mentre il treno precedente occupa ancora il tratto di fronte al segnale. Il rischio deve essere controllato ad un livello accettabile.

d uso di un sistema di riferimento [sezione 2.4]:

Il livello di sicurezza del sistema prima della modifica (loop) è considerato accettabile. Esso viene quindi usato come "sistema di riferimento" per ricavare i requisiti di sicurezza per il sottosistema radio infill.

e stima e valutazione del rischio esplicite [sezione2.5]:

(1) la stima e la valutazione esplicite del rischio analizzano le differenze fra i sottosistemi "loop" e "radio infill+GSM". Per il sottosistema "radio infill + GSM" vengono identificati i seguenti nuovi eventi pericolosi:

(i) trasmissione da parte di pirati informatici di informazioni non sicure nel air gap dal momento che il "radio infill+GSM" è un sottosistema di trasmissione aperto;
(ii) ritardo nella trasmissione o trasmissione di pacchetti di dati memorizzati nel air gap;

(2) stima del rischio esplicita ed uso del RAC-TS per la parte del dispositivo di controllo del radio infill;

f uso di codici di buona pratica [sezione 2.3]:

(1) la norma EN 50159-2 (*"Applicazioni ferroviarie: Parte 2: Comunicazioni in sicurezza in sistemi di trasmissione aperti"*) fornisce i requisiti di sicurezza per controllare i nuovi eventi pericolosi ad un livello accettabile, p.es.:

(i) cifratura e protezione dei dati;
(ii) ordinamento dei messaggi e marca temporale;

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) uso, per esempio, della norma EN 50 128 per lo sviluppo del software del dispositivo di controllo del Radio infill;

g dimostrazione della conformità del sistema ai requisiti di sicurezza [sezione 3]:

(1) sorveglianza dell'attuazione dei requisiti di sicurezza attraverso il procedimento di sviluppo del sottosistema "radio infill + GSM";
(2) verifica che il sistema, così com'è progettato e installato, è conforme ai requisiti di sicurezza;

h gestione degli eventi pericolosi [sezione 4.1]:

Gli eventi pericolosi identificati, le misure di sicurezza e i conseguenti requisiti di sicurezza emersi dalla valutazione del rischio e l'applicazione dei tre principi di accettazione del rischio, sono annotati e gestiti in un registro degli eventi pericolosi.

i valutazione indipendente [Articolo 6]:

Viene effettuata anche una valutazione indipendente da un terzo al fine di:

(1) verificare che la gestione e la valutazione del rischio vengano realizzate correttamente;
(2) verificare che la modifica tecnica sia idonea e mantenga lo stesso livello di sicurezza precedente alla modifica stessa.

C.7.6. L'esempio mostra che i tre principi di accettazione del rischio richiesti dal metodo comune di sicurezza vengono utilizzati in modo complementare per definire i requisiti di sicurezza per il sistema sottoposto a valutazione. La valutazione del rischio nell'esempio soddisfa tutti i requisiti del metodo comune di sicurezza sintetizzati nella Figura 1, compresi la gestione del registro degli eventi pericolosi e la valutazione indipendente della sicurezza eseguita da un terzo.

C.8. Esempio delle direttive svedesi BVH 585.30 per la valutazione del rischio di gallerie ferroviarie

C.8.1. **Nota:** questo esempio di valutazione del rischio non è stato elaborato come conseguenza dell'applicazione del procedimento del metodo comune di sicurezza perché è precedente all'esistenza di quest'ultimo. Lo scopo dell'esempio è:

a identificare le somiglianze fra i metodi di valutazione del rischio esistenti e il procedimento del metodo comune di sicurezza;
b dare tracciabilità fra il procedimento esistente e quello richiesto dal metodo comune di sicurezza;
c fornire una giustificazione del valore aggiunto rappresentato dall'esecuzione delle fasi aggiuntive (se ve ne sono) richieste dal metodo comune di sicurezza.

Occorre sottolineare che questo esempio viene illustrato a titolo puramente informativo. Il suo scopo è quello di aiutare il lettore a comprendere il procedimento del metodo comune di sicurezza. L'esempio in sé non deve essere però applicato su un'altra modifica significativa né utilizzato come sistema di riferimento per quest'ultima. La valutazione del rischio deve essere effettuata per ogni modifica significativa, conformemente al regolamento sul metodo comune di sicurezza.

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.8.2. Lo scopo dell'esempio è quello di confrontare il procedimento previsto dal metodo comune di sicurezza con le direttive BVH 585.30 utilizzate dal gestore dell'infrastruttura svedese Banverket per progettare e verificare il raggiungimento di un congruo livello di sicurezza nella pianificazione e nella costruzione di nuove gallerie ferroviarie. I punti comuni e le differenze con il metodo comune di sicurezza sono elencati di seguito; i requisiti per la valutazione del rischio figurano nelle direttive BVH 585.30.

C.8.3. Rispetto al procedimento del metodo comune di sicurezza della Figura 1:

a le direttive BVH 585.30 presentano i seguenti punti comuni:

(1) descrizione del sistema [sezione 2.1.2]:

Le direttive richiedono una descrizione del sistema dettagliata che contenga:

(i) una descrizione della galleria;
(ii) una descrizione del binario;
(iii) una descrizione del tipo di materiale rotabile (compreso il personale di bordo);
(iv) una descrizione del traffico e delle operazioni desiderate;
(v) una descrizione dell'assistenza esterna (compresi i servizi di soccorso);

(2) individuazione degli eventi pericolosi [sezione 2.2]:

Le direttive non richiedono esplicitamente l'individuazione degli eventi pericolosi. Richiedono l'individuazione del rischio e un "catalogo degli incidenti" contenente i tipi di potenziali incidenti identificati che si ritiene abbiano un impatto significativo sul livello di rischio della galleria e che devono essere contemplati nella valutazione successiva. Esempi di incidenti:

(i) "deragliamento di treno passeggeri";
(ii) "deragliamento di treno merci";
(iii) "incidente con merci pericolose";
(iv) "incendio nel veicolo";
(v) "collisione fra treno passeggeri e un oggetto leggero/pesante";
(vi) ecc.

(3) non vi sono disposizioni per l'applicazione di codici di buona pratica o sistemi di riferimento simili. Si ritiene che l'analisi del rischio debba essere effettuata in ogni caso;

(4) stima e valutazione del rischio esplicite [sezione 2.5]:

(i) in linea di massima, le direttive raccomandano di eseguire per ogni tipo di incidente un albero degli eventi, in base ad un'analisi quantitativa del rischio. Poiché, però, l'intenzione dell'analisi del rischio è quella di analizzare il livello di sicurezza complessivo della galleria piuttosto che analizzare la sicurezza di singoli aspetti in modo più dettagliato, si valutano le conseguenze di tutti gli scenari per ottenere il livello di rischio complessivo per la galleria;
(ii) l'accettabilità di questo livello di rischio complessivo per la galleria si deve confrontare con il seguente criterio esplicito quantitativo di accettazione del rischio: *"il traffico ferroviario per chilometro in galleria deve essere sicuro come il traffico ferroviario per chilometro su binari all'aperto, esclusi i passaggi a livello"*. Questo criterio viene trasformato in una curva F-N basata su dati storici di incidenti ferroviari in Svezia e viene elaborato per coprire anche conseguenze che non figurano nelle statistiche;
(iii) oltre a questo criterio per il livello di rischio complessivo della galleria, vi sono anche altri requisiti da soddisfare, specificamente per l'evacuazione in galleria e le possibilità per i servizi di soccorso:

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

- di verificare che l'autosoccorso sia possibile nel caso di incendio di un treno per un "caso verosimilmente peggiore" (sono indicati anche i criteri per questa valutazione);
- la galleria deve essere progettata per consentire le operazioni di soccorso per un determinato numero di scenari;

(5) risultati della valutazione del rischio [sezione 2.1.6]:

I risultati della valutazione del rischio sono:

(i) un elenco di misure di sicurezza secondo gli standard minimi basate sulle norme STI-SRT e sulle norme nazionali da usare per la progettazione della galleria, e;
(ii) tutte le misure di sicurezza supplementari identificate come necessarie dall'analisi del rischio, indicando il loro scopo. Si specifica che si devono scegliere le misure di sicurezza in base al seguente ordine prioritario:

- prevenire incidenti;
- ridurre conseguenze di incidenti;
- facilitare l'evacuazione;
- facilitare gli interventi di soccorso;

(6) gestione degli eventi pericolosi [sezione 4.1]:

Le direttive non richiedono esplicitamente di tenere un registro degli eventi pericolosi. Ciò è legato al fatto che il livello della valutazione è complessivo e quindi gli eventi pericolosi non sono valutati e controllati singolarmente. Si valuta l'accettabilità del rischio complessivo della galleria senza alcuna ripartizione del criterio di accettazione del rischio complessivo a diversi tipi di incidenti o eventi pericolosi indiretti.

Vi è comunque un elenco di tutte le misure di sicurezza, sia quelle derivanti dal "standard minimi" sia quelle identificate come necessarie dall'analisi del rischio: cfr. il punto (5)(ii) di cui sopra. Nell'elenco delle misure di sicurezza si deve indicare se queste riguardano l'infrastruttura della galleria, il binario, le operazioni o il materiale rotabile, ed anche quali sono gli effetti desiderati in base all'elenco numerato del punto (5)(ii). Ma le direttive non richiedono di dichiarare esplicitamente quali eventi pericolosi controllano le misure di sicurezza e chi è responsabile di ogni misura.

(7) valutazione indipendente [Articolo 6]:

È obbligatoria una valutazione indipendente effettuata da un terzo al fine di:

(i) verificare che il procedimento di valutazione del rischio raccomandato dalle direttive BVH 585.30 sia eseguito correttamente;
(ii) considerare accettabile l'analisi del rischio;
(iii) verificare che sia indicato chiaramente come si deve realizzare la futura gestione della sicurezza nel progetto;

Il documento finale dell'analisi del rischio viene firmato dal valutatore indipendente ed anche dal coordinatore della sicurezza all'interno del progetto.

b le direttive BVH 585.30 sono diverse nei seguenti aspetti:

(1) dimostrazione della conformità del sistema ai requisiti di sicurezza [sezione 3]:

Le direttive BVH 585.30 non richiedono né di descrivere come vengono messi in atto i requisiti di sicurezza identificati, né di verificare che il progetto finale della galleria soddisfi i requisiti di sicurezza specificati. Essi descrivono esclusivamente

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

come questi requisiti devono essere trasferiti per fare in modo che siano messi in atto nella fase di costruzione.

Le direttive prevedono che i requisiti di sicurezza siano utilizzati per verificare che l'analisi del rischio sia stata eseguita correttamente e in modo trasparente, e che possa essere accettata dal progetto.

C.8.4. In conclusione, il confronto con il metodo comune di sicurezza mostra che:

a le direttive BVH 585.30 soddisfano le relative parti del metodo comune di sicurezza sebbene il loro scopo ed ambito di applicazione non siano identici alle disposizioni del regolamento;
b le direttive BVH 585.30 valutano il livello di rischio complessivo della galleria ferroviaria;
c gli eventi pericolosi non sono controllati singolarmente e quindi si enfatizza meno la gestione degli eventi pericolosi;
d la dimostrazione di conformità e la verifica della corretta attuazione di tutte le misure di sicurezza non sono indicate esplicitamente. Gli orientamenti indicano tuttavia che il ruolo del coordinatore della sicurezza all'interno del progetto (un ruolo ed una competenza richiesta dalle direttive BVH 585.30) è quello di verificare che le conclusioni dell'analisi del rischio siano inserite nei documenti e nei disegni progettuali, ed anche di controllare che siano messe in atto correttamente nella fase di costruzione;

C.8.5. Le disposizioni del metodo comune di sicurezza sono più generali delle direttive BVH 585.30 nel senso che offrono l'applicazione di tre diversi principi di accettazione del rischio. Tuttavia, l'applicazione delle direttive BVH 585.30 all'interno del metodo comune di sicurezza non pone alcun problema in quanto è compatibile con l'uso del terzo principio di stima esplicita del rischio.

C.9. Esempio di valutazione del rischio a livello di sistema per la metropolitana di Copenaghen

C.9.1. **Nota:** questo esempio di valutazione del rischio non è stato elaborato come conseguenza dell'applicazione del procedimento del metodo comune di sicurezza perché è precedente all'esistenza di quest'ultimo. Lo scopo dell'esempio è:

a identificare le somiglianze fra i metodi di valutazione del rischio esistenti e il procedimento del metodo comune di sicurezza;
b dare tracciabilità fra il procedimento esistente e quello richiesto dal metodo comune di sicurezza;
c fornire una giustificazione del valore aggiunto rappresentato dall'esecuzione delle fasi aggiuntive (se ve ne sono) richieste dal metodo comune di sicurezza.

Occorre sottolineare che questo esempio viene illustrato a titolo puramente informativo. Il suo scopo è quello di aiutare il lettore a comprendere il procedimento del metodo comune di sicurezza. L'esempio in sé non deve essere però applicato su un'altra modifica significativa né utilizzato come sistema di riferimento per quest'ultima. La valutazione del rischio deve essere effettuata per ogni modifica significativa, conformemente al regolamento sul metodo comune di sicurezza.

C.9.2. L'esempio riguarda un sistema di metropolitana completo e complesso senza macchinista, compresi sottosistemi tecnici componenti (p.es. protezione automatica del treno (ATP) e materiale rotabile), nonché il funzionamento e la manutenzione del sistema. Per valutare il

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

sistema e i sottosistemi componenti è stato adottato un approccio basato sulla valutazione del rischio. Il progetto prevedeva anche la certificazione del sistema di gestione della sicurezza dell'impresa che doveva gestire il sistema. Ciò riguarda la capacità dell'impresa ferroviaria e del gestore dell'infrastruttura di gestire e mantenere in condizioni di sicurezza l'intero sistema per tutto il ciclo di vita dello stesso.

C.9.3. Rispetto al procedimento del metodo comune di sicurezza, sono stati applicati i seguenti passi (cfr. anche la Figura 1):

a descrizione del sistema [sezione 2.1.2]:

(1) descrizione dei requisiti prestazionali del sistema;
(2) descrizione delle norme operative;
(3) chiara descrizione dei punti d'interazione e delle responsabilità fra i diversi operatori, in particolare fra i sottosistemi tecnici;
(4) definizione di requisiti di sistema di alto livello (in termini di frequenza accettabile di incidenti e definizione di una zona ALARP);

b individuazione degli eventi pericolosi [sezione 2.2]:

(1) un'analisi preliminare degli eventi pericolosi a livello di sistema;
(2) analisi funzionale a livello di sistema evidenziando tutti i sottosistemi, e non soltanto quelli logicamente essenziali per la sicurezza (p.es. ATP e materiale rotabile), che partecipano a funzioni di sicurezza ed hanno un ruolo attivo nel garantire la sicurezza dei passeggeri e del personale;
(3) intenso coordinamento fra gli operatori (imprese appaltatrici, fornitori di sottosistemi dei sottosistemi tecnici e delle opere di ingegneria):

(i) per identificare sistematicamente tutti gli eventi pericolosi ragionevolmente prevedibili;
(ii) per identificare possibili azioni volte a controllare a un livello accettabile tutti i rischi connessi agli eventi pericolosi identificati;

c uso di codici di buona pratica [sezione 2.3]:

Sono stati utilizzati diversi codici di buona pratica, diverse norme e regolamenti, p.es:

(1) il regolamento BOStrab per la costruzione e la gestione di vetture stradali (regolamento tedesco applicabile a sistemi ferroviari urbani) e sul funzionamento senza macchinista;
(2) i documenti VDV (codici di buona pratica tedeschi) relativi a requisiti sulle apparecchiature, per garantire la sicurezza dei passeggeri nelle stazioni, per il funzionamento senza macchinista;
(3) norme CENELEC per sistemi ferroviari (EN 50 126, 50 128 e 50 129). Queste norme trattano in particolare sistemi tecnici ferroviari. Ma poiché contengono un approccio metodologico con una validità generale, sono state ampiamente adottate dalla metropolitana di Copenaghen:

(i) la norma EN 50 126 è stata utilizzata per le attività di gestione della sicurezza e di valutazione del rischio del sistema ferroviario completo;
(ii) la norma EN 50 129 è stata utilizzata per l'intero sistema di segnalamento;
(iii) la norma EN 50 128 è stata usata per lo sviluppo del software (comprese verifica e validazione) dei sottosistemi tecnici;

(4) norme di prevenzione contro gli incendi per gallerie (NEPA 130);
(5) norme per i lavori di genio civile e gli impianti civili (Eurocodici);

d uso di un sistema di riferimento [sezione 2.4]:

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 metropolitana doveva raggiungere il livello di sicurezza dei corrispondenti impianti moderni in Germania, Francia o Gran Bretagna. Questi sistemi esistenti sono stati usati come sistemi di riferimento simili per ricavare i criteri di accettazione del rischio in termini di frequenze di incidenti accettabili per la metropolitana di Copenaghen;

e stima e valutazione del rischio esplicite [sezione 2.5]:

(1) per la stima di rischi connessi a eventi pericolosi specifici;
(2) per il controllo della ventilazione d'emergenza delle gallerie (compresi i fattori umani che coinvolgono unità di vigili del fuoco);
(3) per identificare misure di riduzione del rischio;
(4) per valutare se si ottiene un livello di rischio accettabile per l'intero sistema;

f dimostrazione della conformità del sistema ai requisiti di sicurezza [sezione 3]:

(1) attività di gestione e tecniche conformi alla complessità del sistema per dimostrarne la sicurezza;
(2) ripartizione di requisiti di sicurezza del sistema a sottosistemi tecnici e impianti civili, nonché a tutte le funzioni della metropolitana che interessano la sicurezza;
(3) dimostrazione che ogni sottosistema soddisfa, costruito, i propri requisiti di sicurezza;
(4) per le funzioni di sicurezza svolte da più di un sottosistema, non è stato possibile concludere la dimostrazione di conformità ai requisiti di sicurezza a livello di sottosistema. È stata eseguita a livello di sistema integrando i diversi sottosistemi, strumenti e procedure;
(5) dimostrazione che tutto il sistema è conforme ai requisiti di sicurezza di alto livello;

g gestione degli eventi pericolosi [sezione 4.1]:

I pericoli identificati, le misure di sicurezza connesse e i conseguenti requisiti di sicurezza sono stati annotati e gestiti per mezzo di un registro degli eventi pericolosi centrale. Il responsabile della sicurezza del progetto complessivo gestiva questo registro degli eventi pericolosi, nel quale sono stati annotati i pericoli operativi sorti durante la progettazione e l'installazione, nonché gli eventi pericolosi connessi al funzionamento e alla manutenzione;

h prove della gestione e della valutazione del rischio [sezione 5]:

I risultati della valutazione del rischio sono stati documentati formalmente e corredati da un *safety case* conformemente ai requisiti delle norme CENELEC:

(1) *safety case* dell'intero sistema;
(2) *safety case* per ogni sottosistema tecnico (compresi i sottosistemi di segnalamento e gli impianti civili);
(3) *safety case* per impianti civili (stazioni, gallerie, viadotti, massicciate);
(4) *safety case* per l'installazione;
(5) *safety case* per i veicoli;
(6) *safety case* per gli operatori (a sostegno della certificazione del sistema di gestione della sicurezza dell'impresa ferroviaria e del gestore dell'infrastruttura, cioè dimostrazione della capacità del proponente di gestire e mantenere il sistema in condizioni di sicurezza);

i valutazione indipendente [Articolo 6]:

Il processo complessivo è stato sorvegliato e valutato da un valutatore indipendente della sicurezza insieme ad una delegazione dell'Organo di tutela tecnica (cioè il Ministero dei Trasporti danese). I ruoli del valutatore indipendente della sicurezza sono descritti in un opportuno codice di buona pratica. Fra questi rientrano:

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) la verifica della corretta gestione e valutazione del rischio;
(2) la verifica che il sistema è idoneo allo scopo previsto e che sarà gestito e manutenuto in condizioni di sicurezza per tutto il suo ciclo di vita;
(3) la raccomandazione di omologazione all'Organo di tutela tecnica.

C.9.4. Il progetto completo è stato sostenuto da un opportuno procedimento di gestione della qualità.

C.9.5. Nel progetto, le prove dei fornitori (cioè *safety case* e documentazione di supporto dettagliata per i sottosistemi tecnici e gli impianti civili) sono state fornite al responsabile della sicurezza del proponente. Queste prove sono state poi riviste dall'impresa di gestione della sicurezza, nonché dal valutatore indipendente della sicurezza le cui conclusioni sono state riportate in una relazione di valutazione.

La relazione della valutazione indipendente della sicurezza è stata rivista dal responsabile della sicurezza del proponente e sottoposta al proponente, il quale ha inoltrato tutta la documentazione all'Organo di tutela tecnica (cioè il Ministero dei Trasporti danese) per l'accettazione finale.

C.9.6. L'esempio dimostra che i principi richiesti dal metodo di sicurezza comune sono metodi esistenti nel settore ferroviario. La valutazione del rischio nell'esempio soddisfa tutti i requisiti del metodo comune di sicurezza. In particolare, essa utilizza tutti e tre i principi di accettazione del rischio consentiti dall'approccio armonizzato del metodo comune di sicurezza.

C.10. Esempio di orientamenti dell'OTIF per il calcolo del rischio dovuto al trasporto ferroviario di merci pericolose

C.10.1. **Nota:** questo esempio di valutazione del rischio non è stato elaborato come conseguenza dell'applicazione del procedimento del metodo comune di sicurezza perché è precedente all'esistenza di quest'ultimo. Lo scopo dell'esempio è:

a identificare le somiglianze fra i metodi di valutazione del rischio esistenti e il procedimento del metodo comune di sicurezza;
b dare tracciabilità fra il procedimento esistente e quello richiesto dal metodo comune di sicurezza;
c fornire una giustificazione del valore aggiunto rappresentato dall'esecuzione delle fasi aggiuntive (se ve ne sono) richieste dal metodo comune di sicurezza.

Occorre sottolineare che questo esempio viene illustrato a titolo puramente informativo. Il suo scopo è quello di aiutare il lettore a comprendere il procedimento del metodo comune di sicurezza. L'esempio in sé non deve essere però applicato su un'altra modifica significativa né utilizzato come sistema di riferimento per quest'ultima. La valutazione del rischio deve essere effettuata per ogni modifica significativa, conformemente al regolamento sul metodo comune di sicurezza.

C.10.2. La filosofia complessiva degli orientamenti dell'OTIF è in linea con lo scopo del metodo comune di sicurezza, ma gli orientamenti hanno un ambito di applicazione limitato. L'obiettivo degli orientamenti dell'OTIF *"è quello di ottenere un approccio più uniforme per la valutazione del rischio del trasporto di merci pericolose negli Stati membri della COTIF e, di conseguenza, di rendere comparabili le singole valutazioni del rischio"*. Essi, pertanto,

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

sostengono il riconoscimento transnazionale, fra gli stati membri della COTIF, delle valutazioni del rischio del trasporto di merci pericolose per ferrovia.

C.10.3. Rispetto al metodo comune di sicurezza e al diagramma di flusso della Figura 1:

a gli orientamenti OTIF presentano i seguenti punti comuni:

(1) si tratta di un approccio comune per la valutazione del rischio basato, tuttavia, soltanto su una stima esplicita del rischio (cioè il terzo principio di accettazione del rischio del metodo comune di sicurezza);
(2) la valutazione del rischio dell'OTIF è composta da:

(i) una fase di analisi del rischio che comprende:

- una fase di individuazione degli eventi pericolosi;
- una fase di stima del rischio;

(ii) una fase di valutazione del rischio basata su criteri (di accettazione) del rischio non ancora armonizzati. In realtà, numerose specificità nazionali possono influenzare tali criteri;

b gli orientamenti OTIF sono diversi nei seguenti aspetti:

(1) l'ambito di applicazione è diverso. Mentre il metodo comune di sicurezza deve essere applicato soltanto per modifiche significative al sistema ferroviario, gli orientamenti OTIF devono essere applicati per valutare i rischi nel trasporto di merci pericolose per ferrovia, indipendentemente dal fatto che ciò costituisca o meno una modifica significativa al sistema ferroviario;
(2) non c'è la possibilità di scegliere fra tre principi di accettazione del rischio per controllare i rischi. Il terzo principio, cioè la stima esplicita del rischio, è l'unico principio ammesso. Inoltre, essa si deve basare esclusivamente su una stima quantitativa più che qualitativa. L'analisi qualitativa del rischio può essere adatta soltanto a confrontare opzioni di misure (di sicurezza) per la riduzione del rischio;
(3) è richiesta l'applicazione del principio ALARP al fine di determinare se misure supplementari potrebbero ridurre ulteriormente il rischio valutato a un prezzo ragionevole;
(4) non vi è alcun concetto di "eventi pericolosi connessi a rischi ampiamente accettabili" che consenta di concentrare la valutazione del rischio sugli eventi pericolosi con un'influenza maggiore. Ciononostante, si raccomanda di ridurre il numero di potenziali scenari di incidenti ad un numero ragionevole di scenari di base (cfr. la sezione 3.2 in {Ref. 10});
(5) il procedimento si concentra sulla valutazione del rischio ma non comprende:

(i) il procedimento per la selezione e l'attuazione di misure (di sicurezza) per modificare il rischio;
(ii) il procedimento per l'accettazione del rischio;
(iii) il procedimento per dimostrare la conformità del sistema ai requisiti di sicurezza;
(iv) il procedimento per comunicare il rischio ad altri operatori interessati (cfr. il punto qui di seguito);

(6) non danno direttive sulla prova da fornire mediante il procedimento di valutazione del rischio;
(7) non si richiede la gestione degli eventi pericolosi;
(8) non si richiede una valutazione indipendente da parte di un terzo della corretta applicazione del metodo comune.

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.10.4. Il confronto fra gli orientamenti OTIF e il metodo comune di sicurezza dimostra che entrambi sono compatibili sebbene il loro scopo ed ambito di applicazione non siano identici. Il metodo comune di sicurezza è più generale degli orientamenti OTIF, nel senso che è più flessibile. D'altra parte, il metodo comune di sicurezza prevede anche più attività di gestione del rischio:

a esso consente di utilizzare tre principi di accettazione del rischio basati su prassi esistenti nelle ferrovie: cfr. la sezione 2.1.4.
b la sua applicazione è richiesta soltanto per modifiche significative, e un'ulteriore analisi del rischio è richiesta soltanto per gli eventi pericolosi non connessi con un rischio ampiamente accettabile;
c comprende la scelta e la messa in atto delle misure di sicurezza che si suppone controllino gli eventi pericolosi identificati e i rischi connessi;
d armonizza il procedimento di gestione del rischio, ivi compresi:

(1) l'armonizzazione dei criteri di accettazione del rischio di cui si occupa l'Agenzia nel lavoro che sta realizzando sui rischi ampiamente accettabili e sui criteri di accettazione del rischio,
(2) la dimostrazione della conformità del sistema ai requisiti di sicurezza;
(3) i risultati e le prove del procedimento di valutazione del rischio;
(4) lo scambio di informazioni relative alla sicurezza fra gli operatori coinvolti nei punti d'interazione;
(5) la gestione, in un registro degli eventi pericolosi, di tutti i pericoli identificati e delle misure di sicurezza connesse;
(6) la valutazione indipendente da parte di un terzo della corretta applicazione del metodo comune di sicurezza.

C.10.5. Ad ogni modo, l'applicazione degli orientamenti OTIF all'interno del metodo comune di sicurezza (nel caso in cui il trasporto di merci pericolose costituisca una modifica significativa per un gestore dell'infrastruttura o per un'impresa ferroviaria) non pone alcun problema, in quanto è compatibile con l'uso del terzo principio della stima esplicita del rischio.

C.11. Esempio di valutazione del rischio di un'applicazione per l'omologazione di un nuovo tipo di materiale rotabile

C.11.1. **Nota:** questo esempio di valutazione del rischio non è stato elaborato come conseguenza dell'applicazione del procedimento del metodo comune di sicurezza perché è precedente all'esistenza di quest'ultimo. Lo scopo dell'esempio è:

a identificare le somiglianze fra i metodi di valutazione del rischio esistenti e il procedimento del metodo comune di sicurezza;
b dare tracciabilità fra il procedimento esistente e quello richiesto dal metodo comune di sicurezza;
c fornire una giustificazione del valore aggiunto rappresentato dall'esecuzione delle fasi aggiuntive (se ve ne sono) richieste dal metodo comune di sicurezza.

Occorre sottolineare che questo esempio viene illustrato a titolo puramente informativo. Il suo scopo è quello di aiutare il lettore a comprendere il procedimento del metodo comune di sicurezza. L'esempio in sé non deve essere però applicato su un'altra modifica significativa né utilizzato come sistema di riferimento per quest'ultima. La valutazione del rischio deve essere effettuata per ogni modifica significativa, conformemente al regolamento sul metodo comune di sicurezza.

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.11.2. Questo esempio di valutazione riguarda un'applicazione per l'accettazione di un nuovo tipo di materiale rotabile. È stata realizzata un'analisi del rischio per valutare i rischi connessi all'introduzione di un nuovo vagone merci.

C.11.3. Lo scopo della modifica era quello di aumentare l'efficienza, la capacità, le prestazioni e l'affidabilità per il trasporto di merci alla rinfusa su una specifica linea merci. Poiché i vagoni erano destinati al traffico transfrontaliero, occorreva anche l'accettazione di due diverse NSA. Il proponente era l'operatore di trasporto merci che, a sua volta, è di proprietà della società che produce le merci da trasportare.

C.11.4. Lo sviluppo del progetto comprendeva la costruzione, la produzione, il montaggio, la messa in servizio e la verifica del nuovo materiale rotabile. È stata effettuata l'analisi del rischio per verificare che il nuovo progetto soddisfacesse i requisiti di sicurezza per ognuno dei sottosistemi nonché per il sistema completo.

C.11.5. Nell'analisi del rischio si è fatto riferimento alle procedure e definizioni CENELEC EN 50126 e la valutazione del rischio è stata effettuata in base a questa norma.

C.11.6. Rispetto al procedimento del metodo comune di sicurezza, sono stati applicati i seguenti passi:

a descrizione del sistema [sezione 2.1.2]:

Per ogni fase di progettazione vi erano requisiti sulla documentazione di verifica della sicurezza e sulla descrizione del progetto del sistema:

(1) fase concettuale: descrizione preliminare delle esigenze operative dell'operatore;

(2) fase di specifica: specifiche funzionali, norme tecniche applicabili, piano di test e verifica. Erano compresi anche i requisiti dell'operatore sull'uso e sulla manutenzione del vagone;

(3) fase di produzione: documentazione tecnica del produttore, compresi disegni, norme, calcoli, analisi ecc. Analisi approfondita del rischio per progetti nuovi o innovativi o per nuovi settori d'uso;

(4) fase di verifica:

(i) la verifica del produttore delle prestazioni tecniche del vagone (relazioni di test, calcoli, verifiche conformemente a norme e requisiti funzionali);
(ii) documentazione di misure di riduzione del rischio e rapporti di prova per dimostrare la conformità dei vagoni all'infrastruttura ferroviaria;
(iii) documenti di manutenzione e formazione, manuali d'uso ecc.

(5) fase di accettazione:

(i) la dichiarazione di sicurezza del produttore e le prove di sicurezza (*safety case*);
(ii) l'accettazione da parte dell'operatore sia del vagone sia della relativa documentazione;

b individuazione degli eventi pericolosi [sezione 2.2]:

eseguita costantemente in tutte le fasi di progettazione. È stato usato prima un approccio "bottom-up", nei casi in cui i diversi produttori hanno valutato le sequenze di rischio derivanti dal guasto di componenti all'interno del loro sottosistema. La divisione in sottosistemi era la seguente:

(1) telaio;

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) sistema frenante;
(3) accoppiamento centrale**;**
(4) ecc.

È stato poi applicato un approccio complementare “top-down” per individuare eventuali lacune o informazioni mancanti. I rischi che non è stato possibile accettare immediatamente sono stati trasferiti nel registri degli eventi pericolosi per un ulteriore trattamento e classificazione.

c uso di principi di accettazione del rischio [sezione 2.1.4]:

Una stima esplicita del rischio è stata eseguita sul sistema nel suo insieme. Tuttavia, è stato possibile utilizzare codici di buona pratica o sistemi di riferimento simili per valutare singoli eventi pericolosi. Il principio è che ogni nuovo sottosistema deve essere sicuro almeno tanto quanto il sottosistema che sostituisce, dando così vita a un nuovo sistema completo con un livello di sicurezza maggiore del precedente. La matrice di rischio della norma EN50126 è stata usata per organizzare gli eventi pericolosi identificati. Sono stati anche applicati diversi criteri di accettazione del rischio supplementari, fra cui:

(1) il guasto singolo non deve determinare una situazione in cui persone, materiale o l'ambiente possono essere seriamente danneggiati;
(2) se ciò non si può evitare con mezzi costruttivi tecnici, si deve evitare mediante norme operative o requisiti di manutenzione. Questa misura si è rivelata applicabile soltanto per gli eventi pericolosi per i quali è stato possibile identificare il guasto verificatosi prima che creasse una situazione pericolosa;
(3) per i componenti con un’elevata probabilità di guasto, o i cui guasti non possono essere individuati in anticipo o evitati mediante la manutenzione o norme operative, devono essere studiate funzioni e barriere di sicurezza supplementari;
(4) sistemi ridondanti con componenti che possono sviluppare guasti impossibili da rilevare durante il funzionamento, devono essere protetti da misure di manutenzione volte ad evitare la riduzione della ridondanza;
(5) il livello di sicurezza finale è stato una decisione della direzione basata sull’analisi quantitativa e qualitativa del rischio;

d dimostrazione della conformità del sistema ai requisiti di sicurezza [sezione 3]:

Sono stati registrati tutti i rischi e gli eventi pericolosi identificati, e l’elenco è stato costantemente consultato e aggiornato. Gli eventi pericolosi restanti sono stati annotati nel registro degli eventi pericolosi insieme con il relativo elenco di misure per la riduzione dei rischi da adottare durante la costruzione, il funzionamento e la manutenzione. Sulla scorta di tutto ciò, è stata elaborata una relazione di sicurezza finale con la verifica sull’avvenuta applicazione dei requisiti di sicurezza;

e gestione degli eventi pericolosi [sezione 4.1]:

Come specificato sopra, gli eventi pericolosi e le relative misure di sicurezza sono stati annotati in un registro degli eventi pericolosi che tiene traccia di tutti gli eventi pericolosi e le misure di sicurezza identificate. Ad ogni modo, gli eventi pericolosi connessi ai rischi accettabili senza tali misure non sono stati inseriti nel registro degli eventi pericolosi;

f valutazione indipendente [Articolo 6]:

Non c’era menzione di una valutazione indipendente all’interno dei documenti ricevuti in relazione a questa modifica significativa.

C.11.7. L’esempio della valutazione del rischio si basa sulla norma CENELEC EN 50126 ed è ben conforme al procedimento del metodo comune di sicurezza. La valutazione del rischio

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

dell'esempio soddisfa tutti i requisiti del metodo comune di sicurezza, ad eccezione del requisito per la valutazione indipendente che non è stato chiarito esplicitamente nei documenti ricevuti. Sono stati usati e indicati chiaramente criteri espliciti di accettazione del rischio.

C.12. Esempio di valutazione del rischio di una modifica operativa significativa – Funzionamento con un solo macchinista

C.12.1. **Nota:** questo esempio di valutazione del rischio non è stato elaborato come conseguenza dell'applicazione del procedimento del metodo comune di sicurezza perché è precedente all'esistenza di quest'ultimo. Lo scopo dell'esempio è:

a identificare le somiglianze fra i metodi di valutazione del rischio esistenti e il procedimento del metodo comune di sicurezza;
b dare tracciabilità fra il procedimento esistente e quello richiesto dal metodo comune di sicurezza;
c fornire una giustificazione del valore aggiunto rappresentato dall'esecuzione delle fasi aggiuntive (se ve ne sono) richieste dal metodo comune di sicurezza.

Occorre sottolineare che questo esempio viene illustrato a titolo puramente informativo. Il suo scopo è quello di aiutare il lettore a comprendere il procedimento del metodo comune di sicurezza. L'esempio in sé non deve essere però applicato su un'altra modifica significativa né utilizzato come sistema di riferimento per quest'ultima. La valutazione del rischio deve essere effettuata per ogni modifica significativa, conformemente al regolamento sul metodo comune di sicurezza.

C.12.2. L'esempio è una modifica operativa in cui l'impresa ferroviaria ha deciso che il treno dovesse essere guidato soltanto da un macchinista (Driver Only Operated – DOO) su un itinerario in cui precedentemente c'era un capotreno a bordo che affiancava il macchinista nelle operazioni di partenza del treno.

C.12.3. Rispetto al procedimento del metodo comune di sicurezza, sono stati applicati i seguenti passi (cfr. anche la Figura 1):

a importanza della modifica [Articolo 4]:

L'impresa ferroviaria ha realizzato una valutazione del rischio preliminare dalla quale è emerso che la modifica operativa era significativa. Poiché il macchinista doveva gestire il treno da solo, senza assistenza, non si poteva trascurare la probabilità che i passeggeri potessero restare impigliati fra le porte o cadere sui binari (p.es. se avessero aperto le porte sul lato sbagliato).

Quando è stata confrontata questa valutazione del rischio preliminare con i criteri dell'Articolo 4 del regolamento sul metodo comune di sicurezza, è stato possibile catalogare la modifica come significativa in base ai seguenti criteri:

(1) importanza per la sicurezza: la modifica riguarda la sicurezza in quanto l'impatto del modo completamente diverso di gestire il funzionamento del servizio ferroviario potrebbe essere catastrofico;
(2) conseguenze in termini di guasti: l'effetto potenziale delle prestazioni del macchinista potrebbe provocare conseguenze catastrofiche se il funzionamento non viene controllato efficacemente;

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) novità: il funzionamento ad opera soltanto del macchinista potrebbe richiedere modi innovativi di far funzionare i treni, i cui rischi devono essere valutati;

b definizione del sistema [sezione 2.1.2]:

La definizione del sistema descriveva:

(1) il sistema esistente, spiegando chiaramente quali compiti fossero realizzati dal macchinista e quali altri dal personale a bordo (o dal capotreno) per affiancare il macchinista;
(2) la modifica delle responsabilità del macchinista dovuta all'eliminazione del personale di assistenza a bordo;
(3) i requisiti tecnici del sistema a copertura delle modifiche nel funzionamento;
(4) i punti d'interazione esistenti fra il personale di assistenza a bordo, il macchinista e il personale a terra del gestore dell'infrastruttura;

Durante le diverse iterazioni, la definizione del sistema è stata aggiornata con i requisiti di sicurezza derivanti dal procedimento di valutazione del rischio. Persone chiave (compresi macchinisti, rappresentanti del personale e il gestore dell'infrastruttura) sono stati coinvolti in questo procedimento iterativo per l'individuazione di eventi pericolosi e l'aggiornamento della definizione del sistema.

c individuazione degli eventi pericolosi [sezione 2.2]:

Gli eventi pericolosi e le possibili misure di sicurezza sono stati identificati mediante un brainstorming di un gruppo di esperti, fra cui:

(1) i rappresentanti dei macchinisti e del personale per la loro esperienza operativa;
(2) i rappresentanti del Gestore dell'Infrastruttura in quanto anche l'infrastruttura poteva essere interessata dalla modifica, per esempio in termini di modifiche alle stazioni (p.es. installazione di specchi/ televisione a circuito chiuso [CCTV] sui marciapiedi);

I compiti supplementari del macchinista sono stati analizzati a fondo per identificare tutti gli eventi pericolosi prevedibili che potrebbero verificarsi a conseguenza dell'eliminazione del personale di assistenza a bordo. In particolare, l'individuazione degli eventi pericolosi ha esaminato quali potessero essere i pericoli operativi più importanti alle stazioni, sugli itinerari esistenti in cui prima vi era l'assistenza del personale a bordo o a terra, compresi la partenza sicura dei treni, questioni specifiche relative al macchinista, materiale rotabile (p.es. controllo dell'apertura/chiusura delle porte), requisiti di manutenzione ecc.

Ad ogni evento pericoloso identificato è stato assegnato un livello di gravità di rischio e di conseguenze (alto, medio, basso) ed è stato rivisto l'impatto della modifica proposta rispetto a questi valori (rischio aumentato, inalterato, ridotto).

d uso di codici di buona pratica [sezione 2.3] ed uso di sistemi di riferimento simili [sezione 2.4]:

Per definire i requisiti di sicurezza per gli eventi pericolosi identificati sono stati usati sia codici di buona pratica (cioè una serie di norme per il DOO) sia sistemi di riferimento simili. Fra i requisiti di sicurezza identificati rientravano:

(1) la revisione delle procedure operative per il macchinista che deve guidare in sicurezza i treni senza assistenza a bordo;
(2) qualsiasi apparecchiatura aggiuntiva necessaria a bordo o a terra per garantire mezzi sicuri ed affidabili per far partire i treni;

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) una lista di controllo per garantire che la cabina di guida è idonea, tenendo conto del punto d'interazione fra il sistema ferroviario (sia a bordo che a terra) e il macchinista;

Sono state riviste le necessarie norme operative conformemente ai requisiti dei codici di buona pratica applicabili e dei relativi sistemi di riferimento. Tutte le parti necessarie sono state coinvolte nella revisione delle procedure operative e nella decisione condivisa di portare avanti la modifica.

e dimostrazione della conformità del sistema ai requisiti di sicurezza [sezione 3]:

Il sistema è stato implementato conformemente ai requisiti di sicurezza identificati (apparecchiatura aggiuntiva e procedure riviste). È stato verificato se fossero mezzi atti a garantire un congruo livello di sicurezza per il sistema sottoposto a valutazione.

Le procedure operative riviste sono state introdotte nel sistema di gestione di sicurezza dell'impresa ferroviaria. Sono state controllate, e all'occorrenza riviste, per garantire che gli eventi pericolosi identificati continuassero ad essere controllati correttamente durante il funzionamento del sistema ferroviario.

f gestione degli eventi pericolosi [sezione 4.1]:

Cfr. il punto qui sopra in quanto per le imprese ferroviarie il procedimento di gestione degli eventi pericolosi può fare parte del loro sistema di gestione della sicurezza per registrare e gestire i rischi. Gli eventi pericolosi identificati sono stati annotati in un registro degli eventi pericolosi con i requisiti di sicurezza che controllano il rischio connesso, cioè facendo riferimento ad apparecchiature supplementari a bordo e a terra nonché alle procedure operative riviste.
Le procedure revisionate sono state controllate, e all'occorrenza riviste, per garantire che gli eventi pericolosi identificati continuassero ad essere controllati correttamente durante il funzionamento del sistema ferroviario.

g valutazione indipendente [Articolo 6]:

Il procedimento di valutazione e gestione del rischio è stato valutato da una persona competente all'interno dell'impresa ferroviaria e indipendente dal procedimento di valutazione. La persona competente ha valutato sia il procedimento sia i risultati, cioè i requisiti di sicurezza identificati.

L'impresa ferroviaria ha basato la sua decisione di attuare il nuovo sistema sulla relazione di valutazione indipendente prodotta dalla persona competente.

C.12.4. L'esempio dimostra che i principi e il procedimento utilizzati dall'impresa ferroviaria sono il linea con il metodo di sicurezza comune. Il procedimento di gestione e valutazione del rischio ha soddisfatto tutti i requisiti del metodo comune di sicurezza.

C.13. Esempio dell'uso di un sistema di riferimento per ricavare requisiti di sicurezza per nuovi sistemi elettronici di interlocking in Germania

C.13.1. **Nota:** questo esempio di valutazione del rischio non è stato elaborato come conseguenza dell'applicazione del procedimento del metodo comune di sicurezza perché è precedente all'esistenza di quest'ultimo. Lo scopo dell'esempio è:

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 identificare le somiglianze fra i metodi di valutazione del rischio esistenti e il procedimento del metodo comune di sicurezza;
b dare tracciabilità fra il procedimento esistente e quello richiesto dal metodo comune di sicurezza;
c fornire una giustificazione del valore aggiunto rappresentato dall'esecuzione delle fasi aggiuntive (se ve ne sono) richieste dal metodo comune di sicurezza.

Occorre sottolineare che questo esempio viene illustrato a titolo puramente informativo. Il suo scopo è quello di aiutare il lettore a comprendere il procedimento del metodo comune di sicurezza. L'esempio in sé non deve essere però applicato su un'altra modifica significativa né utilizzato come sistema di riferimento per quest'ultima. La valutazione del rischio deve essere effettuata per ogni modifica significativa, conformemente al regolamento sul metodo comune di sicurezza.

C.13.2. Al fine di ricavare requisiti di sicurezza standard per futuri sistemi di interlocking elettronici, le ferrovie tedesche (Deutsche Bahn) avevano realizzato un'analisi del rischio di un sistema elettronico già accettato. Quest'ultimo era stato accettato precedentemente in base ai codici di buona pratica tedeschi (Mü 8004).

C.13.3. L'analisi del rischio è stata effettuata conformemente alle norme CENELEC (EN 50126 ed EN 50129) e contemplava i seguenti passi:

a definizione del sistema;
b individuazione degli eventi pericolosi;
c analisi e quantificazione degli eventi pericolosi.

C.13.4. Per la definizione del sistema si era fatta attenzione a definire i limiti del sistema, le sue funzioni ed i suoi punti d'interazione. La sfida principale era definire il sistema in modo tale che fosse indipendente dall'architettura interna del sistema di interlocking restando, al tempo stesso, compatibile con i sistemi di interlocking esistenti. È stata prestata particolare attenzione a definire molto chiaramente i punti d'interazione con sistemi esterni che interagiscono con l'interlocking, senza descrivere dettagliatamente le funzioni interne di quest'ultimo.

C.13.5. Sono stati quindi identificati soltanto gli eventi pericolosi nei punti d'interazione per rimanere sul generico (cioè per evitare qualsiasi dipendenza da architetture specifiche). Sono stati presi in considerazione esclusivamente gli eventi pericolosi derivanti da guasti tecnici. Per ogni punto d'interazione, sono stati così identificati due eventi pericolosi generici:

a segnale di uscita errato trasmesso dall'interlocking al punto d'interazione
b il segnale di ingresso (corretto) viene corrotto nel punto d'interazione

C.13.6. A questi eventi pericolosi generici sono state poi date caratteristiche più specifiche per ogni punto d'interazione.

C.13.7. Nella fase successiva, sono stati analizzati e riuniti in un albero degli eventi i contributi dei componenti del sistema esistente ad ognuno degli eventi pericolosi identificati. In questo modo, in base alla stima degli indici di guasto dei componenti, è stato possibile calcolare un indice di occorrenza per ogni evento pericoloso e usare tali indici come indici di pericolo tollerabile (THR) per le future generazioni di sistemi di interlocking elettronici.

C.13.8. L'analisi del rischio è stata sorvegliata e valutata dall'autorità nazionale preposta alla sicurezza (EBA).

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.13.9. Nell'ambito dell'analisi del rischio è stata condotta altresì un'analisi per le funzioni di controllo e visualizzazione in sistemi elettronici. Anche in questo caso è stato preso come riferimento un sistema di interlocking elettronico esistente già accettato, al fine di ricavare requisiti di sicurezza delle funzioni di punto d'interazione uomo-macchina (MMI) per controllare sia i guasti casuali che i difetti, e per controllare i guasti sistematici. Di conseguenza, sono stati determinati i livelli d'integrità di sicurezza (SIL) per diverse funzioni: per le funzioni MMI in funzionamento standard, per le funzioni MMI in funzionamento "rilascio comandi" (modalità di degrado) e per la funzione di visualizzazione.

C.13.10. L'analisi del rischio è stata anche sorvegliata e valutata dall'autorità nazionale preposta alla sicurezza (EBA).

C.13.11. Questi esempi di valutazione del rischio illustrano come si può utilizzare il secondo criterio di accettazione del rischio (sistema di riferimento) del metodo comune di sicurezza per ricavare requisiti di sicurezza per nuovi sistemi. Inoltre, essi si basavano sulle norme CENELEC è quindi sono ben conformi al procedimento del metodo comune di sicurezza. La valutazione del rischio degli esempi soddisfa i requisiti del metodo comune di sicurezza relativi alle fasi previste. Poiché, però, non figura alcuna attività di progettazione, non si menzionano né la gestione dei registri di eventi pericolosi né la dimostrazione di conformità del sistema sottoposto a valutazione ai requisiti di sicurezza identificati.

C.13.12. Maggiori informazioni su queste analisi del rischio si possono trovare in:

a Ziegler, P., Kupfer, L., Wunder, H.: *"Erfahrungen mit der Risikoanalyse ESTW (DB AG)"*, Signal+Draht, 10, 2003, pp. 10-15, e

b Bock, H., Braband, J., and 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, pp. 234-253.

C.14. Esempio di un criterio esplicito di accettazione del rischio per il funzionamento di treni via radio in Germania (FFB)

C.14.1. **Nota:** questo esempio di valutazione del rischio non è stato elaborato come conseguenza dell'applicazione del procedimento del metodo comune di sicurezza perché è precedente all'esistenza di quest'ultimo. Lo scopo dell'esempio è:

a identificare le somiglianze fra i metodi di valutazione del rischio esistenti e il procedimento dle metodo comune di sicurezza;
b dare tracciabilità fra il procedimento esistente e quello richiesto dal metodo comune di sicurezza;
c fornire una giustificazione del valore aggiunto rappresentato dall'esecuzione delle fasi aggiuntive (se ve ne sono) richieste dal metodo comune di sicurezza.

Occorre sottolineare che questo esempio viene illustrato a titolo puramente informativo. Il suo scopo è quello di aiutare il lettore a comprendere il procedimento del metodo comune disicurezza. L'esempio in sé non deve essere però applicato su un'altra modifica significativa né utilizzato come sistema di riferimento per quest'ultima. La valutazione del rischio deve essere effettuata per ogni modifica significativa, conformemente al regolamento sul metodo comune di sicurezza.

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.14.2. È stata effettuata, conformemente alle norme CENELEC, un'analisi del rischio per una procedura operativa completamente nuova che era stata prevista (ma mai introdotta) in Germania per linee ferroviarie tradizionali. L'idea consisteva nel far funzionare i treni in condizioni di sicurezza soltanto mediante controllo via radio (dell'itinerario e del treno). Poiché non esistevano codici di buona pratica (regole ingegneristiche riconosciute) e sistemi di riferimento per un nuovo sistema di questo tipo, è stata effettuata la stima esplicita del rischio al fine di dimostrare la sicurezza della nuova procedura. È stato necessario dimostrare che il livello di rischio per un passeggero dovuto al nuovo sistema non avrebbe superato un valore di rischio accettabile (criterio esplicito di accettazione del rischio).

C.14.3. Questo criterio esplicito di accettazione del rischio è stato stimato sulla base di statistiche tedesche di incidenti attribuibili a sistemi di segnalamento e controllo, ed anche la sua plausibilità è stata verificata rispetto al criterio MEM. Tale dimostrazione di sicurezza è conforme al requisito tedesco EBO di avere "lo stesso livello di sicurezza" in caso di deviazioni da regole ingegneristiche. L'analisi del rischio è stata anche sorvegliata e valutata dall'autorità nazionale preposta alla sicurezza (EBA).

C.14.4. Questo esempio di valutazione del rischio mostra come si può ricavare un criterio esplicito complessivo (per il terzo principio di accettazione del rischio del metodo comune di sicurezza) per nuovi sistemi senza codici di buona pratica applicabili né sistemi di riferimento. L'analisi del rischio effettuata successivamente per il nuovo sistema si basa sulle norme CENELEC ed è quindi ben conforme al procedimento del metodo comune di sicurezza. L'analisi del rischio dell'esempio soddisfa i requisiti del metodo comune di sicurezza, ma non si menziona né la gestione di registri di eventi pericolosi né la dimostrazione della conformità del sistema sottoposto a valutazione ai requisiti di sicurezza identificati.

C.14.5. Maggiori informazioni su questa analisi del rischio si possono trovare in: Braband, J., Günther, J., Lennartz, K., Reuter, D.: *"Risikoakzeptanzkriterien für den FunkFahrBetrieb (FFB)"*, Signal + Draht, Nr.5, 2001, pp. 10-15

C.15. Esempio di test di applicabilità del RAC-TS

C.15.1. Lo scopo di quest'appendice è quello di illustrare, in un esempio della funzione del sottosistema di bordo ETCS, come utilizzare il criterio della sezione 2.5.4 e come determinare se il RAC-TS è applicabile.

C.15.2. Il sottosistema di bordo ETCS è un sistema tecnico. Si studia la seguente funzione: *"fornire al macchinista le informazioni necessarie affinché possa guidare il treno in condizioni di sicurezza e frenare in caso di eccesso di velocità"*.

Descrizione della funzione: sulla base delle informazioni ricevute da terra (velocità ammessa) e della velocità del treno calcolata dal sottosistema di bordo ETCS:

a il macchinista guida il treno e garantisce che la velocità del treno non superi i valori consentiti;

b parallelamente, il sottosistema di bordo ETCS controlla che il treno non superi mai il limite di velocità consentito. In caso di eccesso di velocità, applica automaticamente i freni.

Sia il macchinista che il sottosistema di bordo ETCS utilizzano la valutazione della velocità del treno calcolata dal sottosistema di bordo ETCS.

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.15.3. Domanda: “Il RAC-TS si applica alla valutazione della velocità del treno fatta dal sottosistema di bordo?"

C.15.4. Applicazione del diagramma di flusso della Figura 14 e risposte alle diverse domande:

a Evento pericoloso analizzato per il sistema tecnico:

"Superamento della velocità di sicurezza raccomandata all'ETCS" (cfr. UNISIG SUBSET 091).

b Può questo evento pericoloso essere controllato da un codice di buona pratica o da un sistema di riferimento?

NO. Si presume che il sistema ETCS sia un progetto nuovo e innovativo. Di conseguenza, non ci sono codici di buona pratica o sistemi di riferimento che possano consentire di controllare l'evento pericoloso ad un livello di rischio accettabile.

c È probabile che l'evento pericoloso provochi conseguenze catastrofiche?

SÌ, poiché *"superare la velocità di sicurezza raccomandata all'ETCS"* può portare al deragliamento del treno che, potenzialmente, può provocare *"vittime mortali e/o numerose lesioni gravi e/o ingenti danni all'ambiente"*.

d La conseguenza catastrofica è il risultato diretto del guasto del sistema tecnico?

SÌ se non vi sono barriere di sicurezza aggiuntive. La stessa valutazione della velocità del treno calcolata dal sottosistema di bordo ETCS viene fornita sia al macchinista sia alla funzione di controllo dei freni del sottosistema di bordo ETCS. Di conseguenza, supponendo che il macchinista stia guidando il treno alla velocità massima ammessa dagli impianti a terra (per motivi di rendimento), né il macchinista né il sottosistema di bordo ETCS rileveranno che il treno è in eccesso di velocità nel caso in cui la velocità del treno venga sottostimata. Questa situazione può portare potenzialmente al deragliamento del treno con conseguenze catastrofiche.

e Conclusioni:

(1) per i requisiti quantitativi: applicare un THR di 10^{-9} h^{-1} per i guasti casuali dell'hardware del sottosistema di bordo ETCS, garantendo che:

(i) la valutazione di questo target quantitativo tiene conto, per sistemi ridondanti, dei componenti comuni (p.es. input singoli o input comuni a tutti i canali, alimentazione comune, comparatori, voter, ecc.);
(ii) sono coperti i tempi di rilevamento dei guasti latenti;
(iii) viene effettuata un'analisi dei guasti per causa/di modo comune (CCF/CMF;
(iv) viene effettuata una valutazione indipendente;

(2) per i requisiti di procedimento: applicare un procedimento SIL per la gestione di guasti/errori sistematici del sottosistema di bordo ETCS. Ciò richiede l'applicazione di:

(i) un procedimento di gestione della qualità conforme al SIL 4;
(ii) un procedimento di gestione della sicurezza conforme al SIL 4;
(iii) le norme pertinenti, p.es.:

- per lo sviluppo del software l'uso della norma EN 50 128;
- per lo sviluppo dell'hardware l'uso delle norme 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 ecc.;

(3) una valutazione indipendente del(i) procedimento(i).

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. Esempi di possibili strutture per il registro degli eventi pericolosi

C.16.1. Introduzione

C.16.1.1. I requisiti minimi da annotare nel registro degli eventi pericolosi sono identificati nella sezione 4.1.2 del regolamento sul metodo comune di sicurezza. Negli esempi riportati di seguito sono indicati con uno sfondo ombreggiato.

C.16.1.2. Vi possono essere diversi modi di strutturare un registro degli eventi pericolosi, così come qualsiasi informazione supplementare che potrebbe caratterizzare gli eventi pericolosi e le misure di sicurezza connesse. Per esempio, gli eventi pericolosi e le misure di sicurezza connesse possono essere dotati di un campo per ciascuna informazione. Tuttavia, indipendentemente dalla struttura utilizzata, è importante che il registro degli eventi pericolosi fornisca chiari collegamenti fra i pericoli e le misure di sicurezza connesse. Una possibile soluzione è che il registro degli eventi pericolosi contenga, per ogni evento pericoloso e per ogni misura di sicurezza, almeno un campo con:

a una chiara descrizione, compresi riferimenti alla sua origine e al principio di accettazione del rischio selezionato per controllare l'evento pericoloso connesso. Questo campo consente di comprendere l'evento pericoloso e le misure di sicurezza connesse, nonché di sapere in quali analisi di sicurezza sono identificati.

Poiché il registro degli eventi pericolosi è usato e gestito per l'intero ciclo di vita del sistema (cioè durante il funzionamento e la manutenzione del sistema), è utile dare una chiara tracciabilità, o un collegamento, fra ogni evento pericoloso e:

(1) il rischio connesso;
(2) le cause degli eventi pericolosi ove già identificate;
(3) le misure di sicurezza connesse, nonché le ipotesi che definiscono i limiti del sistema sottoposto a valutazione;
(4) le relative analisi di sicurezza in cui è identificato l'evento pericoloso;

Inoltre, la formulazione di misure di sicurezza (specialmente di quelle da trasferire ad altri operatori come ad esempio il proponente) e la formulazione degli eventi pericolosi e dei rischi connessi devono essere chiare e sufficienti. "Chiare e sufficienti" significa che è possibile capire quali rischi ci si aspetta che le misure di sicurezza e gli eventi pericolosi connessi controllino, senza dover consultare le relative analisi di sicurezza precedenti.

b il principio di accettazione del rischio utilizzato per controllare l'evento pericoloso al fine di sostenere il reciproco riconoscimento e aiutare l'organismo di valutazione a valutare la corretta applicazione del metodo comune di sicurezza;

c una chiara informazione sul suo stato: questo campo indica se l'evento pericoloso/la misura di sicurezza connessi sono ancora aperti o già controllati/validati.

(1) un evento pericoloso/una misura di sicurezza vengono tracciati fino a che non sono controllati/validati;
(2) reciprocamente, gli eventi pericolosi/le misure controllate/validate non sono più tracciate a meno che non si verifichino delle modifiche significative durante il funzionamento o la manutenzione del sistema: cfr. il punto [G 6](b) della sezione 2.1.1. Se ciò accade:

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) il metodo comune di sicurezza viene applicato nuovamente alle modifiche richieste, conformemente all'Articolo 2. Cfr. anche il punto [G 6](b)(1) della sezione 2.1.1;
(ii) tutti gli eventi pericolosi e le misure di sicurezza controllati vengono riesaminati per verificare che non siano interessati dalle modifiche. In caso contrario, i pericoli in questione e le misure di sicurezza connesse vengono riaperti e gestiti nuovamente nel registro degli eventi pericolosi;

Potrebbe accadere che vengono implementate misure di sicurezza diverse da quelle annotate nel registro degli eventi pericolosi (p.es. per motivi di costi). Le misure di sicurezza implementate vengono quindi annotate nel registro degli eventi pericolosi con la prova/giustificazione della loro idoneità e la dimostrazione che con tali misure il sistema è conforme ai requisiti di sicurezza.

d il riferimento alle prove connesse che controllano un evento pericoloso o validano una misura di sicurezza. Questo campo consente di trovare in un secondo momento la prova che ha permesso di controllare l'evento pericoloso e di validare la(le) misura(e) di sicurezza connesse.

Un evento pericoloso potrebbe essere considerato controllato nel registro degli eventi pericolosi soltanto quando tutte le misure di sicurezza connesse, legate al pericolo, sono già validate;

e la(e) società o l'ente/gli enti responsabile(i) di gestirlo.

C.16.1.3. Un altro esempio di possibile contenuto di un registro degli eventi pericolosi è riportato nell'appendice A.3 della guida EN 50126-2 {Ref. 9}.

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. Esempio del registro degli eventi pericolosi per la modifica organizzativa della sezione C.5. dell'appendice C

Tabella 6: Esempio del registro degli eventi pericolosi per la modifica organizzativa della sezione C.5. dell'appendice C.

Descrizione dell'evento pericoloso	**Misure di sicurezza**	**Priorità/ Sicurezza Puntualità**	**Imple-mentazione[18)]**	**Note**	**Respon-sabilità[18)]**	**Origine**	**Principio di accettazione del rischio utilizzato**	**Responsabilità della verifica**	**Modalità di verifica**	**Stato xx.xx.xx**
Ridotta motivazione fra i dipendenti che restano nell'azienda. Il personale, quindi, continua ad andare via regolarmente. Responsabili demotivati / sfiniti	Nuova tornata di lavoro di motivazione per il personale, da realizzare in piccoli gruppi Riassegnazione di fondi in modo tale che la società acquisisca compiti importanti da svolgere Ispezioni più frequenti da parte del gestore della linea. Assegnare fondi per fare in modo che il personale chiave resti per tutta la durata delle attività. Prestare particolare attenzione a fare sì che vi sia il trasferimento di informazioni e conoscenza fra i dipendenti che lasciano l'azienda e quelli che rilevano i loro compiti ecc.	Alta/Alta	Coordinata da XYZ. Le sedi periferiche devono studiare misure atte ad aumentare il controllo di linee, sovrapposizione di dipendenti e supervisione da parte del gestore della linea	Nei contratti si devono inserire maggiori ispezioni ecc.	Direttore dell'impresa	Brainstorming Relazione HAZID R_X	N/D			Il cambiamento di condizioni e circostanze ha ridotto sensibilmente questo rischio Realizzazione di analisi dell'ambiente di lavoro e formazione del personale.
Subappaltatori degli imprenditori mancano di abilità, competenza e controllo di qualità	Maggiore richiesta di competenze documentate. Controllo sistematico dei compiti svolti	Alta/ Media	Il Gestore dell'Infrastruttura deve coordinare. Le sedi periferiche devono mettere in atto misure atte a	Attuata mediante la supervisione dei contratti. Suggerimento di una pianificazione di revisioni.	Gestore dell'infrastruttura	Brain-storming Relazione HAZID R_X	N/D	Responsabile della sicurezza		Maggiore attenzione ai programmi di controllo (2 controlli operativi al mese e per settore operativo)

(18) *Queste due colonne riguardano le informazioni/il campo sugli operatori responsabili di controllare gli eventi pericolosi identificati.*

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

Tabella 6: Esempio del registro degli eventi pericolosi per la modifica organizzativa della sezione C.5. dell'appendice C.

Descrizione dell'evento pericoloso	Misure di sicurezza	Priorità/ Sicurezza Puntualità	Imple-mentazione[18]	Note	Respon-sabilità[18]	Origine	Principio di accettazione del rischio utilizzato	Responsabilità della verifica	Modalità di verifica	Stato xx.xx.xx
			richiedere competenza e a controllare il lavoro							
Incertezza di ruoli e responsabilità nel punto d'interazione fra la società e il gestore dell'infrastruttura (gestore della linea).	Definire ruoli e responsabilità. Mappare tutti i punti d'interazione e definire chi ne è il responsabile.	Media/ Media	In ogni sede periferica separatamente	Attuata dal contratto di manutenzione e dal piano strategico per la riorganizzazione	Direttori delle sedi periferiche	Brain-storming relazione HAZID R_X	N/D	Responsabile della sicurezza		Le sedi periferiche hanno presentato la loro strategia.

C.16.3. Esempio di un registro degli eventi pericolosi completo per un sottosistema di controllo-comando di bordo

C.16.3.1. Questa sezione illustra un esempio di un unico registro degli eventi pericolosi (cfr. il punto [G 3] della sezione 4.1.1) per gestire:

a tutti i requisiti di sicurezza interni applicabili al sottosistema di cui l'operatore è responsabile; e,

b tutti gli eventi pericolosi identificati e le misure di sicurezza connesse che l'operatore non può implementare e che devono essere trasferite ad altri operatori.

Tabella 7: Esempio di un registro degli eventi pericolosi del produttore per un sottosistema di controllo-comando di bordo.

N° PER.	Origine	Descrizione dell'evento pericoloso	Informazioni supplementari	Operatore responsabile	Misura di sicurezza	Principio di accettazione del rischio utilizzato	Esportato	Stato
1	Relazione HAZOP	Impostazione troppo alta della velocità massima del treno (Vmax)	Configurazione specifica errata del sottosistema di bordo (personale di manutenzione). Immissione dati errata a bordo (macchinista)	Impresa ferroviaria	• Definire una procedura per l'approvazione dei dati di configurazione del sottosistema	Stima esplicita del rischio	Sì	Controllato (esportato alla RU) Cfr. anche 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

Tabella 7: Esempio di un registro degli eventi pericolosi del produttore per un sottosistema di controllo-comando di bordo.

N° PER.	Origine	Descrizione dell'evento pericoloso	Informazioni supplementari	Operatore responsabile	Misura di sicurezza	Principio di accettazione del rischio utilizzato	Esportato	Stato
	R_X				di bordo; • Definire una procedura operativa per il processo di immissione dati da parte del macchinista;			sezione C.16.4.2. dell'appendice C
2	Relazione HAZOP R_X	Curve di frenatura (cioè autorizzazione al movimento) nei dati di configurazione del sottosistema di bordo troppo tolleranti	La procedura per la specifica configurazione del sottosistema di bordo dipende da: • i margini di sicurezza presi per il sistema frenante del treno; • il ritardo di reazione del sistema frenante del treno (questo dipende direttamente dalla lunghezza del treno, specialmente per treni merci)	Impresa ferroviaria	• Specificare correttamente i requisiti del sistema nella definizione del sistema; • Prendere margini di sicurezza sufficienti per il sistema frenante dello specifico treno;	Stima esplicita del rischio	Sì	Controllato (esportato alla RU) Cfr. anche la sezione C.16.4.2. dell'appendice C
3	Relazione HAZOP R_X	• Impostazione troppo alta della velocità massima del treno (Vmax) • Curve di frenatura (cioè autorizzazione al movimento) nei dati di configurazione del sottosistema di bordo troppo tolleranti	Mancato aggiornamento del diametro delle ruote del treno nella specifica configurazione del sottosistema di bordo (personale di manutenzione).	Impresa ferroviaria	• Definire una procedura per la misurazione del diametro delle ruote dei treni da parte del personale addetto alla manutenzione; • Definire una procedura per l'aggiornamento regolare del diametro delle ruote dei treni nel sottosistema di bordo;	Stima esplicita del rischio	Sì	Controllato (esportato alla RU) Cfr. anche la sezione C.16.4.2. dell'appendice C
			Problema nella procedura del produttore per la preparazione e il caricamento dei dati di configurazione nel sottosistema di bordo	Produttore	Definire una procedura per aggiornare il diametro delle ruote dei treni nei dati di configurazione di bordo	Stima esplicita del rischio	Sì	Controllato mediante procedura P_X
4	Relazione HAZOP R_X	Ingresso del treno ad alta velocità (160 km/h se il segnale a terra è di libero) sul binario senza un sottosistema di bordo attivo e senza segnalamento di terra	Potrebbe essere controllato soltanto dalla vigilanza del macchinista. L'ingresso in una zona dotata di sistema ATP di terra dipende dalla procedura di conferma del macchinista prima del punto di transito. Senza tale conferma vi è l'applicazione automatica dei freni del treno azionata dal sottosistema di controllo-comando di bordo.	Gestore dell'infrastruttura	Il gestore dell'infrastruttura deve garantire che i treni che non sono dotati di un sottosistema di controllo-comando di bordo attivo non entrino nel binario in questione. Definire una procedura per la gestione del traffico.	Stima esplicita del rischio	Sì	Controllato (esportato all'IM) Cfr. anche la sezione C.16.4.2. dell'appendice C
				Impresa	Garantire la formazione dei	Stima	Sì	Controllato

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

Tabella 7: Esempio di un registro degli eventi pericolosi del produttore per un sottosistema di controllo-comando di bordo.

N° PER.	Origine	Descrizione dell'evento pericoloso	Informazioni supplementari	Operatore responsabile	Misura di sicurezza	Principio di accettazione del rischio utilizzato	Esportato	Stato
				ferroviaria	macchinisti per l'ingresso in una zona dotata di sistema ATP di terra	esplicita del rischio		(esportato alla RU) Cfr. anche la sezione C.16.4.2. dell'appendice C
5	Relazione HAZOP R_X	Impostazione della velocità massima del treno visualizzata al macchinista troppo elevata (Vmax)	Le informazioni visualizzate sul punto d'interazione del macchinista vengono controllate dal sottosistema SIL 4 di controllo-comando di bordo che applica i freni di emergenza in caso di divergenza fra il valore visualizzato e il valore previsto. In caso di non conformità all'autorizzazione al movimento, il sottosistema di controllo-comando di bordo applica i freni di emergenza	Produttore	Sviluppare un sottosistema SIL 4 di controllo-comando di bordo	Stima esplicita del rischio	Sì	Safety Case che dimostra un sottosistema SIL 4 valutato da un Valutatore indipendente della sicurezza
6	Relazione HAZOP R_X	Il treno è in partenza senza il punto d'interazione macchinista-macchina	Perdita dell'architettura ridondante del sottosistema di bordo	Produttore	Sviluppare un sottosistema SIL 4 di controllo-comando di bordo	Stima esplicita del rischio	Sì	Safety Case che dimostra un sottosistema SIL 4 valutato da un Valutatore indipendente della sicurezza
etc.								

C.16.4. Esempio di un registro degli eventi pericolosi per il trasferimento di informazioni ad altri operatori

C.16.4.1 Questa sezione illustra in un esempio un registro degli eventi pericolosi per il trasferimento ad altri operatori degli eventi pericolosi identificati e delle misure di sicurezza connesse che un determinato operatore non è in grado di implementare. Vedere il punto [G 1] della sezione 4.1.1.
Questo esempio è uguale all'esempio della sezione C.16.3. dell'appendice C. L'unica differenza è che tutti gli eventi pericolosi interni e le misure di sicurezza che potrebbero essere controllate dall'operatore in questione sono rimossi.

C.16.4.2. L'ultima colonna della Tabella 8 è usata per soddisfare il requisito della sezione 4.2 del regolamento sul metodo comune di sicurezza. Vi sono diverse soluzioni per poterlo fare. Uno dei modi potrebbe essere quello di consultare le prove utilizzate dall'operatore che riceve le informazioni di sicurezza

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

esportate. Un altro potrebbe essere quello di tenere una riunione fra i due operatori affinché trovino insieme la soluzione adatta a controllare il(i) rischio(i) connesso(i). I risultati di questa riunione potrebbero essere riportati su un documento condiviso (per esempio un verbale) che l'operatore che esporta le informazioni relative alla sicurezza può consultare per chiudere gli eventi pericolosi connessi nel proprio registro degli eventi pericolosi.

Tabella 8: Esempio di un registro degli eventi pericolosi per il trasferimento di informazioni relative alla sicurezza ad altri operatori.

N° PERICOLO	Origine del pericolo		Descrizione dell'evento pericoloso	Informazioni supplementari	Operatore responsabile	Misura di sicurezza	Commento del ricevente
	N° in Tabella 7	Altro					
1	N°1	Relazione HAZOP R_X	Impostazione troppo alta della velocità massima del treno (Vmax)	Configurazione specifica errata del sottosistema di bordo (personale di manutenzione). Immissione dati errata a bordo (macchinista)	Impresa ferroviaria	• Definire una procedura per l'approvazione dei dati di configurazione del sottosistema di bordo; • Definire una procedura operativa per il processo di immissione dati da parte del macchinista;	• I dati di configurazione del sottosistema di controllo-comando di bordo dipendono da caratteristiche fisiche del materiale rotabile. • Margini di sicurezza sono poi applicati a questi dati dal gestore dell'infrastruttura in collaborazione con l'impresa ferroviaria. • I dati sono poi caricati nel sottosistema di bordo conformemente alla relativa procedura del produttore durante l'installazione, l'integrazione nel materiale rotabile e l'omologazione del sottosistema di controllo-comando. • I macchinisti vengono formati e valutati secondo i criteri della procedura D_P. • I macchinisti sono anche valutati dall'IM in base alle norme applicabili all'infrastruttura dell'IM.
2	N°2	Relazione HAZOP R_X	Curve di frenatura (cioè autorizzazione al movimento) nei dati di configurazione del sottosistema di bordo troppo tolleranti	La procedura per la specifica configurazione del sottosistema di bordo dipende da: • i margini di sicurezza presi per il sistema frenante del treno; • il ritardo di reazione del sistema frenante del treno (questo dipende direttamente dalla lunghezza del treno, specialmente per treni merci)	Impresa ferroviaria	• Specificare correttamente i requisiti del sistema nella definizione del sistema; • Prendere margini di sicurezza sufficienti per il sistema frenante dello specifico treno;	Cfr. commento per la linea 1 di cui sopra.
3	N°3	Relazione HAZOP R_X	• Impostazione troppo alta della velocità massima del treno (Vmax) • Curve di frenatura (cioè autorizzazione al movimento) nei	Mancato aggiornamento del diametro delle ruote del treno nella specifica configurazione del sottosistema di bordo (personale di manutenzione).	Impresa ferroviaria	• Definire una procedura per la misurazione del diametro delle ruote dei treni da parte del personale addetto alla manutenzione; • Definire una procedura per l'aggiornamento regolare	• La manutenzione del sottosistema di controllo-comando di bordo avviene conformemente alla "Procedura di manutenzione MP_Z". • Il diametro delle ruote dei treni è aggiornato a intervalli stabiliti in base alla procedura P_W. • Per il processo di immissione dati, i macchinisti sono formati e valutati in base ai criteri della "Procedura 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

Tabella 8: Esempio di un registro degli eventi pericolosi per il trasferimento di informazioni relative alla sicurezza ad altri operatori.

N° PERICOLO	Origine del pericolo		Descrizione dell'evento pericoloso	Informazioni supplementari	Operatore responsabile	Misura di sicurezza	Commento del ricevente
	N° in Tabella 7	Altro					
			dati di configurazione del sottosistema di bordo troppo tolleranti			del diametro delle ruote dei treni nel sottosistema di bordo;	
4	N°4	Relazione HAZOP R_X	Ingresso del treno ad alta velocità (160 km/h se il segnale a terra è di libero) sul binario senza un sottosistema di bordo attivo e senza segnalamento di terra	Potrebbe essere controllato soltanto dalla vigilanza del macchinista. L'ingresso in una zona dotata di sistema ATP di terra dipende dalla procedura di conferma del macchinista prima del punto di transito. Senza tale conferma vi è l'applicazione automatica dei freni del treno azionata dal sottosistema di controllo-comando di bordo.	Gestore dell'infrastruttura	Il gestore dell'infrastruttura deve garantire che i treni che non sono dotati di un sottosistema di controllo-comando di bordo attivo non entrino nel binario in questione. Definire una procedura per la gestione del traffico.	La gestione del traffico sull'infrastruttura dell'IM è regolata dalle norme R_{TM}
					Impresa ferroviaria	Garantire la formazione dei macchinisti per l'ingresso in una zona dotata di sistema ATP di terra	• I macchinisti sono formati regolarmente secondo la procedura P_{IM_DP} dell'IM. • I macchinisti sono anche valutati dall'IM in base alle norme (S_R) applicabili sull'infrastruttura dell'IM.
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. Esempio di un elenco di eventi pericolosi generici per il funzionamento ferroviario

C.17.1. Il progetto ROSA (Rail Optimisation Safety Analysis) [Anali di sicurezza per l'ottimizzazione delle ferrovie], svolto nell'ambito del programma DEUFRAKO (cooperazione franco-tedesca) ha cercato di creare un elenco di eventi pericolosi generici ed esaustivi nell'ambito del funzionamento standard delle ferrovie. L'obiettivo, e la sfida, erano quelli di definire questi eventi pericolosi con il massimo livello di dettaglio possibile pur non riflettendo le specificità delle ferrovie francesi e tedesche. L'elenco è stato creato utilizzando elenchi di pericoli attualmente in uso di entrambi i paesi (SNCF e DB) ed è stato anche confrontato con gli elenchi di eventi pericolosi di altri paesi. Malgrado l'obiettivo dichiarato di essere completo e generico, l'elenco viene riportato esclusivamente a titolo di esempio indicativo che potrebbe essere utile agli operatori al momento di identificare gli eventi pericolosi per un determinato progetto. Si suppone che gli eventi pericolosi indicati in questo elenco probabilmente dovranno essere perfezionati o integrati per riflettere le specificità di un determinato progetto.

C.17.2. Gli eventi pericolosi descritti nella bozza di elenco in basso sono detti "pericoli di partenza" (SPH), cioè eventi pericolosi dai quali si potrebbe effettuare sia un'analisi delle conseguenze sia un'analisi delle cause, al fine di determinare misure di sicurezza/barriere e requisiti di sicurezza per controllare gli eventi pericolosi.

C.17.3. Elenco degli eventi pericolosi del progetto ROSA:

SPH 01	Errata determinazione iniziale del limite di velocità (relative all'infrastruttura)
SPH 02	Errata determinazione del limite di velocità (relativo al treno)
SPH 03	Errata determinazione della distanza di frenata/ errato profilo di velocità/ errate curve di frenatura
SPH 04	Decelerazione insufficiente (cause fisiche)
SPH 05	Errato/inadeguato comando di velocità/freno
SPH 06	Errata velocità rilevata (treno a velocità errata)
SPH 07	Mancata comunicazione del limite di velocità
SPH 08	Il treno si muove
SPH 09	Errata direzione di Marcia/ retromarcia intenzionale - (abbinamento di SPH 08 ed SPH 14)
SPH 10	Errata registrazione della posizione assoluta/relativa
SPH 11	Mancato rilevamento del treno
SPH 12	Perdita di integrità del treno
SPH 13	Possibile itinerario errato per il treno
SPH 14	Mancata trasmissione/comunicazione dell'orario/MA (autorizzazione al movimento)
SPH 15	Guasto strutturale al binario
SPH 16	Componente deviatoio rotto
SPH 17	Comando deviazione errato
SPH 18	Stato deviatoio errato
SPH 19	Oggetto di sistema sul binario/ entro CE (sagoma limite) (escl. massicciata)
SPH 20	Oggetto estraneo sul binario/ entro CE
SPH 21	Utente del traffico stradale nell'aerea del passaggio a livello
SPH 22	Effetti scia sulla massicciata
SPH 23	Sollecitazioni aerodinamiche interessano il treno
SPH 24	Apparecchiatura / elemento/ carico del treno viola la CE
SPH 25	Inadeguata dimensione CE per il treno (lato)
SPH 26	Errata distribuzione del carico

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 27	Ruota rota, asse rotto
SPH 28	Asse / ruota / supporto bollenti
SPH 29	Guasto al carrello/alla sospensione, smorzamento
SPH 30	Guasto del telaio/cassa della vettura
SPH 31	Introduzione abusiva (aspetto di sicurezza)
SPH 32	Una persona autorizzata attraversa il binario
SPH 33	Personale al lavoro sul binario
SPH 34	Una persona non autorizzata si introduce nella zona tra i binari (negligenza)
SPH 35	Una persona cade dal bordo della banchina sul binario
SPH 36	Scia/persona troppo vicina al bordo della banchina
SPH 37	Personale al lavoro vicino al binario p.es. binario adiacente
SPH 38	Una persona lascia il treno intenzionalmente (escl. ingresso/uscita dei passeggeri)
SPH 39	Una persona cade dalla porta (laterale)
SPH 40	Una persona cade dalla porta sulla parete di fondo
SPH 41	Il treno parte/si allontana con le porte aperte (non viola la CE)
SPH 42	Una persona cade nella zona di passaggio fra due vetture
SPH 43	Un passeggero si sporge dalla porta
SPH 44	Un passeggero si sporge dal finestrino
SPH 45	Il personale/l'assistente di bordo treno si sporge dalla porta
SPH 46	Il personale/l'assistente di bordo treno si sporge dal finestrino
SPH 47	Il personale di manovra sul veicolo si sporge dal predellino
SPH 48	Una persona cade dalla banchina nello spazio vuoto fra il veicolo e la banchina, e viceversa
SPH 49	Una persona cade/esce dal treno senza la banchina
SPH 50	Una persona cade nella zona porte nella fase di ingresso/uscita dei passeggeri
SPH 51	Le porte del treno si chiudono con una persona in zona porte
SPH 52	Il treno si muove durante lo scambio di passeggeri
SPH 53	Possibilità di persona ferita sul treno
SPH 54	Pericolo d'incendio/esplosione (sul/al treno) – categoria incidenti, Conseguenza di SPH 55, SPH 56)
SPH 55	Temperatura inadeguata (sul treno)
SPH 56	Intossicazione/asfissia (sul/al treno)
SPH 57	Elettrocuzione (sul/al treno)
SPH 58	Una persona cade sul binario (escluso lo scambio passeggeri)
SPH 59	Temperatura inadeguata(sulla banchina)
SPH 60	Intossicazione/asfissia (sulla banchina)
SPH 61	Elettrocuzione (sulla banchina)

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