| Europäische Eisenbahnagentur | |
|---|---|
| **Sammlung von Beispielen für Risikobewertungen und möglicher Werkzeuge zur Unterstützung der CSM-Verordnung** | |
| **Zeichen in ERA:** | ERA/GUI/02-2008/SAF |
| **Version in ERA:** | 1.1 |
| **Datum:** | 06/01/2009 |

| | |
|---|---|
| **Dokument erstellt von:** | Europäische Eisenbahnagentur<br>Boulevard Harpignies, 160<br>BP 20392<br>F-59307 Valenciennes Cedex<br>Frankreich |
| **Dokumenttyp:** | Leitlinie |
| **Dokumentenstatus:** | Öffentlich |

| | **Name** | **Funktion** |
|---|---|---|
| **Freigegeben von:** | Marcel VERSLYPE | Leitender Direktor |
| **Geprüft von:** | Anders LUNDSTRÖM<br>Thierry BREYNE | Leiter Sicherheitsreferat<br>Leiter Sicherheitsbewertung |
| **Verfasser (Autor)** | Dragan JOVICIC | Sicherheitsreferat - Projektkoordinator |



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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

# DOKUMENTINFORMATION

## Änderungsverwaltung

***Tabelle 1: Dokumentenstatus***

| Fassung Datum | Verfasser | Dokumentteil | Änderungsbeschreibung |
|---|---|---|---|
| **Titel und Struktur des alten Dokuments: *„Gebrauchsanleitung zur Empfehlung der ersten Reihe gemeinsamer Sicherheitsmethoden (CSM)“*** | | | |
| Anleitung Version 0.1 15/02/2007 | Dragan JOVICIC | Komplett | Erste Fassung der „Gebrauchsanleitung“ im Zusammenhang mit der Version 1.0 der „Ersten Reihe von CSM-Empfehlungen“. Dies ist auch die erste Fassung des Dokumentes, die der CSM-Arbeitsgruppe zur formalen Prüfung vorgelegt wurde. |
| Anleitung Version 0.2 07/06/2007 | Dragan JOVICIC | Komplett | Umstrukturierung des Dokuments zur Anpassung an die Struktur der Version 4.0 der CSM-Empfehlung. Aktualisierung ggü. formalem Prüfverfahren durch die CSM-Arbeitsgruppe der Version 1.0 der Empfehlung. |
| | | Komplett | Aktualisierung des Dokuments durch zusätzliche Informationen aus ERA-internen Besprechungen und durch Anforderungen der Taskforce und Arbeitsgruppe CSM zur Entwicklung neuer Punkte. |
| | | Abbildung 1 | Änderung der Abbildung „Risikomanagementrahmen für die erste Reihe gemeinsamer Sicherheitsmethoden“ entsprechend den Prüfkommentaren und der ISO-Terminologie. |
| Anleitung Version 0.3 20/07/2007 | Dragan JOVICIC | Anhänge | Umstrukturierung vorhandener und Erstellung neuer Anhänge. Neue Anlage zur Zusammenführung aller Grafiken, die die Lektüre und das Verständnis der Leitlinie illustrieren und erleichtern. |
| | | Alle Abschnitte | Dokument wie folgt aktualisiert:<br>• größtmögliche Entwicklung bestehender x-Abschnitte;<br>• Weiterentwicklung in punkto „Nachweis der Einhaltung der Sicherheitsanforderungen“;<br>• Verknüpfung mit CENELEC V-Darstellung (d. h. Abb. 8 und Abb. 10 von EN 50 126);<br>• Weiterentwicklung des Bedarfs an Zusammenarbeit und Koordinierung der verschiedenen Akteure der Eisenbahnbranche, deren Aktivitäten eine potenziellen Einfluss auf die Sicherheit des Eisenbahnsystems haben;<br>• Klärungen zu den Nachweisen (z. B. Gefährdungsprotokoll und Sicherheitsnachweis), die die ordnungsgemäße Anwendung des CSM-Risikobewertungsverfahrens gegenüber den Bewertungsstellen belegen;<br>Hinzu kommt die Aktualisierung des Dokumentes entsprechend einer ersten agenturinternen Prüfung (Revision). |
| Anleitung Version 0.4 16/11/2007 | Dragan JOVICIC | Alle Abschnitte | Aktualisierung des Dokuments nach Abschluss des formalen Prüfungsverfahrens entsprechend den Anmerkungen, die von den folgenden Mitgliedern der CSM-Arbeitsgruppe bzw. Organisationen in Bezug auf Version 0.3 vorgelegt und mit diesen telefonisch abgesprochen wurden:<br>• Nationale Sicherheitsbehörden Belgien, Spanien, Finnland, Norwegen, Frankreich und Dänemark;<br>• SIEMENS (UNIFE-Mitglied);<br>• Norwegischer Fahrwegbetreiber (Jernbaneverket – EIM-Mitglied); |
| Anleitung Version 0.5 27/02/2008 | Dragan JOVICIC | Alle Abschnitte | Aktualisierung des Dokuments entsprechend den Rücklauf-bemerkungen, die von den folgenden Mitgliedern der CSM-Arbeitsgruppe bzw. Organisationen in Bezug auf Version 0.3 vorgelegt und mit diesen telefonisch abgesprochen wurden: |



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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

***Tabelle 1: Dokumentenstatus***

| Fassung Datum | Verfasser | Dokumentteil | Änderungsbeschreibung |
|---|---|---|---|
| | | | • CER<br>• Niederländische Nationale Sicherheitsbehörde |
| | | Alle Abschnitte | Aktualisierung des Dokuments entsprechend der unterzeichneten Fassung der CSM-Empfehlung.<br>Aktualisierung des Dokuments entsprechend den Bemerkungen von Christophe CASSIR und Marcus ANDERSSON im Rahmen der Agentur-internen Prüfung |
| | | Alle Abschnitte Anhänge | Vollständige Neunummerierung der Absätze im Dokument ggü. Empfehlung<br>Einbeziehung von Anwendungsbeispielen der CSM-Empfehlung. |
| **Neuer Titel und neue Struktur des Dokuments: *„Sammlung von Beispielen für Risikobewertungen und möglicher Werkzeuge zur Unterstützung der CSM-Verordnung“*** | | | |
| Leitlinie Version 0.1 23/05/2008 | Dragan JOVICIC | Komplett | Erste Fassung des Dokuments nach Aufspaltung der „Gebrauchs-anleitung“ Version 0.5 in zwei ergänzende Dokumente. |
| Leitlinie Version 02 03/09/2008 | Dragan JOVICIC | Komplett | Aktualisierung des Dokuments gemäß:<br>• CSM-Verordnung der Europäischen Kommission {Ref. 3};<br>• Kommentare aus dem Workshop vom 1. Juli 2008 mit Mitgliedern des RISC (Ausschuss Interoperabilität und Sicherheit)<br>• Anmerkungen der CSM-Arbeitsgruppenmitglieder (der nationalen Sicherheitsbehörden Norwegens, Finnlands, des Vereinigten Königreichs und Frankreichs sowie von CER, EIM, Jens BRABAND [UNIFE] und Stéphane ROMEI [UNIFE]) |
| Leitlinie Version 1.0 10/12/2008 | Dragan JOVICIC | Komplett | Aktualisierung des Dokuments entsprechend der vom RISC auf seiner Plenartagung am 25. November 2008 angenommenen CSM-Verordnung der Europäischen Kommission für die Evaluierung und Bewertung der Risiken {Ref. 3} |
| Leitlinie Version 1.1 06/01/2009 | Dragan JOVICIC | Komplett | Aktualisierung des Dokuments entsprechend den von den Rechts- und Sprachabteilungen der Europäischen Kommission vorgebrachten Anmerkungen zur CSM-Verordnung. |



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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

# Inhaltsverzeichnis





European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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

## Abbildungen





European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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

## Tabellen





European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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. EINLEITUNG

## 0.1. Anwendungsbereich

0.1.1. Die vorliegende Leitlinie bezweckt weitergehende Klärungen zur „Verordnung der Kommission über die Festlegung einer gemeinsamen Sicherheitsmethode für die Evaluierung und Bewertung von Risiken gemäß Artikel 6 Absatz 3 Buchstabe a der Richtlinie 2004/49/EG des Europäischen Parlaments und des Rates“ {Ref. 3}. Die Verordnung wird im vorliegenden Dokument als „CSM-Verordnung“ bezeichnet.

0.1.2. Das vorliegende Dokument ist nicht rechtsverbindlich und sein Inhalt ist nicht als einzige Art und Weise zur Erreichung der CSM-Anforderungen zu interpretieren. Das vorliegende Dokument soll ergänzend zur Leitlinie zur Anwendung der CSM-Verordnung {Ref. 4} Aufschluss darüber geben, wie der Prozess der CSM-Verordnung eingesetzt und verwendet werden kann. Es gibt zusätzliche praktische Informationen, ohne jedoch zwingend zu befolgende Verfahrensweisen zu diktieren und ohne rechtsverbindliche Praktiken aufzustellen. Diese Informationen können für alle Akteure[(3)] von Nutzen sein, deren Aktivitäten sich potenziell auf die Sicherheit von Eisenbahnsystemen auswirken können und die die CSM-Verordnung unmittelbar oder mittelbar anwenden müssen. Das Dokument gibt Beispiele von Risikobewertungen und mögliche Werkzeuge zur Unterstützung der Anwendung der CSM. Diese Beispiele sollen ausschließlich Hinweise und Unterstützung geben. Akteure können für die Einhaltung der CSM alternative Methoden verwenden oder ihre bestehenden eigenen Methoden und Werkzeuge weiter verwenden, falls ihnen diese geeigneter erscheinen.
Die im vorliegenden Dokument enthaltenen Beispiele und Zusatzformationen beanspruchen keine Vollständigkeit und betreffen nicht alle möglichen Situationen, die im Rahmen geplanter signifikanter Änderungen auftreten können, so dass das Dokument nur als rein informativ angesehen werden kann.

0.1.3. Das vorliegende Informationsdokument ist ausschließlich als zusätzliche Hilfe für die Anwendung der CSM-Verordnung zu lesen. Soweit das vorliegende Dokument verwendet wird, sollte es in Zusammenhang mit der CSM-Verordnung {Ref. 3} und der damit verbundenen Leitlinie {Ref. 4} zur weiteren Vereinfachung der Anwendung der CSM gelesen werden, ersetzt jedoch nicht die CSM-Verordnung.

0.1.4. Das Dokument wird von der Europäischen Eisenbahnagentur (ERA) mit Unterstützung von Fachleuten des Eisenbahnverbands und nationaler Sicherheitsbehörden aus der CSM-Arbeitsgruppe erstellt. Es ist eine Sammlung von Ideen und Informationen, die die Agentur im Zuge interner Besprechungen sowie im Verlaufe von Besprechungen mit der CSM-Arbeitsgruppe und CSM-Taskforce zusammengetragen hat. Die ERA wird die Leitlinie bei Bedarf überprüfen und entsprechend den Fortschritten im Bereich der europäischen Normen, den Änderungen an der CSM-Verordnung für die Risikobewertung sowie dem eventuellen Erfahrungsrücklauf aus der Anwendung der CSM-Verordnung aktualisieren. Da zum Zeitpunkt der Erstellung ein genauer Terminplan für diesen Überprüfungsprozess nicht absehbar ist, sollte sich der Leser bei der Europäischen Eisenbahnagentur nach der letztgültigen Ausgabe des Dokumentes erkundigen.

---

(3) *Die betroffenen Akteure sind die Auftraggeber laut Definition in Artikel 2 Buchstabe r der Richtlinie 2008/57/EG über die Interoperabilität des Eisenbahnsystems in der Gemeinschaft oder die Hersteller, die in der Verordnung zusammenfassend als „Vorschlagender“ bezeichnet werden, oder deren Zulieferer und Dienstleister.*



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

## 0.2. Nicht im Anwendungsbereich

0.2.1. Das vorliegende Dokument gibt keine Anleitung, wie ein Eisenbahnsystem ganz oder in Teilen zu organisieren, zu betreiben oder zu planen (und herzustellen) ist. Ferner werden hier auch keine vertraglichen und sonstigen Vereinbarungen festgelegt, die zwischen Akteuren für die Anwendung des Risikomanagementverfahrens bestehen können. Die projektspezifischen Vertragsvereinbarungen liegen weder im Anwendungsbereich der CSM-Verordnung noch im Geltungsbereich des vorliegenden Dokumentes.

0.2.2. Die zwischen den entsprechenden Akteuren getroffenen Vereinbarungen gehören zwar nicht in den Anwendungsbereich des vorliegenden Dokumentes, können aber bei Projektbeginn in den entsprechenden Verträgen schriftlich festgehalten werden, ohne dass dadurch jedoch die Bestimmung der CSM berührt werden. Das könnte beispielsweise Folgendes betreffen:

(a) die anfallenden Kosten für die Verwaltung sicherheitsbezogener Risiken an den Schnittstellen;
(b) die anfallenden Kosten für bei Projektbeginn noch unbekannte Übertragungen von Gefährdungen und damit zusammenhängen Sicherheitsmaßnahmen zwischen den Akteuren;
(c) die Art und Weise der Verwaltung von im Projektverlauf eventuell entstehenden Konflikten;
(d) usw.

Sollte es im Verlaufe der Projektentwicklung zwischen dem Vorschlagenden und seinen Subunternehmern zu Meinungsverschiedenheiten oder zu einem Konflikt kommen, kann zur Unterstützung der Konfliktlösung auf die entsprechenden Verträge verwiesen werden.

## 0.3. Grundsatz für das vorliegende Dokument

0.3.1. Das vorliegende Dokument mag zwar als einzelnstehende Unterlage zur Lesehilfe erscheinen, es ersetzt jedoch nicht die CSM-Verordnung {Ref. 3}. Zur besseren Bezugnahme werden die einzelnen Artikel der CSM-Verordnung im vorliegenden Dokument zitiert. Soweit notwendig, wird der entsprechende Artikel in der Leitlinie zur Anwendung der CSM-Verordnung {Ref. 4} vorab erläutert. In den nachfolgenden Abschnitten werden dann zusätzliche Informationen gegeben, die ein besseres Verständnis der CSM-Verordnung fördern sollen, wann immer dies für notwendig erachtet wird.

*0.3.2. Die von der CSM Verordnung Artikeln und deren unterliegenden Absätze sind in der vorliegenden Leitlinie mit italischem Font „Bookman Old Style“ in einem Text Box kopiert. Dies erlaubt den originalen Text der CSM Verordnung {Ref. 3} von den in diesem Dokument bereitgestellten Erläuterungen leicht zu unterscheiden. Der Text aus der Leitlinie zur Anwendung der CSM Verordnung {Ref. 4} ist im vorliegenden Dokument nicht kopiert.*

0.3.3. Zur besseren Lesbarkeit ist das vorliegende Dokument entsprechend der CSM-Verordnung und der mit ihr verbundenen Leitlinie strukturiert.

## 0.4. Dokumentbeschreibung

0.4.1. Das Dokument gliedert sich in die folgenden Teile:



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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) Kapitel 0 bestimmt den Anwendungsbereich des Dokumentes und listet Verweisquellen auf;
(b) Anhang I und Anhang II geben zusätzliche Informationen über die entsprechenden Abschnitte der CSM-Verordnung {Ref. 3} und die mit ihr verbundene Leitlinie {Ref. 4};
(c) Neue Anlagen dienen der eingehenderen Diskussion besonderer Aspekte und geben Beispiele.

## 0.5. Quellenverweise

***Tabelle 2: Tabelle der Quellenverweise***

| {Ref. N°} | Titel | Verweisquelle | Fassung |
|---|---|---|---|
| {Ref. 1} | Richtlinie 2004/49/EG des Europäischen Parlaments und des Rates vom 29. April 2004 über Eisenbahnsicherheit in der Gemeinschaft und zur Änderung der Richtlinie 95/18/EG des Rates über die Erteilung von Genehmigungen an Eisenbahnunternehmen und der Richtlinie 2001/14/EG über die Zuweisung von Fahrwegkapazität der Eisenbahn, die Erhebung von Entgelten für die Nutzung von Eisenbahninfrastruktur und die Sicherheitsbescheinigung (Richtlinie über die Eisenbahnsicherheit) | 2004/49/EG ABl. L 164, 30.4.2004, S. 44, berichtigt durch ABl. L 220, 21.6.2004, S. 16. | - |
| {Ref. 2} | Richtlinie 2008/57/EG des Europäischen Parlaments und des Rates vom 17. Juni 2008 über die Interoperabilität des Eisenbahnsystems in der Gemeinschaft | 2008/57/EG ABl. L 191, 18.7.2008, S.1. | - |
| {Ref. 3} | Verordnung (EG) Nr. 352/2009. der Kommission vom 24 April 2009 über die Festlegung einer gemeinsamen Sicherheitsmethode für die Evaluierung und Bewertung von Risiken gemäß Artikel 6 Absatz 3 Buchstabe a der Richtlinie 2004/49/EG des Europäischen Parlaments und des Rates | EG 352/2009 | 24 April 2009 |
| {Ref. 4} | Leitlinie zur Anwendung der Verordnung über die Festlegung einer gemeinsamen Sicherheitsmethode für die Evaluierung und Bewertung von Risiken gemäß Artikel 6 Absatz 3 Buchstabe a der Eisenbahnsicherheitsrichtlinie | ERA/GUI/01-2008/SAF | 1.0 |
| {Ref. 5} | Richtlinie 2008/57/EG des Europäischen Parlaments und des Rates vom 17. Juni 2008 über die Interoperabilität des Eisenbahnsystems in der Gemeinschaft | 2008/57/EG ABl. L 191, 18.7.2008, S.1. | - |
| {Ref. 6} | Sicherheitsmanagementsystem – Bewertungskriterien für Eisenbahnunternehmen und Fahrwegbetreiber | SMS-Bewertungskriterien Teil A Sicherheits-bescheinigungen und Sicherheitsgenehmigungen | 31/05/2007 |
| {Ref. 7} | Bahnanwendungen - Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme - Sicherheitsrelevante elektronische Systeme für Signaltechnik | EN 50129 | Februar 2003 |
| {Ref. 8} | Bahnanwendungen - Spezifikation und Nachweis der Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit, Sicherheit (RAMS) – Teil 1: Die Norm selbst | EN 50126-1 | September 2006 |
| {Ref. 9} | Bahnanwendungen - Spezifikation und Nachweis der Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit, Sicherheit (RAMS) – Teil 2: Leitfaden zur Anwendung der EN 50126-1 für Sicherheit | EN 50126-2 (Leitfaden) | Endgültiger Entwurf (August 2006) |
| {Ref. 10} | Allgemeiner Leitfaden für die Berechnung von Risiken durch die Eisenbahnbeförderung gefährlicher Güter | OTIF-Leitfaden, genehmigt durch den RID-Fachausschuss | 24. November 2005 |
| {Ref. 11} | Risikoakzeptanzkriterium für technische Systeme | Note 01/08 | 1.1 (25/01/2008) |



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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

***Tabelle 2: Tabelle der Quellenverweise***

| {Ref. N°} | Titel | Verweisquelle | Fassung |
|---|---|---|---|
| {Ref. 12} | ERA Sicherheitsreferat: Machbarkeitsstudie – „Zuweisung von Sicherheitszielen (zu TSI-Teilsystemen) und Konsolidierung von TSI aus dem Blickwinkel der Sicherheit“ WP1.1 - Bewertung der Machbarkeit der Aufteilung gemeinsamer Sicherheitsziele | WP1.1 | 1.0 |
| {Ref. 13} | „Bahnanwendungen – Kennzeichnungssystematik für Schienenfahrzeuge – Teil 4: EN 0015380 Teil 4: Funktionsgruppen“. | EN 0015380 Teil 4 | |

## 0.6. Allgemeine Definitionen, Begriffe und Abkürzungen

0.6.1. Die im vorliegenden Dokument verwendeten allgemeinen Definitionen, Begriffe und Abkürzungen sind in einem Standardwörterbuch auffindbar.

0.6.2. Neue Definitionen, Begriffe und Abkürzungen in der vorliegenden Leitlinie werden in den nachstehenden Abschnitten bestimmt.

## 0.7. Besondere Definitionen

0.7.1. Siehe Artikel 3

## 0.8. Besondere Begriffe und Abkürzungen

0.8.1. Dieser Abschnitt enthält die Begriffsbestimmungen der im vorliegenden Dokument häufig vorkommenden neuen Begriffe und Abkürzungen.

***Tabelle 3: Tabelle der Begriffe***

| Begriff | Definition |
|---|---|
| Agentur | die Europäische Eisenbahnagentur (ERA – European Railway Agency) |
| Leitlinie | die „Leitlinie für die Anwendung der Verordnung (EG) Nr.352/2009 der Kommission vom 24 April 2009 über die Festlegung einer gemeinsamen Sicherheitsmethode für die Evaluierung und Bewertung von Risiken gemäß Artikel 6 Absatz 3 Buchstabe a der Richtlinie 2004/49/EG des Europäischen Parlaments und des Rates“ |
| CSM-Verordnung | die „Verordnung (EG) Nr. 352/2009 der Kommission vom 24 April 2009 über die Einführung einer gemeinsamen Sicherheitsmethode für die Evaluierung und Bewertung von Risiken gemäß Artikel 6 Absatz 3 Buchstabe a der Richtlinie 2004/49/EG des Europäischen Parlaments und des Rates“ {Ref. 3} |

***Tabelle 4: Tabelle der Abkürzungen***

| Abkürzung | Bedeutung |
|---|---|
| BEST | Benannte Stelle |
| CSM | Gemeinsame Sicherheitsmethode(n) |
| CST | Gemeinsame Sicherheitsziele |
| EBU | Eisenbahnunternehmen |


European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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

### *Tabelle 4: Tabelle der Abkürzungen*

| Abkürzung | Bedeutung |
|---|---|
| EC | Europäische Kommission |
| ERA | Europäische Eisenbahnagentur |
| FB | Fahrwegbetreiber |
| MS | Mitgliedstaat |
| NSA | Nationale Sicherheitsbehörde |
| OTIF | Zwischenstaatliche Organisation für den internationalen Eisenbahnverkehr |
| QMP | Qualitätsmanagementprozess |
| QMS | Qualitätsmanagementsystem |
| RISC | Ausschuss Interoperabilität und Eisenbahnsicherheit |
| SMP | Sicherheitsmanagementprozess |
| SMS | Sicherheitsmanagementsystem |
| SRT | Sicherheit im Eisenbahntunnel |
| TBC | To be completed |
| TSI | Technische Spezifikationen für die Interoperabilität |
| USB | Unabhängiger Sicherheitsbegutachter |
| ZZS | Zugsteuerung, Zugsicherung und Signalgebung |



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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

# Erläuterung der Artikel der CSM-Verordnung

## Artikel 1. Zweck

### Artikel 1 (1)

*Diese Verordnung legt eine gemeinsame Sicherheitsmethode (CSM) für die Evaluierung und Bewertung von Risiken gemäß Artikel 6 Absatz 3 Buchstabe a der Richtlinie 2004/49/EG fest.*

[G 1] Eine zusätzliche Erläuterung erscheint nicht notwendig.

### Artikel 1 (2)

*Zweck der CSM für die Evaluierung und Bewertung von Risiken ist es, das Sicherheitsniveau im Schienenverkehr in der Gemeinschaft aufrechtzuerhalten oder – soweit erforderlich und nach vernünftigem Ermessen durchführbar – zu verbessern. Die CSM erleichtert den Zugang zum Markt für Schienenverkehrsdienste durch eine Harmonisierung:*

*(a) der Risikomanagementverfahren, die zur Bewertung der Sicherheitsniveaus und der Erfüllung der Sicherheitsanforderungen angewandt werden;*

*(b) des Austauschs sicherheitsrelevanter Informationen zwischen den verschiedenen Akteuren des Eisenbahnsektors mit dem Ziel, ein Sicherheitsmanagement über die innerhalb des Sektors bestehenden verschiedenen Schnittstellen hinweg zu gewährleisten;*

*(c) der aus der Anwendung eines Risikomanagementverfahrens resultierenden Ergebnisse.*

[G 1] Eine zusätzliche Erläuterung erscheint nicht notwendig.

## Artikel 2. Anwendungsbereich

### Artikel 2 (1)

*Die CSM für die Evaluierung und Bewertung von Risiken gilt für alle in einem Mitgliedstaat vorgenommenen Änderungen des Eisenbahnsystems im Sinne von Anhang III Ziffer 2 Buchstabe d der Richtlinie 2004/49/EG, die im Sinne von Artikel 4 dieser Verordnung für signifikant erachtet werden. Diese Änderungen können technischer, betrieblicher oder organisatorischer Art sein. Im Falle organisatorischer Änderungen sind nur solche Änderungen zu berücksichtigen, die sich auf die Betriebsbedingungen auswirken können.*

[G 1] Die CSM gilt für das gesamte Eisenbahnsystem und betrifft die Bewertung der folgenden Änderungen in Eisenbahnsystemen, wenn diese durch Anwendung von Artikel 4 als signifikant eingeschätzt werden:

(a) Errichtung neuer Strecken oder Änderungen bestehender Strecken,
(b) Einführung neuer und/oder modifizierter technischer Systeme;
(c) betriebliche Änderungen (wie neue oder modifizierte Betriebsvorschriften und Instandhaltungsverfahren);



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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) organisatorische Änderungen innerhalb der EBU/FB.

Der Begriff „System“ bezieht sich in der CSM auf alle Aspekte eines Systems, darin inbegriffen unter anderem auch dessen Entwicklung, Betrieb, Instandhaltung usw., bis zur Stilllegung bzw. Entsorgung.

[G 2] Die CSM behandelt die signifikanten Änderungen von:

(a) „kleinen und einfachen“ Systemen, die aus wenigen technischen Teilsystemen oder Elementen bestehen können, und
(b) „großen und komplexeren“ Systemen (z. B. mit Bahnhöfen und Tunneln).

## Artikel 2 (2)

*Betreffen die signifikanten Änderungen strukturelle Teilsysteme, die der Richtlinie 2008/57/EG unterliegen, findet die CSM für die Risikoevaluierung und bewertung Anwendung:*

*(a) wenn die relevanten technischen Spezifikationen für die Interoperabilität (TSI) eine Risikobewertung verlangen; in diesem Fall ist in der betreffenden TSI gegebenenfalls anzugeben, welche Teile der CSM Anwendung finden;*

*(b) damit im Einklang mit Artikel 15 Absatz 1 der Richtlinie 2008/57/EG eine sichere Integration der strukturellen Teilsysteme, für die die TSI gelten, in ein bestehendes System gewährleistet werden kann.*

*Im in Unterabsatz 1 Buchstabe b genannten Fall darf die Anwendung der CSM jedoch nicht dazu führen, dass Anforderungen gestellt werden, die den verbindlichen Anforderungen der relevanten TSI widersprechen.*

*Erwächst dennoch aus der Anwendung der CSM eine Anforderung, die den verbindlichen Anforderungen der relevanten TSI widerspricht, informiert der Vorschlagende die betroffenen Mitgliedstaaten, die in diesem Fall beschließen können, eine Überarbeitung der TSI gemäß Artikel 6 Absatz 2 oder Artikel 7 der Richtlinie 2008/57/EG oder eine Ausnahme gemäß Artikel 9 dieser Richtlinie zu beantragen.*

[G 1] Beispielsweise muss gemäß der Eisenbahnsicherheitsrichtlinie {Ref. 1} und der Richtlinie über die Interoperabilität {Ref. 2} ein neuer Fahrzeugtyp für eine Hochgeschwindigkeitsstrecke mit der TSI Hochgeschwindigkeitsfahrzeuge übereinstimmen. Obwohl die meisten zu bewertenden Systeme von der TSI erfasst werden, ist die Kernfrage der Humanfaktoren in Bezug auf den Führerstand nicht in der TSI enthalten. Um sicherzustellen, dass alle nach vernünftigem Ermessen vorhersehbaren Gefährdungen in Bezug auf Humanfaktoren (d. h. Schnittstellen zwischen dem Triebfahrzeugführer, dem Fahrzeug und dem restlichen Eisenbahnsystem) ermittelt und angemessen kontrolliert werden, ist somit der CSM-Prozess zu verwenden.



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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

## Artikel 2 (3)

*Diese Verordnung gilt nicht für:*

*(a) Untergrundbahnen, Straßenbahnen und andere Stadt- und Regionalbahnen;*

*(b) Netze, die vom übrigen Eisenbahnsystem funktional getrennt sind und nur für die Personenbeförderung im örtlichen Verkehr, Stadt- oder Vorortverkehr genutzt werden, sowie Eisenbahnunternehmen, die ausschließlich derartige Netze nutzen;*

*(c) Eisenbahninfrastrukturen in Privateigentum, die vom Eigentümer der Infrastruktur ausschließlich zur Nutzung für den eigenen Güterverkehr unterhalten werden;*

*(d) historische Fahrzeuge, die in nationalen Netzen eingesetzt werden, sofern diese Fahrzeuge den nationalen Sicherheitsvorschriften entsprechen, so dass ihr sicherer Betrieb gewährleistet ist;*

*(e) historische Züge, Museumszüge und Touristenzüge, die auf einem eigenen Schienennetz betrieben werden, einschließlich Werkstätten, Fahrzeugen und Personal.*

[G 1] Eine zusätzliche Erläuterung erscheint nicht notwendig.

## Artikel 2 (4)

*Diese Verordnung gilt nicht für Systeme und Änderungen, die zum Zeitpunkt des Inkrafttretens dieser Verordnung Vorhaben in fortgeschrittenem Entwicklungsstadium im Sinne von Artikel 2 Buchstabe t der Richtlinie 2008/57/EG sind.*

[G 1] Eine zusätzliche Erläuterung erscheint nicht notwendig.

## Artikel 3. Begriffsbestimmungen

*Für die Zwecke dieser Verordnung gelten die Begriffsbestimmungen von Artikel 3 der Richtlinie 2004/49/EG.*

*Darüber hinaus bezeichnet der Ausdruck:*

*(1) „Risiko“: die Kombination der Wahrscheinlichkeit des Eintretens von (durch Gefährdungen verursachten) Unfällen und Zwischenfällen, die zu einem Schaden führen, und des Ausmaßes dieses Schadens* (EN 50126-2)*;*

*(2) „Risikoanalyse“: die systematische Auswertung aller verfügbaren Informationen zur Identifizierung von Gefährdungen und Abschätzung von Risiken* (ISO/IEC 73)*;*

*(3) „Risikoevaluierung“: das auf der Risikoanalyse beruhendes Verfahren zur Feststellung, ob das Risiko auf ein vertretbares Niveau gesenkt wurde* (ISO/IEC 73)*;*

*(4) „Risikobewertung“: den aus Risikoanalyse und Risikoevaluierung bestehender Gesamtprozess* (ISO/IEC 73)*;*

*(5) „Sicherheit“: die Abwesenheit von unvertretbaren Schadensrisiken* (EN 50126-1)*;*

*(6) „Risikomanagement“: die systematische Anwendung von Managementstrategien, verfahren und praktiken bei der Analyse, Evaluierung und Kontrolle von Risiken* (ISO/IEC 73)*;*

*(7) „Schnittstellen“: alle Interaktionspunkte innerhalb des Lebenszyklus eines Systems oder Teilsystems, einschließlich Betrieb und Instandhaltung, an denen die verschiedenen Akteure des Eisenbahnsektors im Rahmen des Risikomanagements zusammenarbeiten;*

*(8) „Akteure“: alle Parteien, die gemäß Artikel 5 Absatz 2 direkt oder aufgrund vertraglicher Vereinbarungen in die Anwendung dieser Verordnung einbezogen sind;*



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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

*(9) „Sicherheitsanforderungen“: die (qualitativen oder quantitativen) Sicherheitsmerkmale eines Systems und dessen Betriebs (einschließlich Betriebsvorschriften), die zur Erfüllung gesetzlicher oder unternehmensspezifischer Sicherheitsziele erforderlich sind;*

*(10) „Sicherheitsmaßnahmen“: eine Reihe von Maßnahmen, die entweder die Häufigkeit des Auftretens einer Gefährdung verringert oder ihre Folgen mildert, so dass ein vertretbares Risikoniveau erreicht und/oder aufrechterhalten werden kann;*

*(11) „Vorschlagender“: die Eisenbahnunternehmen oder Infrastrukturbetreiber im Rahmen der Risikokontrollmaßnahmen, die sie nach Artikel 4 der Richtlinie 2004/49/EG zu treffen haben, die Auftraggeber oder Hersteller, die gemäß Artikel 18 Absatz 1 der Richtlinie 2008/57/EG bei einer benannten Stelle das EG-Prüfverfahren durchführen lassen, oder die Antragsteller, die eine Genehmigung für die Inbetriebnahme von Fahrzeugen beantragen;*

*(12) „Sicherheitsbewertungsbericht“: das Dokument, das die Schlussfolgerungen der von einer Bewertungsstelle vorgenommenen Bewertung des zu bewertenden Systems enthält;*

*(13) „Gefährdung“: den Umstand, der zu einem Unfall führen könnte* (EN 50126-2)*;*

*(14) „Bewertungsstelle“: die unabhängige, fachkundige Person, Organisation oder Stelle, die eine Untersuchung vornimmt, um auf der Grundlage von Nachweisen zu beurteilen, ob ein System die gestellten Sicherheitsanforderungen erfüllt;*

*(15) „Risikoakzeptanzkriterien“: die Bezugskriterien, anhand deren die Vertretbarkeit eines spezifischen Risikos bewertet wird; diese Kriterien werden herangezogen, um zu bestimmen, ob das Risiko so gering ist, dass keine Sofortmaßnahmen zu seiner weiteren Eindämmung erforderlich sind;*

*(16) „Gefährdungsprotokoll“: die Unterlage, in der erkannte Gefährdungen, die damit zusammenhängenden Maßnahmen und die Ursache der Gefährdungen dokumentiert und Angaben zu der für das Gefährdungsmanagement verantwortlichen Organisation gemacht werden;*

*(17) „Gefährdungsermittlung“: das Verfahren zur Ermittlung, Auflistung und Charakterisierung von Gefährdungen* (ISO/IEC Guide 73)*;*

*(18) „Grundsatz der Risikoakzeptanz“: die Regeln, anhand deren festgestellt wird, ob das mit einer oder mehreren spezifischen Gefährdungen verbundene Risiko vertretbar ist;*

*(19) „anerkannte Regeln der Technik“: die schriftlich festgelegte Regeln, die bei ordnungsgemäßer Anwendung dazu dienen können, eine oder mehrere spezifische Gefährdungen zu kontrollieren;*

*(20) „Referenzsystem“: ein System, das sich in der Praxis bewährt hat, ein akzeptables Sicherheitsniveau gewährleistet und es ermöglicht, im Wege eines Vergleichs die Vertretbarkeit der von einem zu bewertenden System ausgehenden Risiken zu evaluieren;*

*(21) „Risikoabschätzung“: das Verfahren, das der Festlegung eines Maßstabs zur Bestimmung der analysierten Risiken dient und aus folgenden Schritten besteht: Abschätzung der Häufigkeit, Konsequenzanalyse und Integration* (ISO/IEC 73)*;*

*(22) „technisches System“: das Bauteil oder die Baugruppe, einschließlich Planung, Realisierung und Begleitdokumentation; die Entwicklung eines technischen Systems beginnt mit der Festlegung der Anforderungen an das System und endet mit seiner Zulassung; auch wenn dabei die relevanten Schnittstellen zum menschlichen Verhalten berücksichtigt werden, sind das Personal und dessen Handlungen nicht Bestandteil eines technischen Systems; der Wartungsprozess wird in den Wartungshandbüchern beschrieben, ist aber selbst nicht Bestandteil des technischen Systems;*

*(23) „katastrophale Folge“: Todesfälle und/oder zahlreiche schwere Verletzungen und/oder schwerwiegende Umweltschäden infolge eines Unfalls* (Table 3 from EN 50126)*;*

*(24) „bescheinigte Sicherheit“: den Status, der einer Änderung durch den Vorschlagenden auf der Grundlage des von der Bewertungsstelle vorgelegten Sicherheitsbewertungsberichts zuerkannt wird;*

*(25) „System“: jeden Teil des Eisenbahnsystems, der Gegenstand einer Änderung ist;*



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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

*(26) „notifizierte nationale Vorschrift“: jede nationale Vorschrift, die von Mitgliedstaaten auf der Grundlage der Richtlinie 96/48/EG des Rates , der Richtlinie 2001/16/EG des Europäischen Parlaments und des Rates , und der Richtlinien 2004/49/EG und 2008/57/EG notifiziert wurde.*

[G 1] Eine zusätzliche Erläuterung erscheint nicht notwendig.

## Artikel 4. Signifikante Änderungen

### Artikel 4 (1)

*Wurde keine nationale Vorschrift notifiziert, anhand deren bestimmt werden kann, ob eine Änderung in einem Mitgliedstaat signifikant ist oder nicht, prüft der Vorschlagende die potenziellen Auswirkungen der betreffenden Änderung auf die Sicherheit des Eisenbahnsystems.*

*Hat die vorgeschlagene Änderung keinerlei Auswirkungen auf die Sicherheit, kann auf die Anwendung des in Artikel 5 beschriebenen Risikomanagementverfahrens verzichtet werden.*

[G 1] Wenn es keine notifizierte nationale Vorschrift gibt, liegt die Entscheidung in der Verantwortung des Vorschlagenden. Die Signifikanz der Änderung beruht auf einem Fachurteil. Wenn beispielsweise an einem bestehenden System eine komplexe Änderung geplant ist, kann diese als signifikant beurteilt werden, wenn das Risiko einer Auswirkung auf die bestehenden Funktionen[4] des Systems hoch ist, auch wenn es sich bei der Änderung an sich nicht zwangsläufig um eine hoch sicherheitsrelevante Änderung handelt.

### Artikel 4 (2)

*Hat die vorgeschlagene Änderung Auswirkungen auf die Sicherheit, entscheidet der Vorschlagende auf der Grundlage eines Sachverständigenurteils über die Signifikanz der Änderung, wobei er folgende Kriterien berücksichtigt:*

*(a) Folgen von Ausfällen: Szenario des schlechtesten anzunehmenden Falls („credible worst-case scenario“) bei einem Ausfall des zu bewertenden Systems unter Berücksichtigung etwaiger außerhalb des Systems bestehender Sicherheitsvorkehrungen;*

*(b) innovative Elemente in der Implementierung der Änderung; dabei geht es nicht nur darum, ob es sich um eine Innovation für den Eisenbahnsektor als Ganzes handelt, sondern auch darum, ob es sich aus der Sicht der Organisation, die die Änderung einführt, um eine Innovation handelt;*

*(c) Komplexität der Änderung;*

*(d) Überwachung: Unmöglichkeit, die eingeführte Änderung über den gesamten Lebenszyklus des Systems hinweg zu überwachen und in geeigneter Weise einzugreifen;*

*(e) Umkehrbarkeit: Unmöglichkeit, zu dem vor Einführung der Änderung bestehenden System zurückzukehren;*

---

*(4) Da die Funktionen in einem System nicht immer unabhängig sind, können Änderungen bestimmter Funktionen sich auch auf andere Funktionen des Systems auswirken, die selbst nicht unmittelbar von den Änderungen betroffen scheinen.*



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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

*(f) additive Wirkung: Bewertung der Signifikanz der Änderung unter Berücksichtigung aller sicherheitsrelevanten Änderungen des zu bewertenden Systems, die in jüngster Zeit vorgenommen und nicht als signifikant beurteilt wurden.*

*Der Vorschlagende bewahrt zweckdienliche Unterlagen auf, die es ihm ermöglichen, die Gründe für seine Entscheidung zu dokumentieren.*

[G 1] **Beispiel für kleine Änderungen:** Die einmalige Erhöhung der Streckenhöchstgeschwindigkeit um 5 km/h nach der Inbetriebsetzung könnte eine nicht signifikante Änderung sein. Wenn jedoch die Streckenhöchstgeschwindigkeit in mehreren Stufen jeweils um weitere 5 km/h erhöht wird, könnten die aufeinanderfolgenden Änderungen (die jeweils für sich nichtsignifikante Änderungen sind) in der Summe eine signifikante Änderung gegenüber den anfänglichen Sicherheitsanforderungen des Systems sein.

[G 2] Um zu beurteilen, ob eine Reihe mehrerer aufeinanderfolgender (nicht signifikanter) Änderungen zusammengenommen signifikant sind, müssen alle Gefährdungen und damit verbundenen Risiken im Zusammenhang mit den Änderungen bewertet werden. Die Reihe der betrachteten Änderungen kann für nicht signifikant erachtet werden, wenn sie zu einem weitgehend akzeptablen Risiko führt.

[G 3] Die Agentur hat sich mit signifikanten Änderungen befasst und ist zu folgendem Schluss gekommen:

(a) Es lassen sich keine einheitlichen Grenzen oder Regeln feststellen, anhand derer bei Vorliegen einer Änderung eine Entscheidung über die Signifikanz der Änderung getroffen werden kann und

(b) es ist nicht möglich, eine allumfassende Liste signifikanter Änderungen zu erstellen;

(c) die Entscheidung kann keine Gültigkeit für alle Vorschlagenden und alle technischen, betrieblichen, organisatorischen und Umgebungsbedingungen beanspruchen.

Es ist somit wesentlich, dass die Verantwortung für die Entscheidung bei den Vorschlagenden verbleibt, die gemäß Artikel 4 Absatz 3 der Eisenbahnsicherheitsrichtlinie {Ref. 1} für den sicheren Betrieb und die Kontrolle der mit ihrem Systemanteil verbundenen Risiken verantwortlich sind.

[G 4] Als Hilfestellung für den Vorschlagenden wird in Abschnitt C.2 von Alage C ein Beispiel für die „Bewertung und Verwendung von Kriterien“ gegeben.

[G 5] Die CSM muss nicht angewendet werden, wenn eine sicherheitsbezogene Änderung für nicht signifikant eingeschätzt wird. Das bedeutet jedoch nicht, dass hier nichts zu tun ist. Um über die Signifikanz der Änderung zu entscheiden, führt der Vorschlagende bestimmte (vorläufige) Risikoanalysen durch. Diese Risikoanalysen nebst Begründungen und Argumenten sind zu dokumentieren, so dass Audits der nationalen Sicherheitsbehörde (NSA) ermöglicht werden. Die Beurteilung der Signifikanz einer Änderung und die Entscheidung, dass eine Änderung nicht signifikant ist, bedarf keiner unabhängigen Bewertung durch eine Bewertungsstelle.



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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

# Artikel 5. Risikomanagementverfahren

## Artikel 5 (1)

*Das in Anhang I beschriebene Risikomanagementverfahren findet Anwendung:*

*(a) bei signifikanten Änderungen im Sinne des Artikels 4, einschließlich im Falle der Inbetriebnahme struktureller Teilsysteme im Sinne des Artikels 2 Absatz 2 Buchstabe b;*

*(b) in dem in Artikel 2 Absatz 2 Buchstabe a genannten Fall, wenn eine TSI unter Bezugnahme auf diese Verordnung die Anwendung des in Anhang I beschriebenen Risikomanagementverfahrens vorschreibt.*

[G 1] Eine zusätzliche Erläuterung erscheint nicht notwendig.

## Artikel 5 (2)

*Das in Anhang I beschriebene Risikomanagementverfahren wird vom Vorschlagenden angewandt.*

[G 1] Eine zusätzliche Erläuterung erscheint nicht notwendig.

## Artikel 5 (3)

*Der Vorschlagende gewährleistet das Management der von Zulieferern und Dienstleistern, einschließlich ihrer Subunternehmer, ausgehenden Risiken. Zu diesem Zweck kann er verlangen, dass Zulieferer und Dienstleister, einschließlich ihrer Subunternehmer, an dem in Anhang I beschriebenen Risikomanagementverfahren mitwirken.*

[G 1] Eine zusätzliche Erläuterung erscheint nicht notwendig.

# Artikel 6. Unabhängige Bewertung

## Artikel 6 (1)

*Die ordnungsgemäße Anwendung des in Anhang I beschriebenen Risikomanagementverfahrens und die Ergebnisse dieser Anwendung werden von einer Stelle, die den in Anhang II genannten Kriterien entspricht, einer unabhängigen Bewertung unterzogen. Soweit die zuständige Bewertungsstelle noch nicht in gemeinschaftlichen oder nationalen Rechtsvorschriften festgelegt ist, benennt der Vorschlagende selbst eine Bewertungsstelle, bei der es sich um eine andere Organisation oder auch um eine interne Abteilung handeln kann.*

[G 1] Der für die Bewertungsstelle notwendige Grad der Unabhängigkeit hängt davon ab, welches Sicherheitsniveau für das zu bewertende System erforderlich ist. Bis zur Harmonisierung dieser Thematik findet sich die beste diesbezügliche Praxis in IEC61508-1:2001 Abschnitt 8 oder in § 5.3.9 der Norm EN 50 129 {Ref. 7}. Der Unabhängigkeitsgrad ist sowohl von der Folgenschwere der mit der Ausrüstung verbundenen Gefährdung als auch vom Neuheitsgrad der Ausrüstung abhängig. In Abschnitt § 9.7.2 von EN 50 126-2 und in EN 50129 ist der Unabhängigkeitsgrad für Signalanlagen festgelegt. Dies könnte grundsätzlich so auch für andere Anlagen und Systeme übernommen werden.



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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] Die Agentur arbeitet nach wie vor an der Festlegung, welche Rollen und Verantwortlichkeiten den unterschiedlichen Bewertungsstellen zukommen (NSA, BEST und USB) und welche Schnittstellen zwischen ihnen notwendig sind. Damit wird (soweit möglich) festgelegt, welche dieser Bewertungsstellen welche Aufgaben auf welche Weise ausführt. Damit wird letztendlich auch festgelegt werden können:

(a) wie anhand von Nachweisen geprüft wird, dass die von der CSM behandelten Risikomanagement- und Risikobewertungsverfahren sachgerecht angewendet werden und

(b) wie der Vorschlagende in seiner Entscheidung über die Akzeptanz der signifikanten Änderung im zu bewertenden System unterstützt wird.

## Artikel 6 (2)

*Doppelarbeit zwischen der gemäß Richtlinie 2004/49/EG erforderlichen Konformitätsbewertung des Sicherheitsmanagementsystems, der gemäß Richtlinie 2008/57/EG durchgeführten Konformitätsbewertung durch eine benannte oder eine nationale Stelle und einer gemäß dieser Verordnung von der Bewertungsstelle durchgeführten unabhängigen Sicherheitsbewertung gilt es zu vermeiden.*

[G 1] Die weitere Arbeit der Agentur zu den Rollen und Verantwortlichkeiten der Bewertungsstellen wird zusätzliche Informationen hervorbringen.

## Artikel 6 (3)

*In folgenden Fällen signifikanter Änderungen kann die Sicherheitsbehörde als Bewertungsstelle agieren:*

*(a) wenn für die Inbetriebnahme eines Fahrzeugs gemäß Artikel 22 Absatz 2 und Artikel 24 Absatz 2 der Richtlinie 2008/57/EG eine Genehmigung erforderlich ist;*

*(b) wenn für die Inbetriebnahme eines Fahrzeugs gemäß Artikel 23 Absatz 5 und Artikel 25 Absatz 4 der Richtlinie 2008/57/EG eine zusätzliche Genehmigung erforderlich ist;*

*(c) wenn aufgrund einer Änderung der Art oder des Umfangs des Betriebs gemäß Artikel 10 Absatz 5 der Richtlinie 2004/49/EG die Sicherheitsbescheinigung aktualisiert werden muss;*

*(d) wenn aufgrund wesentlicher Änderungen des rechtlichen Rahmens im Bereich der Sicherheit gemäß Artikel 10 Absatz 5 der Richtlinie 2004/49/EG die Sicherheitsbescheinigung überprüft werden muss;*

*(e) wenn aufgrund wesentlicher Änderungen der Infrastruktur, der Signalgebung oder der Energieversorgung oder der Grundsätze für ihren Betrieb und ihre Instandhaltung gemäß Artikel 11 Absatz 2 der Richtlinie 2004/49/EG die Sicherheitsgenehmigung aktualisiert werden muss;*

*(f) wenn aufgrund wesentlicher Änderungen des rechtlichen Rahmens im Bereich der Sicherheit gemäß Artikel 11 Absatz 2 der Richtlinie 2004/49/EG die Sicherheitsgenehmigung überprüft werden muss.*

[G 1] Eine zusätzliche Erläuterung erscheint nicht notwendig.



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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

### Artikel 6 (4)

*Betrifft eine signifikante Änderung ein strukturelles Teilsystem, für dessen Inbetriebnahme eine Genehmigung gemäß Artikel 15 Absatz 1 oder Artikel 20 der Richtlinie 2008/57/EG erforderlich ist, kann die Sicherheitsbehörde als Bewertungsstelle agieren, sofern der Vorschlagende diese Aufgabe nicht bereits einer gemäß Artikel 18 Absatz 2 der Richtlinie 2008/57/EG benannten Stelle übertragen hat.*

[G 1] Eine zusätzliche Erläuterung erscheint nicht notwendig.

## Artikel 7. Sicherheitsbewertungsberichte

### Artikel 7 (1)

*Die Bewertungsstelle unterbreitet dem Vorschlagenden einen Sicherheitsbewertungsbericht.*

[G 1] Eine zusätzliche Erläuterung erscheint nicht notwendig.

### Artikel 7 (2)

*In dem in Artikel 5 Absatz 1 Buchstabe a genannten Fall wird der Sicherheitsbewertungsbericht von der nationalen Sicherheitsbehörde bei ihrer Entscheidung über die Genehmigung der Inbetriebnahme von Teilsystemen und Fahrzeugen berücksichtigt.*

[G 1] Eine zusätzliche Erläuterung erscheint nicht notwendig.

### Artikel 7 (3)

*In dem in Artikel 5 Absatz 1 Buchstabe b genannten Fall gehört die unabhängige Bewertung zu den Aufgaben der benannten Stelle, sofern die TSI nichts anderes vorschreibt.*
*Wenn die unabhängige Bewertung nicht zu den Aufgaben der benannten Stelle gehört, wird der Sicherheitsbewertungsbericht von der benannten Stelle, die für die Ausstellung der Konformitätsbescheinigung verantwortlich ist, oder vom Auftraggeber, der für die Ausstellung der EG-Prüferklärung zuständig ist, berücksichtigt.*

[G 1] Eine zusätzliche Erläuterung erscheint nicht notwendig.

### Artikel 7 (4)

*Wurde ein System oder Teilsystem bereits in Anwendung des in dieser Verordnung festgelegten Risikomanagementverfahrens zugelassen, kann der daraus resultierende Sicherheitsbewertungsbericht nicht von einer anderen Bewertungsstelle, die mit einer erneuten Bewertung desselben Systems beauftragt ist, in Frage gestellt werden. Voraussetzung für die Anerkennung ist der Nachweis, dass das System unter denselben funktionalen, betrieblichen und Umweltbedingungen wie das bereits zugelassene System eingesetzt wird und dass gleichwertige Risikoakzeptanzkriterien angelegt werden.*



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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] Dieser Grundsatz der gegenseitigen Anerkennung wird bereits von den CENELEC-Normen zugelassen: Siehe Abschnitt § 5.5.2 in EN 50 129 und Abschnitt § 5.9 in EN 50 126-2. In CENELEC wird der Grundsatz der länderübergreifenden gegenseitigen Anerkennung von Vorschlagenden oder unabhängigen Sicherheitsbegutachtern auf generische Produkte und generische Anwendungen(5) angewendet, vorausgesetzt, dass die Sicherheitsbewertung und der Sicherheitsnachweis in Übereinstimmung mit den CENELEC-Normanforderungen durchgeführt werden.

[G 2] Die gegenseitige Anerkennung muss auch für die Zulassung neuer oder modifizierter Systeme angewendet werden, wenn deren Risikobewertung und der Nachweis der Übereinstimmung des Systems mit den Sicherheitsanforderungen entsprechend den Bestimmungen der CSM-Verordnung {Ref. 3} durchgeführt werden.

## Artikel 8. Risikokontrolle / interne und externe Prüfungen

### Artikel 8 (1)

*Die Eisenbahnunternehmen und Infrastrukturbetreiber sehen im Rahmen der regelmäßigen Überprüfung des gemäß Artikel 9 der Richtlinie 2004/49/EG einzuführenden Sicherheitsmanagementsystems eine Überprüfung der Anwendung der CSM für die Risikoevaluierung und –bewertung vor.*

[G 1] Eine zusätzliche Erläuterung erscheint nicht notwendig.

### Artikel 8 (2)

*Im Rahmen der ihr durch Artikel 16 Absatz 2 Buchstabe e der Richtlinie 2004/49/EG übertragenen Aufgaben überwacht die zuständige nationale Sicherheitsbehörde die Anwendung der CSM für die Risikoevaluierung und –bewertung.*

[G 1] Eine zusätzliche Erläuterung erscheint nicht notwendig.

## Artikel 9. Rückmeldungen und technischer Fortschritt

### Artikel 9 (1)

*Jeder Infrastrukturbetreiber und jedes Eisenbahnunternehmen berichtet in seinem gemäß Artikel 9 Absatz 4 der Richtlinie 2004/49/EG vorzulegenden jährlichen Sicherheitsbericht kurz über seine Erfahrungen mit der Anwendung der CSM für die Risikoevaluierung und –bewertung. Darüber hinaus enthält der Bericht eine zusammenfassende Darstellung der Entscheidungen bezüglich der Signifikanz der Änderungen.*

[G 1] Eine zusätzliche Erläuterung erscheint nicht notwendig.

(5) *Siehe Punkt [G 5] in Abschnitt 1.1.5 und die Fußnoten (9) und (10) auf Seite 30 sowie Abbildung 3 dieses Dokumentes für weitere Erläuterungen zur Terminologie „generisches Produkt und generische Anwendung“ und für die zugrunde liegenden Grundsätze.*



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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

### Artikel 9 (2)

*Jede nationale Sicherheitsbehörde berichtet in ihrem gemäß Artikel 18 der Richtlinie 2004/49/EG vorzulegenden jährlichen Sicherheitsbericht über die Erfahrungen der Vorschlagenden mit der Anwendung der CSM für die Risikoevaluierung und -bewertung sowie gegebenenfalls über ihre eigenen Erfahrungen.*

[G 1] Eine zusätzliche Erläuterung erscheint nicht notwendig.

### Artikel 9 (3)

*Die Europäische Eisenbahnagentur überwacht die Anwendung der CSM für die Risikoevaluierung und -bewertung, nimmt Rückmeldungen entgegen und richtet gegebenenfalls Empfehlungen für Verbesserungen an die Kommission.*

[G 1] Eine zusätzliche Erläuterung erscheint nicht notwendig.

### Artikel 9 (4)

*Die Europäischen Eisenbahnagentur legt der Kommission spätestens zum 31. Dezember 2011 einen Bericht vor, der Folgendes umfasst:*

*(a) eine Analyse der Erfahrungen mit der Anwendung der CSM für die Risikoevaluierung und –bewertung, einschließlich derjenigen Fälle, in denen von den Vorschlagenden die CSM auf freiwilliger Basis vor dem relevanten in Artikel 10 genannten Geltungsdatum angewandt wurde;*

*(b) eine Analyse der Erfahrungen der Vorschlagenden im Zusammenhang mit den Entscheidungen bezüglich der Signifikanz der Änderungen;*

*(c) eine Analyse der Fälle, in denen gemäß Abschnitt 2.3.8 des Anhangs I anerkannte Regeln der Technik zugrunde gelegt werden;*

*(d) eine Analyse der allgemeinen Wirksamkeit der CSM für die Risikoevaluierung und –bewertung.*

*Die Sicherheitsbehörden unterstützen die Agentur, indem sie Fälle der Anwendung der CSM für die Risikoevaluierung und –bewertung ermitteln.*

[G 1] Eine zusätzliche Erläuterung erscheint nicht notwendig.

## Artikel 10. Inkrafttreten

### Artikel 10 (1)

*Diese Verordnung tritt am zwanzigsten Tag nach ihrer Veröffentlichung im Amtsblatt der Europäischen Union in Kraft.*

[G 1] Eine zusätzliche Erläuterung erscheint nicht notwendig.



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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

## Artikel 10 (2)

*Diese Verordnung gilt ab 1. Juli 2012.*

*Jedoch gilt sie ab 19. Juli 2010:*

*(a) für alle signifikanten technischen Änderungen, die Fahrzeuge im Sinne des Artikels 2 Buchstabe c der Richtlinie 2008/57/EG betreffen;*

*(b) für alle signifikanten Änderungen, die strukturelle Teilsysteme betreffen, in Fällen, in denen Artikel 15 Absatz 1 der Richtlinie 2008/57/EG oder eine TSI dies vorschreibt.*

[G 1] Eine zusätzliche Erläuterung erscheint nicht notwendig.



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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

# ANHANG I – ERLÄUTERUNG DES PROZESSES IN DER CSM-VERORDNUNG

## 1. ALLGEMEINE GRUNDSÄTZE FÜR DAS RISIKO-MANAGEMENTVERFAHREN

### 1.1. Allgemeine Grundsätze und Verpflichtungen

*1.1.1. Das Risikomanagementverfahren, das Gegenstand dieser Verordnung ist, beginnt mit der Definition des zu bewertenden Systems und umfasst folgende Schritte:*

*(a) das Risikobewertungsverfahren, in dessen Rahmen die Gefährdungen, die Risiken, die entsprechenden Sicherheitsmaßnahmen und die sich daraus ergebenden Sicherheitsanforderungen, die das der Bewertung unterzogene System erfüllen muss, ermittelt werden;*
*(b) den Nachweis, dass das System die ermittelten Sicherheitsanforderungen erfüllt;*
*(c) das Management aller ermittelten Gefährdungen und der entsprechenden Sicherheitsmaßnahmen.*

*Das Risikomanagementverfahren ist ein iteratives Verfahren, das in der Anlage grafisch dargestellt ist. Das Verfahren endet, wenn nachgewiesen ist, dass das System alle Sicherheitsanforderungen erfüllt, die im Hinblick auf die Akzeptanz der mit den ermittelten Gefährdungen verbundenen Risiken erforderlich sind.*

[G 1] Der Risikomanagementrahmen für die CSM und das verbundene Risikobewertungsverfahren sind in Abbildung 1 illustriert. Die einzelnen Textboxen/Aktivitäten dieser Abbildung werden bei Bedarf in speziellen Abschnitten des vorliegenden Dokument noch näher beschrieben.

[G 2] CENELEC empfiehlt, dass die Risikomanagement- und der Risikobewertungsverfahren in einem Sicherheitsplan beschrieben werden. Falls dies für das gegebene Projekt nicht zweckdienlich erscheint, kann die entsprechende Beschreibung in einem anderen einschlägigen Dokument erfolgen. Siehe Abschnitt 1.1.6.

[G 3] Das Risikobewertungsverfahren beginnt mit einer vorläufigen Systemdefinition. Im Zuge der Projektentwicklung wird die vorläufige Systemdefinition fortschreitend aktualisiert und schließlich durch die Systemdefinition ersetzt. Wenn eine vorläufige Systemdefinition fehlt, wird für die Durchführung der Risikobewertung die förmliche Systemdefinition verwendet. Dabei ist es allerdings angeraten, dass sich alle von der signifikanten Änderung betroffenen Akteure zu Beginn des Projektes versammeln, um:

(a) sich auf die globalen Systemgrundsätze, Systemfunktionen usw. zu verständigen. Im Prinzip könnte dies in einer vorläufigen Systemdefinition beschrieben werden;
(b) die Projektorganisation zu vereinbaren;
(c) die Rollen- und Aufgabenteilung unter den verschiedenen bereits beteiligten Akteuren, einschließlich gegebenenfalls NSA, BEST und USB, zu vereinbaren.

Eine solche Koordinierung, beispielsweise während der vorläufigen Systemdefinition, gibt dem Vorschlagenden sowie gegebenenfalls den Subunternehmern, NSA, BEST und USB die Möglichkeit, sich in einer frühen Phase auf geeignete, im Projekt anwendbare anerkannte Regeln der Technik oder Referenzsysteme zu einigen.



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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

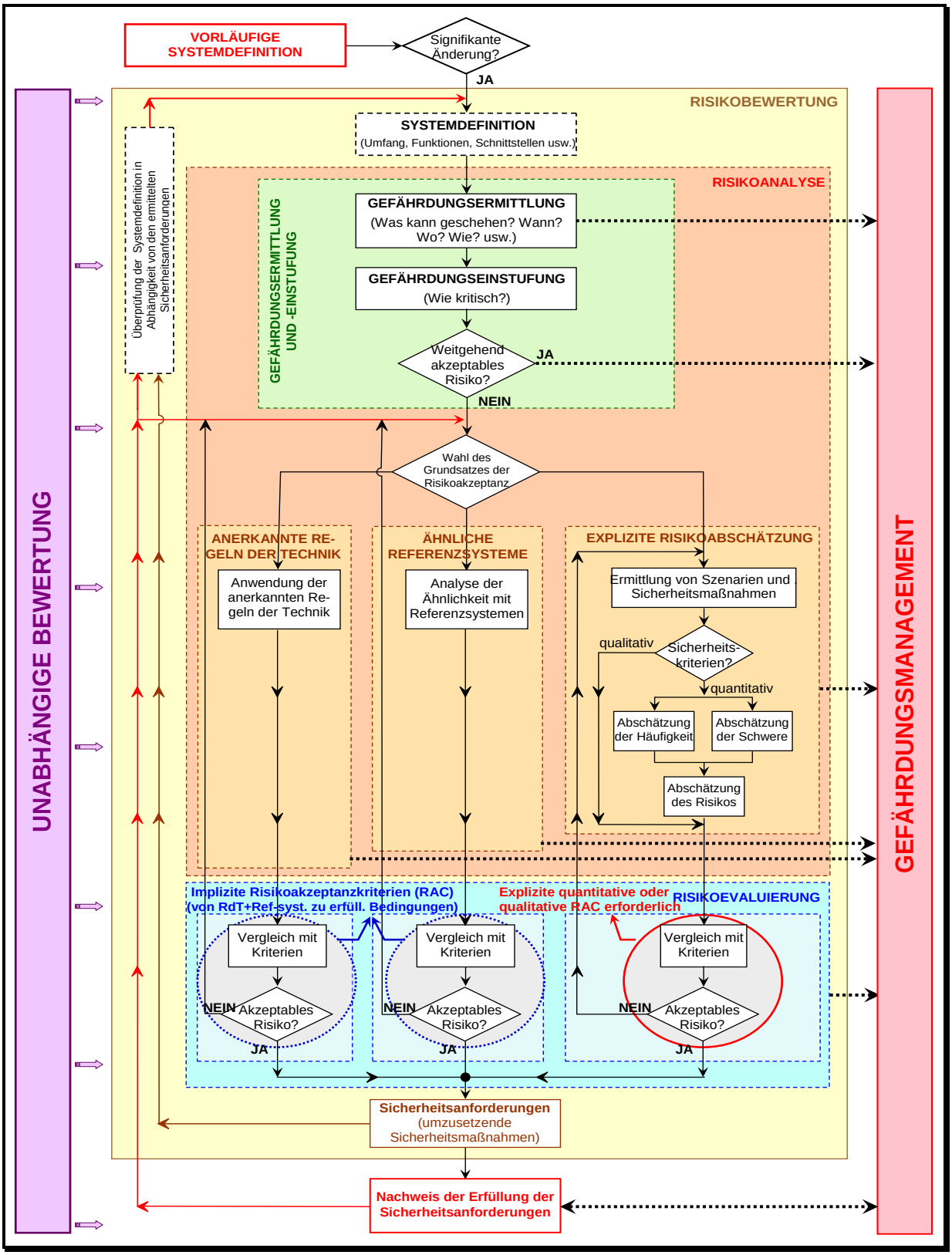


***Abbildung 1 : Risikomanagementrahmen in der CSM-Verordnung {Ref. 3}.***



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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. Dieses iterative Risikomanagementverfahren:*

*(a) beinhaltet angemessene Qualitätssicherungsmaßnahmen und wird von qualifiziertem Personal durchgeführt;*

*(b) wird einer unabhängigen Bewertung durch eine oder mehrere Bewertungsstellen unterzogen.*

[G 1] Das Sicherheitsmanagementsystem (SMS) der Eisenbahnunternehmen und Fahrwegbetreiber legt den Prozess und die Verfahren fest, die:

(a) die ständige Sicherheit des Systems während seines gesamten Lebenszyklus (d. h. während seines Betriebs und seiner Instandhaltung) überwachen;
(b) die sichere Demontage oder Ersetzung des entsprechenden Systems gewährleisten.

Dieser Prozess ist nicht Teil der CSM über die Risikobewertung.

[G 2] Zur Implementierung der CSM ist es notwendig, dass alle beteiligten Parteien entsprechende Kompetenz besitzen (d. h. über die geeigneten Fertigkeiten, Kenntnisse und Erfahrungen verfügen). In den Organisationen der Akteure im Eisenbahnsektor besteht ein ständiger Bedarf an Kompetenzmanagement:

(a) bei den Fahrwegbetreibern und Eisenbahnunternehmen ist dies im Sicherheitsmanagementsystem (SMS) nach Anhang III Ziffer 2 Buchstabe e der Eisenbahnsicherheitsrichtlinie {Ref. 1} erfasst;

(b) bei den anderen Akteuren, deren Aktivitäten die Sicherheit des Eisenbahnsystems beeinflussen können, bei denen aber keine Pflicht zum SMS besteht (siehe Punkt [G 1] in Abschnitt 5.1), wird diese Anforderung durch einen bestehenden Qualitäts-managementprozess (QMP) und/oder Sicherheitsmanagementprozess (SMP) erfüllt.

[G 3] Die folgenden Abschnitte der Norm CENELEC EN 50 126-1 {Ref. 8} betreffen die Frage der Kompetenz:

(a) gemäß § 5.3.5.(b): *„Alles Personal mit Verantwortung im Rahmen des*“ Risiko-*„Management-Prozesses muss kompetent sein, um diese Verantwortung zu übernehmen“*;

(b) § 5.3.5.(d): Die Anforderungen von Risikomanagement und Risikobewertung müssen *„in die Geschäftsprozesse implementiert werden, unterstützt durch ein Qualitätsmanagementsystem (QMS) entsprechend den Anforderungen von EN ISO 9001, EN ISO 9002 oder EN ISO 9003 und angemessen für das zu“* bewertende *„System“.* Ein Beispiel für durch das Qualitätsmanagementsystem kontrollierte Aspekte findet sich in Abschnitt § 5.2 der Norm EN 50 129 {Ref. 7}.

Diese betreffen die Aktivitäten der Qualitätssicherung sowie die Personalkompetenz und Mitarbeiterschulung, die für die Unterstützung des von der CSM erfassten Prozesses erforderlich sind.

[G 4] Sehr oft wird das Risikobewertungsverfahren gleich von Beginn des Projekts an von einer Bewertungsstelle begleitet, wobei eine derart frühzeitige Beteiligung der Bewertungsstelle zwar angeraten, aber keine Pflicht ist, außer in Fällen, wo dies im nationalen Recht eines Mitgliedstaates gefordert wird. Die Fachmeinung der unabhängigen Bewertungsstelle könnte immer dann nützlich sein, wenn der Übergang von einem Schritt der Risikobewertung zum nächsten Schritt bevorsteht. Siehe Artikel 6 für weitere Einzelheiten zur unabhängigen Bewertung.



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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. Der Vorschlagende, der für das durch diese Verordnung vorgeschriebene Risikomanagementverfahren verantwortlich ist, führt ein Gefährdungsprotokoll im Sinne von Abschnitt 4.*

[G 1] Eine zusätzliche Erläuterung erscheint nicht notwendig.

*1.1.4. Akteure, die bereits über Methoden oder Instrumente für die Risikobewertung verfügen, können diese weiterhin anwenden, sofern sie den Bestimmungen dieser Verordnung entsprechen und sofern folgende Bedingungen erfüllt sind:*

*(a) Die Risikobewertungsmethoden oder -instrumente sind im Rahmen eines Sicherheitsmanagementsystems beschrieben, das von einer nationalen Sicherheitsbehörde entsprechend Artikel 10 Absatz 2 Buchstabe a oder Artikel 11 Absatz 1 Buchstabe a der Richtlinie 2004/49/EG zugelassen wurde;*

*(b) oder die Risikobewertungsmethoden oder –instrumente sind aufgrund einer TSI vorgeschrieben oder entsprechen öffentlich zugänglichen anerkannten Normen, die in notifizierten nationalen Vorschriften niedergelegt sind.*

[G 1] Abbildung 2 illustriert die Beziehung zwischen der CSM und den „Sicherheitsmanagement-systemen und Risikobewertungsverfahren“.

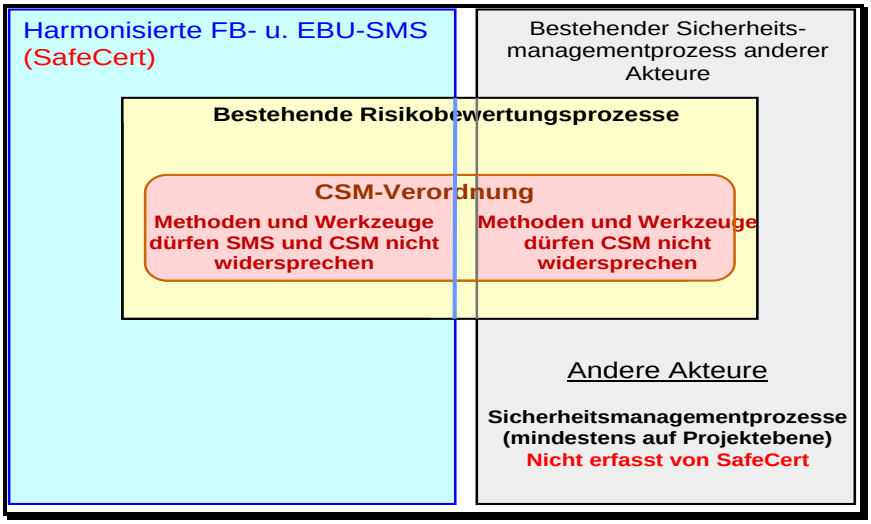


***Abbildung 2 : Harmonisierte SMS und CSM.***

*1.1.5. Unbeschadet der zivilrechtlichen Haftung nach den Rechtsvorschriften der Mitgliedstaaten unterliegt das Risikobewertungsverfahren der Verantwortung des Vorschlagenden. Insbesondere entscheidet der Vorschlagende in Abstimmung mit den betroffenen Akteuren, wer für die Erfüllung der sich aus der Risikobewertung ergebenden Sicherheitsanforderungen verantwortlich ist. Diese Entscheidung ist davon abhängig, welche Art von Sicherheitsmaßnahmen gewählt wurde, um die Risiken auf einem vertretbaren Niveau zu halten. Der Nachweis über die Erfüllung der Sicherheitsanforderungen erfolgt gemäß Abschnitt 3.*



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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] Wenn es sich beim Vorschlagenden um einen Fahrwegbetreiber oder ein Eisenbahnunternehmen handelt, kann es mitunter notwendig sein, weitere Akteure in den Prozess einzubinden(6) (siehe Abschnitt 1.2.1). In einigen Fällen kann es vorkommen, dass der Fahrwegbetreiber oder das Eisenbahnunternehmen die Aktivitäten der Risikobewertung ganz oder teilweise im Unterauftrag vergibt. Die vom jeweiligen Akteur zu übernehmen Rollen und Verantwortlichkeiten werden zwischen den betreffenden Akteuren gewöhnlich in einer frühen Projektphase vereinbart.

[G 2] Es ist wichtig darauf hinzuweisen, dass die Verantwortung für die Anwendung der CSM, für die Risikoakzeptanz und somit für die Sicherheit des Systems beim Vorschlagenden verbleibt. Damit wird sichergestellt:

(a) dass die beteiligten Akteuren lückenlos zusammenarbeiten, so dass alle notwendigen Informationen geliefert werden und
(b) dass eindeutig geregelt ist, wer die besonderen CSM-Anforderungen zu erfüllen hat (beispielsweise Durchführung der Risikoanalyse oder Führung des Gefährdungsprotokolls).

Sollten die Akteure sich nicht einigen können, welche Sicherheitsanforderungen sie jeweils zu erfüllen haben, könnte die NSA um eine Fachmeinung gebeten werden. Die Verantwortung zur Erarbeitung einer Lösung verbleibt jedoch beim Vorschlagenden und kann nicht auf die NSA übertragen werden: Siehe auch Abschnitt 0.2.2.

[G 3] Wenn die Aufgabe im Unterauftrag vergeben wird, hat der Subunternehmer, wenn er weder Fahrwegbetreiber noch Eisenbahnunternehmen ist, keine Pflicht zu einer eigenen Sicherheitsorganisation, insbesondere wenn es sich um einen in Struktur/Größe kleinen Subunternehmer handelt oder wenn sein Beitrag zum Gesamtsystem begrenzt ist. Die Verantwortung für das Risikomanagement, einschließlich Aktivitäten der Risikobewertung und des Gefährdungsmanagements, kann auf der höheren Organisationsebene verbleiben (d. h. beim Auftraggeber des Subunternehmers). Der Subunternehmer ist jedoch immer verantwortlich dafür, dass er in Bezug auf seine Aktivitäten die korrekten Informationen übermittelt, die die höhere Organisationsebene für den Aufbau der Risikomanagement-dokumentation benötigt.
Ferner können in Kooperation arbeitende Organisationen den Aufbau einer gemeinsamen Sicherheitsorganisation vereinbaren, beispielsweise zum Zwecke der Kostenoptimierung. In diesem Falle wird nur eine Organisation die Sicherheitsaktivitäten aller beteiligten Organisationen verwalten. Die Verantwortung für die Richtigkeit und Genauigkeit der Informationen (d. h. Gefährdungen, Risiken und Sicherheitsmaßnahmen) sowie für die Verwaltung der Umsetzung der Sicherheitsmaßnahmen verbleibt bei der Organisation, die mit der Kontrolle der mit diesen Sicherheitsmaßnahmen verbundenen Gefährdungen betraut ist.

[G 4] Im Regelfall würde der Vorschlagende die „Sicherheitsniveaus“ und „Sicherheits-anforderungen“ festlegen, die den projektbeteiligten Akteuren und den verschiedenen Teilsystemen und Ausrüstungen dieser Akteure zugeteilt werden, und zwar:

(a) in den zwischen dem Vorschlagenden und den jeweiligen Akteuren (Subunternehmern) geschlossenen Verträgen;
(b) in einem Sicherheitsplan oder einem anderen einschlägigen Dokument gleichen Zweckes mit der Beschreibung der Gesamtprojektorganisation und der Verantwortlichkeiten der einzelnen Akteure, einschließlich des Vorschlagenden: Siehe Abschnitt 1.1.6;
(c) in dem/den Gefährdungsprotokoll(en) des Vorschlagenden: Siehe Abschnitt 4.1.1.

(6) *In Übereinstimmung mit Anhang A.4 der CENELEC-Norm 50 129 {Ref. 7}.*



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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

Diese Zuweisung der „Sicherheitsniveaus“ und „Sicherheitsanforderungen“ auf die zugrunde liegenden Teilsysteme und Ausrüstungen und damit zu den entsprechenden Akteuren, einschließlich des Vorschlagenden selbst, kann während der „Phase des Nachweises der Übereinstimmung des Systems mit den Sicherheitsanforderungen“ verfeinert/ausgeweitet werden: Siehe Abbildung 1. Im Vergleich mit der V-Darstellung nach CENELEC (siehe Abschnitt 2.1.1 und Abbildung 5 auf Seite 36) entspricht diese Handlung der Phase 5, die die „Zuteilung von Systemanforderungen“ auf die verschiedenen Teilsysteme und Komponenten behandelt.

[G 5] Artikel 5 Absatz 2 erlaubt, dass andere Akteure als EBU und FB die Gesamtverantwortung für die Einhaltung der CSM entsprechend ihren eigenen jeweiligen Bedürfnisse übernehmen. Für generische Produkte oder generische Anwendungen(7) kann der Hersteller beispielsweise die Risikobewertung anhand einer „generischen Systemdefinition“ vornehmen, um die von generischen Produkten und generischen Anwendungen zu erfüllenden Sicherheitsniveaus und Sicherheitsanforderungen zu spezifizieren.

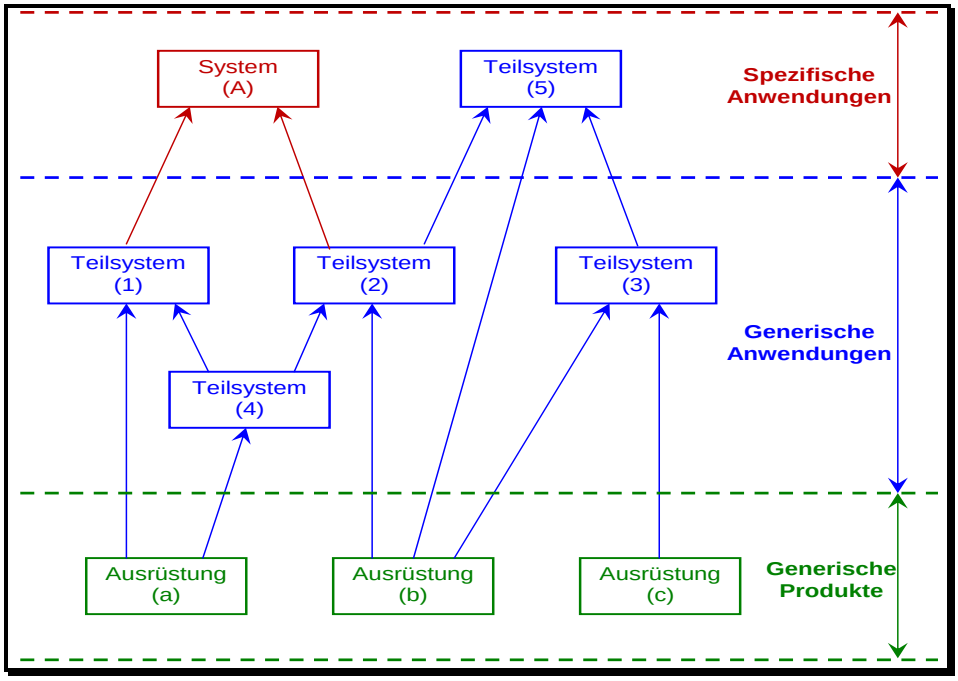


***Abbildung 3 : Beispiele für Abhängigkeiten zwischen Sicherheitsnachweisen (übernommen aus Abbildung 9 der Norm EN 50 129)***

[G 6] CENELEC empfiehlt, dass der Hersteller den dokumentierten Nachweis aus der Risikobewertung in generische Produktsicherheitsnachweise (bzw. Anwendungssicherheitsnachweise(7)) und in Gefährdungsprotokollen übernimmt. Diese Sicherheitsnachweise und

(7) *Die Terminologie „generischer Produktsicherheitsnachweis“ und „generischer Anwendungssicherheitsnachweis“ lehnt sich an CENELEC an, wo drei verschiedene Kategorien von Sicherheitsnachweisen betrachtet werden können (siehe Abbildung 3):*

(a) ***Generischer Produktsicherheitsnachweis*** *(anwendungsunabhängig). Ein generisches Produkt kann für verschiedene voneinander unabhängige Anwendungen wiederverwendet werden.*



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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

Gefährdungsprotokolle enthalten alle Annahmen[8] und festgestellten „Verwendungsbeschränkungen“ (d. h. sicherheitsbezogene Anwendungsbedingungen), die für die entsprechenden generischen Produkte (bzw. generische Anwendung) gelten. Sobald also beim Betrieb einer spezifischen Anwendung ein generisches Produkt und eine generische Anwendung verwendet werden, muss in jeder besonderen Anwendung die Übereinstimmung mit all diesen Annahmen[10] und „Verwendungsbeschränkungen“ (bzw. sicherheitsbezogenen Anwendungsbedingungen) nachgewiesen werden.

*1.1.6. Der erste Schritt des Risikomanagementverfahrens besteht darin, dass in einem vom Vorschlagenden zu erstellenden Dokument die Aufgaben der verschiedenen Akteure sowie ihre Risikomanagementmaßnahmen festgehalten werden. Der Vorschlagende sorgt für eine enge Zusammenarbeit zwischen den verschiedenen beteiligten Akteuren und koordiniert ihre Tätigkeiten – unter Berücksichtigung ihrer jeweiligen Aufgaben – im Sinne eines ordnungsgemäßen Managements der Gefährdungen und der entsprechenden Sicherheitsmaßnahmen.*

[G 1] Ein Projekt beinhaltet sehr oft auch ein Dokument, in dem die Risikomanagementaktivitäten beschrieben werden, außer soweit in den Verträgen zu Projektbeginn anders vereinbart. Sobald das originale System signifikante Änderungen erfährt, wird das einschlägige Dokument entsprechend aktualisiert und überarbeitet.

---

*Continuation of the footnote*

(b) ***Generischer Anwendungssicherheitsnachweis*** *(für eine Anwendungsklasse). Eine generische Anwendung kann für eine Anwendungsklasse/Anwendungsart mit gemeinsamen Funktionen wiederverwendet werden;*

(c) ***Spezifischer Anwendungssicherheitsnachweis*** *(für eine spezifische Anwendung). Eine spezifische Anwendung wird nur in einer besonderen Installation verwendet.*

*Nähere Informationen über die wechselseitige Abhängigkeit finden sich in Abschnitt § 9.4 und Abbildung 9.1 der CENELEC-Richtlinie 50 126-2 {Ref. 9}.*

*(8)* *Diese Annahmen und Verwendungsbeschränkungen bestimmen die Grenzen und die Gültigkeit der „Sicherheitsbewertungen“ und „Sicherheitsanalysen“ in Verbindung mit den generischen Produkt- und Anwendungssicherheitsnachweisen. Wenn diese von der betrachteten spezifischen Anwendung nicht erfüllt werden, ist eine Aktualisierung der entsprechenden „Sicherheitsbewertungen“ und „Sicherheitsanalysen“ (z. B. Ursachenanalysen) oder deren Ersatz durch neue notwendig.*

> *Dies steht im Einklang mit dem folgenden allgemeinen Sicherheitsgrundsatz: „Wenn der Entwurf eines spezifischen (Teil-)Systems auf der Grundlage generischer Anwendungen und generischer Produkte erfolgt, muss der Nachweis erbracht werden, dass das spezifische (Teil-)System alle Annahmen und Verwendungsbeschränken (in CENELEC bezeichnet als sicherheitsbezogene Anwendungsbedingungen) erfüllt, die in die entsprechenden generischen Anwendungs- und Produktsicherheitsnachweise exportiert werden (siehe Abbildung 3).”*

*Wenn bei einer spezifischen Anwendung die Einhaltung bestimmter Annahmen und Verwendungsbeschränkungen auf Teilsystemebene (z. B. im Falle betrieblicher Sicherheitsanforderungen) nicht erreichbar ist, können die entsprechenden Annahmen und Verwendungsbeschränkungen auf eine höhere Ebene (d. h. gewöhnlich auf die Systemebene) übertragen werden. Diese Annahmen und Verwendungsbeschränkungen werden anschließend in dem „spezifischen Anwendungssicherheitsnachweis“ des diesbezüglichen Teilsystems eindeutig gekennzeichnet. Das ist wesentlich, um in solchen Abhängigkeitsbeispielen sicherzustellen, dass die sicherheitsbezogenen Anwendungsbedingungen eines jeden Sicherheitsnachweises im Sicherheitsnachweis der höheren Ebene erfüllt werden oder aber in die sicherheitsbezogenen Anwendungsbedingungen des Sicherheitsnachweises der höchsten Ebene (d. h. des Systemsicherheitsnachweises) aufgenommen werden.*



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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] Ein solches Dokument trifft Festlegungen zu Organisationsstruktur, zu personellen Aufgabenzuweisungen, zu den Prozessen, Verfahren und Aktivitäten, die zusammen dafür sorgen, dass das zu bewertende System den vorgegebenen Sicherheitsniveaus und Sicherheitsanforderungen genügt. Das Dokument muss im Einklang mit der CSM stehen, da es die Bewertungsstelle unterstützt und anleitet. In den CENELEC-Normen wird empfohlen, dass diese Art der Information in einen Sicherheitsplan oder als abgegrenztes Teilthema in ein anderes Dokument aufgenommen wird.

[G 3] Insbesondere der Sicherheitsplan des Vorschlagenden, bzw. ein entsprechendes anderes Dokument, stellt die Gesamtprojektorganisation dar. Er beschreibt die Aufteilung der Rollen und Verantwortlichkeiten unter den beteiligten Akteuren. Für Detailinformationen kann auf die Sicherheitspläne oder Sicherheitsorganisationen der verschiedenen beteiligten Akteure verwiesen werden. Gewöhnlich erfolgt die Erörterung und Vereinbarung der Aufteilung von Verantwortlichkeiten zwischen den verschiedenen Akteuren im Rahmen der vorläufigen Systemdefinition (d. h. zu Projektbeginn), sofern eine solche vorgenommen wird.

[G 4] Der Sicherheitsplan ist ein dynamisches Dokument, das im Zuge der Projektdauer bei Bedarf aktualisiert wird.

[G 5] Nähere Einzelheiten zum Inhalt eines Sicherheitsplans finden sich in der Norm EN 50 126-1 {Ref. 8} und in dem mit ihr verbundenen Leitfaden 50 126-2 {Ref. 9}.

*1.1.7. Für die Bewertung der ordnungsgemäßen Anwendung des in dieser Verordnung beschriebenen Risikomanagementverfahrens ist die Bewertungsstelle zuständig.*

[G 1] Eine zusätzliche Erläuterung erscheint nicht notwendig.

## 1.2. Schnittstellen-Management

*1.2.1. An allen Schnittstellen, die für das zu bewertende System von Bedeutung sind, arbeiten die betroffenen Akteure des Eisenbahnsektors – unbeschadet der in einschlägigen TSI definierten Schnittstellenspezifikationen – zusammen, um gemeinsam die Ermittlung und das Management der Gefährdungen und der entsprechenden Sicherheitsmaßnahmen, die an diesen Schnittstellen relevant sind, zu bewerkstelligen. Das Management gemeinsamer Risiken an den Schnittstellen wird vom Vorschlagenden koordiniert.*

[G 1] Wenn beispielsweise ein Eisenbahnunternehmen aus betrieblichen Gründen einen Fahrwegbetreiber für die Durchführung bestimmter Änderungen am Fahrweg benötigt, so überwacht das EBU gemäß den Anforderungen in Anhang III Ziffer 2 Buchstabe g der Eisenbahnsicherheitsrichtlinie {Ref. 1} auch die Gesamtleistung, um die sachgerechte Erledigung der erwarteten Änderungen zu gewährleisten. Durch die Führungsrolle des EBU wird der entsprechende FB jedoch nicht von seiner Verantwortung entbunden, die anderen Eisenbahnunternehmen entsprechend zu informieren, falls auch diese von der entsprechenden Änderung des Fahrwegs beeinträchtigt werden. Der FB kann sogar zur Durchführung einer Risikobewertung entsprechend der CSM verpflichtet sein, wenn es sich bei der Änderung um eine aus seinem Blickwinkel signifikante Änderung handelt.

[G 2] Übertragungen von Verantwortlichkeiten zwischen den verschiedenen Akteuren sind möglich und unter bestimmten Umständen sogar notwendig. Wenn jedoch mehrere Akteure an einem System tätig werden, wird sehr oft ein Akteur als Verantwortlicher für das gesamte


European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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 ausgewiesen. Es gibt stets Abhängigkeiten zwischen Teilsystemen und Betrieb, die einen besonderen Ermittlungsaufwand erfordern. Dies macht es notwendig, dass jemand die Gesamtverantwortung für die Sicherheitsanalysen übernimmt und auch den kompletten Zugang zu allen einschlägigen Dokumentationen erhält. Es liegt auf der Hand, dass die Gesamtverantwortung für eine systematische und vollständige Risikobewertung in der Regel der Vorschlagende trägt, der die signifikante Änderung einzuführen beabsichtigt.

[G 3] Die zu vereinbarenden Hauptkriterien für die Verwaltung einer Schnittstelle zwischen den betroffenen Akteuren sind:

(a) die Leitung, die in der Regel der Vorschlagende übernimmt, der die signifikante Änderung einzuführen beabsichtigt;
(b) die erforderlichen Eingaben (Inputs);
(c) die Methoden für Gefährdungsermittlung und Risikobewertung;
(d) die erforderlichen Teilnehmer mit der benötigten Kompetenz (d. h. Kombination von Kenntnissen, Fertigkeiten und praktischen Erfahrungen – siehe auch Definition „Personalkompetenz“ in Punkt [G 2](b) von Artikel 3 in {Ref. 4});
(e) die erwarteten Ausgaben (Outputs).

Diese Kriterien werden in den Sicherheitsplänen (oder in anderen einschlägigen Dokumenten) der mit den jeweiligen Schnittstellen befassten Unternehmen beschrieben.

[G 4] Abschnitt C.3 von Alage C gibt Beispiele für Schnittstellen sowie ein Beispiel für die Anwendung der genannten Hauptkriterien beim Schnittstellenmanagement zwischen einem Zughersteller und einem Fahrwegbetreiber bzw. einem Eisenbahnunternehmen.

[G 5] Das Schnittstellenmanagement muss bei der Gestaltung dieser Schnittstellen auch die Risiken berücksichtigen, die an den Schnittstellen mit menschlichen Bedienern (in Betrieb und Instandhaltung) entstehen können.

*1.2.2. Wenn ein Akteur feststellt, dass zur Erfüllung einer Sicherheitsanforderung eine Sicherheitsmaßnahme notwendig ist, die er nicht selbst umsetzen kann, überträgt er die Zuständigkeit für das Management der in Frage stehenden Gefährdung auf einen anderen Akteur, mit dem er eine entsprechende Vereinbarung getroffen hat. Dabei ist das in Abschnitt 4 beschriebene Verfahren einzuhalten.*

[G 1] Der Prozess der Übertragung von Gefährdungen und damit verbundenen Sicherheitsmaßnahmen zwischen Akteuren gilt auch auf den unteren Ebenen der V-Darstellung von CENELEC Bild 5 auf Seite 36. Er kann angewendet werden, sobald der Austausch entsprechender Informationen beispielsweise zwischen einem Akteur und seinen Subunternehmern notwendig ist. Der Unterschied zum gleichen Prozess auf Systemebene besteht darin, dass der Vorschlagende nicht über alle auf Teilsystemebene erfolgten Übertragungen von Gefährdungen und verbundenen Sicherheitsmaßnahmen informiert werden muss. Der Vorschlagende wird nur dann informiert, wenn die übertragenen Gefährdungen und verbundenen Sicherheitsmaßnahmen sich auf Schnittstellen der oberen Ebene beziehen (d. h. bei Auswirkungen auf eine Schnittstelle mit dem Vorschlagenden).



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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. In Bezug auf das System, das der Bewertung unterzogen wird, ist jeder Akteur, der feststellt, dass eine Sicherheitsmaßnahme nicht den Anforderungen genügt oder unzureichend ist, dafür verantwortlich, dass der Vorschlagende davon in Kenntnis gesetzt wird; dieser unterrichtet seinerseits den für die Umsetzung der Sicherheitsmaßnahme zuständigen Akteur.*

[G 1] Das Sicherheitsmanagementsystem (SMS) von EBU und FB umfasst die Vereinbarungen und Verfahren zur Sicherstellung der sachgerechten Behandlung von Nichtübereinstimmungen bzw. Unzulänglichkeiten von Sicherheitsmaßnahmen. Aus diesem Grund sind diese Vereinbarungen und Verfahren nicht Teil der CSM.

[G 2] Gleichermaßen werden Vereinbarungen und Verfahren[9], die von den anderen Akteuren[10] vorzusehen sind, um sicherzustellen, dass Nichtübereinstimmungen oder Unzulänglichkeiten von Sicherheitsmaßnahmen sachgerecht behandelt und, falls notwendig, die Sicherheitsmaßnahmen auf alle entsprechenden Akteure übertragen werden, zu Beginn des Projekts zwischen den entsprechenden Akteuren vereinbart und detailliert in deren jeweiligem Sicherheitsplan dargelegt: Siehe Abschnitt 0.2.

*1.2.4. Der Akteur, der die Sicherheitsmaßnahme umsetzt, informiert daraufhin alle Akteure, die von dem Problem betroffen sind, sei es innerhalb des zu bewertenden Systems oder – soweit dem betreffenden Akteur bekannt – innerhalb anderer bestehender Systeme, die dieselbe Sicherheitsmaßnahme anwenden.*

[G 1] Dies gestattet die Verwaltung einer eventuellen Nichtübereinstimmung oder Unzulänglichkeit der Sicherheitsmaßnahme innerhalb des zu bewertenden Systems oder innerhalb ähnlicher Systeme, in denen die gleiche Maßnahme verwendet wird.

*1.2.5. Wenn zwischen zwei oder mehreren Akteuren keine Einigung erzielt werden kann, obliegt es dem Vorschlagenden, eine angemessene Lösung zu finden.*

[G 1] Eine zusätzliche Erläuterung erscheint nicht notwendig.

*1.2.6. Kann eine in einer notifizierten nationalen Vorschrift festgelegte Anforderung von einem Akteur nicht erfüllt werden, holt der Vorschlagende den Rat der zuständigen Behörde ein.*

[G 1] Eine zusätzliche Erläuterung erscheint nicht notwendig.

*(9) Grundsätzlich werden diese Vereinbarungen und Verfahren vom Qualitätsmanagement- und/oder Sicherheitsmanagementprozess dieser Akteure behandelt, wie mindestens auf Projektebene (siehe auch Abbildung 2) festgelegt.*

*(10) Der Begriff „andere Akteure“ bezeichnet alle betroffenen Akteure außer FB und EBU.*



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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

| | |
|---|---|
| *1.2.7.* | *Unabhängig von der Definition des zu bewertenden Systems hat der Vorschlagende sicherzustellen, dass das Risikomanagement das System selbst wie auch die Integration des Systems in das Eisenbahnsystem als Ganzes abdeckt.* |

[G 1] Eine zusätzliche Erläuterung erscheint nicht notwendig.



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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. BESCHREIBUNG DES RISIKOBEWERTUNGSVERFAHRENS

## 2.1. Allgemeine Beschreibung – Entsprechung zwischen dem Risikobewertungsverfahren der CSM und der V-Darstellung der CENELEC

*2.1.1. Das Risikobewertungsverfahren ist der iterative Gesamtprozess, der folgende Schritte umfasst:*

*(a) Systemdefinition;*
*(b) Risikoanalyse, einschließlich Gefährdungsermittlung;*
*(c) Risikoevaluierung.*

*Das Risikobewertungsverfahren wird in Interaktion mit dem Gefährdungsmanagement gemäß Abschnitt 4.1 durchgeführt.*

[G 1] Das Risikomanagementverfahren der CSM lässt sich als V-Darstellung abbilden, beginnend mit der (vorläufigen) Systemdefinition und endend mit der Systemabnahme: Siehe Abbildung 4. Dieses vereinfachte V-Bild kann daraufhin auf die klassische V-Darstellung von Bild 10 der Norm EN 50 126-1 {Ref. 8} abgebildet werden. Um die Entsprechung des Risikomanagementverfahrens der CSM nach Abbildung 1 zu verdeutlichen, wird in Abbildung 5 die V-Darstellung nach Bild 10 der CENELEC übernommen:

(a) die „vorläufige Systemdefinition“ der CSM nach Abbildung 1 entspricht der Phase 1 im V-Bild der CENELEC, d. h. der „Konzept“-Systemdefinition (siehe BOX 1 in Abbildung 5);
(b) die „Risikobewertung“ der CSM nach Abbildung 1 umfasst die folgenden Phasen der V-Darstellung der CENELEC (siehe BOX 2 in Abbildung 5):

(1) Phase 2 in Abbildung 5: „Systemdefinitionen und Anwendungsbedingungen“;
(2) Phase 3 in Abbildung 5: „Risikoanalyse“;
(3) Phase 4 in Abbildung 5: „Anforderungen an das System“;
(4) Phase 5 in Abbildung 5: „Zuteilung der Systemanforderungen“ zu den verschiedenen Teilsystemen und Komponenten.

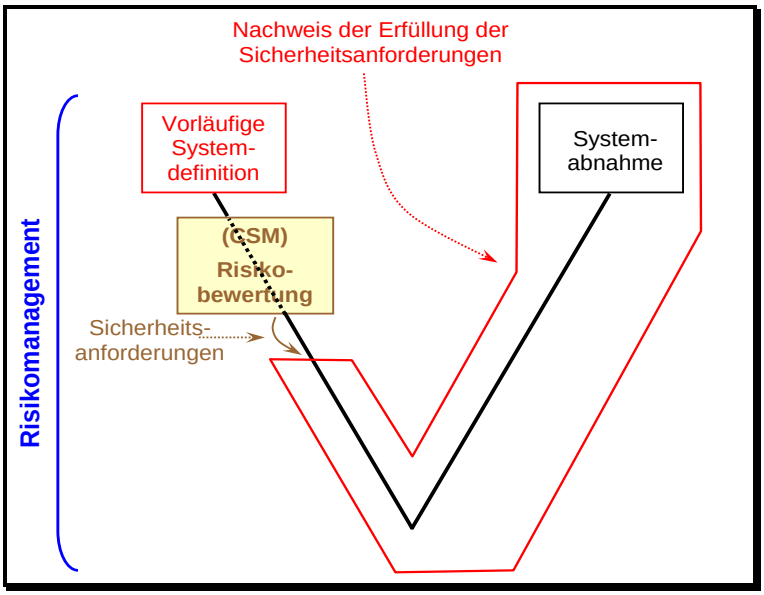


***Abbildung 4 : Vereinfachte V-Darstellung nach Bild 10 der Norm EN 50 126.***



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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

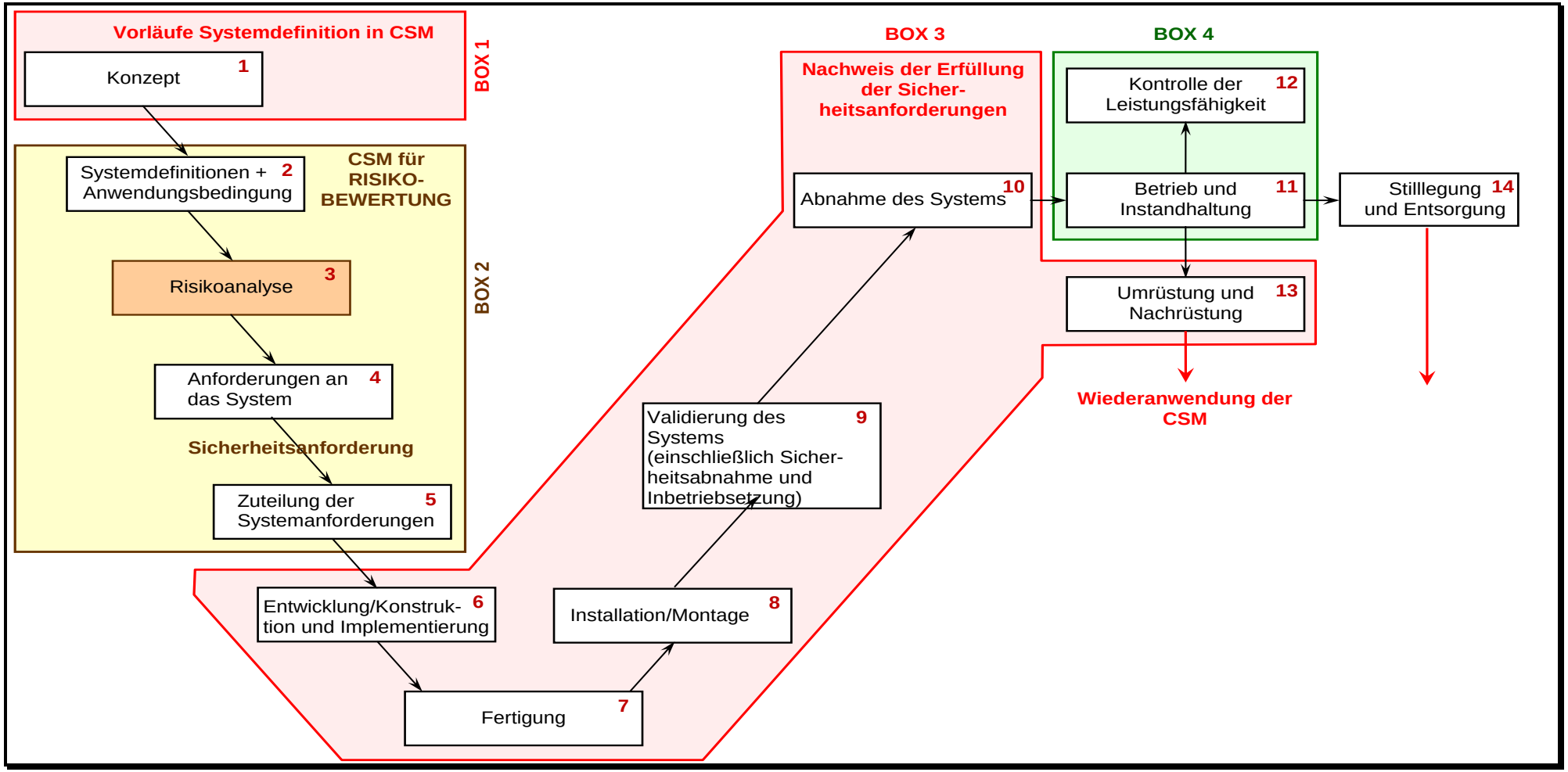


***Abbildung 5 : Bild 10 aus der Norm EN 50 126 V-Darstellung (CENELEC Systemlebenszyklus).***



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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] Die Ausgaben (Outputs) des Risikobewertungsverfahrens in der CSM sind (nach Wiederholungen – siehe Abbildung 1):

(a) die „Systemdefinition“ nach Aktualisierung mit den „Sicherheitsanforderungen“ aus den Aktivitäten der „Risikoanalyse“ und „Risikoevaluierung“ (siehe Abschnitt 2.1.6).
(b) die „Zuteilung der Systemanforderungen“ zu den verschiedenen Teilsystemen und Komponenten (Phase 5 in Abbildung 5);
(c) das „Gefährdungsprotokoll“ mit Angabe:

(1) aller ermittelten Gefährdungen und der damit verbundenen Sicherheitsmaßnahmen;
(2) der daraus folgenden Sicherheitsanforderungen;
(3) der für das System berücksichtigten Annahmen, die die Grenzen und die Gültigkeit der Risikobewertung bestimmen (siehe Punkt (g) in Abschnitt 2.1.2);

(d) und im Allgemeinen alle aus der Anwendung der CSM hervorgehenden Nachweise: Siehe Abschnitt 5.

Diese Ausgaben der CSM-Risikobewertung entsprechen den sicherheitsbezogenen Outputs der Phase 4 in der V-Darstellung der CENELEC, d. h. der Spezifikation der Systemanforderungen in Abbildung 5

[G 3] Die um die Ergebnisse der Risikobewertung aktualisierte Systemdefinition und das Gefährdungsprotokoll stellen die Eingabegrößen dar, anhand derer das System konstruiert und abgenommen wird. Der „Nachweis der Übereinstimmung des Systems mit den Sicherheitsanforderungen“ in der CSM entspricht den folgenden Phasen der V-Darstellung der CENELEC (siehe BOX 3 in Abbildung 5):

(a) Phase 6 in Abbildung 5: „Entwicklung/Konstruktion und Implementierung“;
(b) Phase 7 in Abbildung 5: „Fertigung“;
(c) Phase 8 in Abbildung 5: „Installation/Montage“;
(d) Phase 9 in Abbildung 5: „Validierung des Systems (einschließlich Sicherheitsabnahme und Inbetriebsetzung)“;
(e) Phase 10 in Abbildung 5: „Abnahme des Systems“.

[G 4] Der Nachweis der Systemübereinstimmung mit den Sicherheitsanforderungen hängt davon ab, ob die signifikante Änderung technischer, betrieblicher oder organisatorischer Art ist. So ist es möglich, dass die verschiedenen Schritte im CENELEC-Zyklus der V-Darstellung in Abbildung 5 nicht für alle signifikanten Änderungen der gegebenen Art geeignet sind. Die V-Darstellung in Abbildung 5 muss entsprechend betrachtet und dahingehend beurteilt werden, welche Schritte für eine spezifische Anwendung jeweils zutreffen (z. B. gibt es bei betrieblichen und organisatorischen Änderungen keine Fertigungsphase).

[G 5] Das bedeutet, dass der „Nachweis der Übereinstimmung des Systems mit den Sicherheitsanforderungen“ in der CSM nicht nur die Aktivitäten der „Verifizierung und Validierung“ durch Tests und Simulation beinhaltet. In der Praxis umfasst er alle Phasen „6 bis 10“ (siehe Liste oben und Abbildung 5) der V-Darstellung der CENELEC. Diese beinhalten die Aktivitäten der Entwicklung/Konstruktion, Fertigung, Installation/Montage, Verifizierung und Validierung sowie die verbundenen RAMS-Aktivitäten und die Systemabnahme.

[G 6] Ein allgemeiner Grundsatz beim Führen des „Nachweises der Übereinstimmung des Systems mit den Sicherheitsanforderungen“ besteht in der ausschließlichen Konzentration der Risikobewertung auf die sicherheitsbezogenen Funktionen und Schnittstellen des Systems. Sobald Risiko- und Sicherheitsbewertungshandlungen im Rahmen einer der



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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

Phasen der V-Darstellung der CENELEC aus Abbildung 5 erforderlich sind, konzentriert sich dieser Nachweis also auf:

(a) die sicherheitsbezogenen Funktionen und Schnittstellen;
(b) die Teilsysteme und/oder Komponenten, die an der Erreichung der sicherheitsbezogenen Funktionen und/oder Schnittstellen beteiligt sind, die während der auf höherer Ebene durchgeführten Risikobewertungsaktivitäten bewertet werden.

[G 7] Der Vergleich mit der klassischen V-Darstellung der CENELEC nach Abbildung 5 führt zu folgendem Ergebnis:

(a) Die CSM behandelt die Phasen „1 bis 10“ und „13“ dieser V-Darstellung. Diese beinhalten die für die Abnahme des zu bewertenden Systems erforderliche Reihe von Aktivitäten;

(b) Die CSM behandelt nicht die Phasen „11“, „12“ und „14“ des Systemlebenszyklus.

(1) Die Phasen „11“ und „12“ beziehen sich auf „Betrieb und Instandhaltung“ bzw. „Kontrolle der Leistungsfähigkeit“ des Systems nach seiner Abnahme auf Grundlage der CSM. Diese beiden Phasen werden durch das Sicherheitsmanagementsystem (SMS) der EBU und FB erfasst – (Siehe BOX 4 in Abbildung 5). Falls jedoch im Zuge des Betriebs, der Instandhaltung oder der Kontrolle der Leistungsfähigkeit eine Um- und Nachrüstung des Systems für notwendig erachtet wird (Phase 13 in Abbildung 5), während dieses also bereits betrieben wird, wird die CSM auf die erforderlichen neuen Änderungen gemäß Artikel 2 noch einmal angewendet. Deshalb gilt, wenn es sich um eine signifikante Änderung handelt:

(i) Die CSM-Verfahren von Risikomanagement und Risikobewertung kommen bei diesen neuen Änderungen zur Anwendung;
(ii) Eine Abnahme gemäß Artikel 6 ist für diese neuen Änderungen erforderlich;

(2) Auch die „Stilllegung und Entsorgung“ eines bereits im Betrieb befindlichen Systems (Phase 14) könnte als signifikante Änderung betrachtet werden, so dass für Phase 14 der Abbildung 5 die erneute Anwendung der CSM gemäß Artikel 2 in Betracht käme.

Nähere Informationen über den Umfang der einzelnen Phasen bzw. Aktivitäten aus der hier übernommenen V-Darstellung der CENELEC (Abbildung 5) finden sich in Abschnitt § 6 der Norm EN 50 126-1 {Ref. 8}.

*2.1.2. Bei der Systemdefinition sollten mindestens folgende Aspekte berücksichtigt werden:*

*(a) Zweckbestimmung des Systems, z. B. vorgesehene Verwendung;*
*(b) Funktionen und Bestandteile des Systems, sofern relevant (einschließlich z. B. menschlicher, technischer und betrieblicher Komponenten);*
*(c) Systemgrenzen, einschließlich anderer, interagierender Systeme;*
*(d) physische Schnittstellen (interagierende Systeme) und funktionale (Ein- und Ausgabe-)Schnittstellen;*
*(e) Systemumgebung (z. B. Energie- und Wärmefluss, Erschütterungen, Vibrationen, elektromagnetische Beeinflussung, betriebliche Verwendung);*
*(f) bestehende Sicherheitsmaßnahmen und – nach mehrfacher Anwendung – Definition der im Rahmen des Risikobewertungsverfahrens ermittelten Sicherheitsanforderungen;*
*(g) Annahmen, die die Grenzen der Risikobewertung bestimmen.*

[G 1] Eine zusätzliche Erläuterung erscheint nicht notwendig.



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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. Für das definierte System wird eine Gefährdungsermittlung gemäß Abschnitt 2.2 vorgenommen.*

[G 1] Eine zusätzliche Erläuterung erscheint nicht notwendig.

*2.1.4. Die Vertretbarkeit des Risikos des zu bewertenden Systems wird unter Zugrundelegung eines oder mehrerer der folgenden Grundsätze der Risikoakzeptanz evaluiert:*

*(a) Anwendung der anerkannten Regeln der Technik (Abschnitt 2.3);*

*(b) Vergleich mit ähnlichen Systemen (Abschnitt 2.4);*

*(c) explizite Risikoabschätzung (Abschnitt 2.5).*

*In Übereinstimmung mit dem allgemeinen Grundsatz gemäß Abschnitt 1.1.5 sieht die Bewertungsstelle davon ab, dem Vorschlagenden Auflagen bezüglich des anzuwendenden Grundsatzes der Risikoakzeptanz zu machen.*

[G 1] In der Regel entscheidet der Vorschlagende über den für die Kontrolle der ermittelten Gefährdungen am besten geeigneten Risikoakzeptanzgrundsatz anhand der spezifischen Anforderungen des Projektes sowie anhand der eigenen Erfahrung mit den drei Grundsätzen.

[G 2] Eine Beurteilung (Evaluierung) der Annehmbarkeit von Risiken auf Systemebene mit nur einem der drei Risikoakzeptanzgrundsätze ist nicht immer möglich. Die Risikoakzeptanz verwendet oft eine Kombination dieser Grundsätze. Falls bei einer erheblichen Gefährdung zur Kontrolle des mit ihr verbundenen Risikos mehr als ein Risikoakzeptanzgrundsatz angewendet werden muss, ist die entsprechende Gefährdung in Teilgefährdungen aufzugliedern, so dass jede einzelne Teilgefährdung mit nur einem Risikoakzeptanz-grundsatz adäquat kontrolliert wird.

[G 3] Die Entscheidung über die Kontrolle einer Gefährdung mit Hilfe eines Risikoakzeptanzgrundsatzes muss die Gefährdung und die in der Phase der Gefährdungs-ermittlung bereits ermittelten Gefährdungsursachen in Betracht ziehen. Falls also zwei unterschiedliche und unabhängige Ursachen mit der gleichen Gefährdung verbunden sind, muss die Gefährdung in zwei unterschiedliche Teilgefährdungen aufgespaltet werden. Jede Teilgefährdung wird dann durch einen einzigen Risikoakzeptanzgrundsatz kontrolliert. Die beiden Teilgefährdungen sind im Gefährdungsprotokoll einzutragen und zu verwalten. Falls beispielsweise die Gefährdung durch einen Konstruktionsfehler verursacht wird, kann sie durch Anwendung anerkannter Regeln der Technik verwaltet werden, wohingegen bei einem Instandhaltungsfehler die anerkannten Regeln der Technik allein für das Gefährdungsmanagement eventuell nicht ausreichen, so dass die Anwendung eines anderen Risikoakzeptanzgrundsatzes notwendig ist.

[G 4] Die Verminderung des Risikos auf ein vertretbares Maß verlangt eventuell mehrere Iterationen der Risikoanalyse- und Risikoevaluierungsphasen, bis schließlich geeignete Sicherheitsmaßnahmen ermittelt werden.

[G 5] Das vorliegende Restrisiko aus der praktischen Erfahrung mit bestehenden Systemen und für Systeme, die auf der Anwendung anerkannter Regeln basieren, wird als vertretbar anerkannt. Das mit expliziter Risikoabschätzung festgestellte Risiko beruht auf einem Fachurteil und auf verschiedenen während der Analysen vom Fachmann getroffenen Annahmen bzw. auf unfall- und betriebserfahrungs-bezogenen Datenbeständen. Deshalb kann das durch explizite Risikoabschätzung festgestellte Restrisiko nicht unmittelbar durch



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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

praktischen Erfahrungsrücklauf bestätigt werden. Ein solcher Nachweis erfordert Zeit in Bezug auf Betrieb, Überwachung und Sammlung von repräsentativen Erfahrungen mit dem/den diesbezüglichen System(en). In der Regel hat die Anwendung von anerkannten Regeln der Technik und der Vergleich mit ähnlichen Referenzsystemen den Vorteil der Vermeidung überspezifizierter, unnötig strikter Sicherheitsanforderungen, die durch ausdrücklich konservativ-vorsichtige (Sicherheits-)Annahmen in expliziten Risiko-abschätzungen hergeleitet werden können. Andererseits könnte es dazu kommen, dass Sicherheitsanforderungen aus anerkannten Regeln der Technik oder ähnlichen Referenzsystemen für das zu bewertende System nicht erfüllt werden müssen. In diesem Fall hätte die Anwendung einer expliziten Risikoabschätzung den Vorteil der Vermeidung einer unnötig übertriebenen Gestaltung des zu bewertenden Systems und würde eine kosteneffektivere Gestaltung ermöglichen, die bis dato nicht versucht wurde.

[G 6] Falls die ermittelten Gefährdungen und das bzw. die damit verbundene(n) Risiko/Risiken des zu bewertenden Systems durch Anwendung von anerkannten Regeln der Technik oder von ähnlichen Referenzsystemen nicht kontrolliert werden können, wird eine explizite Risikoabschätzung auf Grundlage quantitativer und qualitativer Analysen gefährlicher Ereignisse durchgeführt. Diese Situation entsteht gewöhnlich dann, wenn das zu bewertende System vollkommen neu (oder die Gestaltung innovativ) ist bzw. wenn das System von anerkannten Regeln der Technik oder von einem ähnlichen Referenzsystem abweicht. Durch die explizite Risikoabschätzung wird dann beurteilt, ob das Risiko akzeptabel ist (d. h. dass eine weitergehende Analyse nicht notwendig ist) oder ob zusätzliche Sicherheitsmaßnahmen zur weiteren Verminderung des Risikos erforderlich sind.

[G 7] Hinweise zur Risikoverminderung und Risikoakzeptanz finden sich auch in Abschnitt § 8 des Leitfadens EN 50 126-2 {Ref. 9}.

[G 8] Der verwendete Risikoakzeptanzgrundsatz und seine Anwendung müssen von der Bewertungsstelle bewertet werden.

*2.1.5. Der Vorschlagende weist in der Risikoevaluierung nach, dass der gewählte Risikoakzeptanzgrundsatz in angemessener Weise angewandt wird. Darüber hinaus überprüft der Vorschlagende, dass die ausgewählten Risikoakzeptanzgrundsätze einheitlich angewandt werden.*

[G 1] Wenn beispielsweise für die Software einer Komponente als Sicherheitsanforderung die Anwendung des SIL4-Entwicklungsprozesses der Norm EN 50 128 spezifiziert ist, muss bei der Nachweisführung der Beweis erbracht werden, dass der von der Norm empfohlene Prozess erfüllt wird. Hierzu gehört beispielsweise der Nachweis:

(a) dass die an die Organisation der Entwicklung, Verifizierung und Validation gestellten Unabhängigkeitsanforderungen erfüllt sind;
(b) dass die ordnungsgemäßen Methoden der Norm EN 50 128 für die Sicherheitsanforderungsstufe SIL 4 angewendet werden;
(c) usw.

[G 2] Wenn beispielsweise zweckgebundene anerkannte Regeln der Technik für die Herstellung von Notbremsventilen zu verwenden sind, muss der Nachweis den Beleg erbringen, dass während des Fertigungsprozesses alle Anforderungen aus den anerkannten Regeln der Technik erfüllt werden.



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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. Mit der Anwendung dieser Risikoakzeptanzgrundsätze werden mögliche Sicherheitsmaßnahmen ermittelt, mit denen die Risiken des zu bewertenden Systems auf ein vertretbares Maß beschränkt werden. Von diesen Sicherheitsmaßnahmen werden diejenigen, die für die Risikokontrolle ausgewählt wurden, zu Sicherheitsanforderungen, die vom System erfüllt werden müssen. Die Erfüllung dieser Sicherheitsanforderungen wird gemäß Abschnitt 3 nachgewiesen.*

[G 1] Es lassen sich zwei Arten von Sicherheitsmaßnahmen erkennen:

(a) „Vorbeugende Sicherheitsmaßnahmen“, die verhindern, dass Gefährdungen und deren Ursachen eintreten, und
(b) „Mindernde Sicherheitsmaßnahmen“, die verhindern, dass Gefährdungen sich zu Unfällen ausweiten, oder die die Folgen von Unfällen nach deren Eintreten abschwächen (Schutzmaßnahmen).

Zugunsten der Betriebsfähigkeit ist die Verhinderung von Ursachen in der Regel effektiver.

[G 2] Der Vorschlagende wird die Sicherheitsmaßnahmen als am besten geeignet betrachten, die den besten Kompromiss zwischen den für die Erreichung der Risikoverminderung notwendigen Kosten und dem Grad des Restrisikos ermöglichen. Die gewählten Sicherheitsmaßnahmen werden zu den Sicherheitsanforderungen für das zu bewertende System.

[G 3] Wichtig ist die Überprüfung, dass die für die Kontrolle einer Gefährdung ausgewählten Sicherheitsmaßnahmen nicht in Konflikt mit anderen Gefährdungen treten. Wie in Abbildung 6 zu sehen, können beispielsweise die folgenden Fälle eintreten[(11)]:

(a) FALL 1: Wenn ein und dieselbe Sicherheitsmaßnahme (Maßnahme A in Abbildung 6) verschiedene Gefährdungen kontrollieren kann, ohne Konflikte zwischen diesen zu verursachen, und soweit ökonomisch begründet, könnte die entsprechende Sicherheitsmaßnahme allein als verbundene „Sicherheitsanforderung“ gewählt werden. Die Gesamtanzahl an zu erfüllenden Sicherheitsanforderungen ist kleiner als bei der Umsetzung der beiden Maßnahmen B und C;

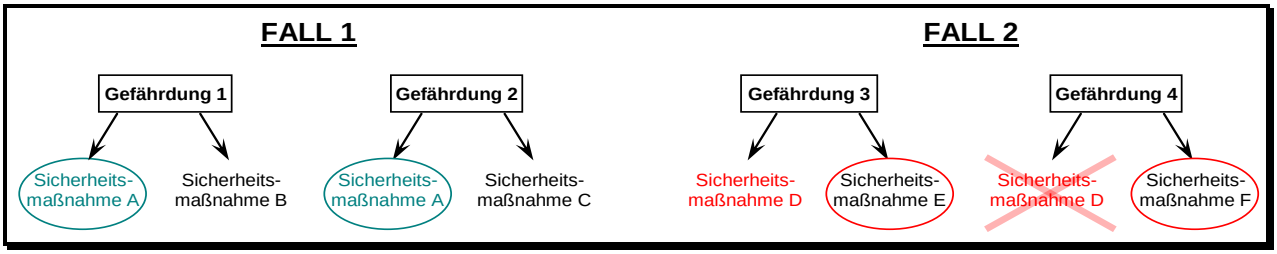


***Abbildung 6 : Auswahl adäquater Sicherheitsmaßnahmen für die Kontrolle von Risiken.***

(b) FALL 2: Hingegen gilt, dass eine Sicherheitsmaßnahme, die eine einzelne Gefährdung kontrollieren kann, aber einen Konflikt mit einer anderen Gefährdung verursacht (Maßnahme D in Abbildung 6), nicht als „Sicherheitsanforderung“ gewählt werden kann. Für die betrachtete Gefährdung müssen die anderen Sicherheitsmaßnahmen verwendet werden (Maßnahmen E und F in Abbildung 6):

---

*(11) Es ist darauf hinzuweisen, dass der Leitfaden nicht alle Situationen auflistet, bei denen Sicherheitsmaßnahmen in Konflikt mit anderen ermittelten Gefährdungen treten könnten. Es werden nur einige wenige illustrative Beispiele gegeben.*



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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) Ein typisches Beispiel im Zugsteuerungs-/Zugsicherungssystem ist die Verwendung der gleisseitigen Zugortung für die Kontrolle der Bremsenauslösung oder für die Freigabe der Beschleunigung. Die Verwendung der Zugfrontseite (bzw. Zugrückseite) für die Zugortung ist nicht in allen Fällen sicher:

(i) wenn das ETCS-Zugsicherungssystem eine sichere Notbremsung einleiten muss, verwendet es die maximale Sicherheitsstufe bezogen auf die Zugfrontseite (MAXIMUM SAFE FRONT END), damit gewährleistet ist, dass der Zug vorderseitig tatsächlich vor dem Erreichen der Gefahrenstelle zum Halt kommt;

(ii) wenn andererseits der Zug die Beschleunigungsfreigabe erhält, beispielsweise nach einer Geschwindigkeitsbegrenzung, bezieht sich das ETCS-Zugsicherungssystem auf die zugrückseitige Mindestsicherheit (MINIMUM SAFE REAR END).

(2) Ein anderes Beispiel ist eine Sicherheitsmaßnahme, die unter fast allen Gegebenheiten für das gefahrlose Stoppen eines Zuges im Fail-Safe-Zustand Gültigkeit haben kann, außer bei einem Tunnel oder bei einer Brücke. Im letzteren Falle darf die Maßnahme D in FALL 2 der Abbildung 6 nicht ergriffen werden.

*2.1.7. Das iterative Risikobewertungsverfahren kann als abgeschlossen betrachtet werden, wenn nachgewiesen ist, dass alle Sicherheitsanforderungen eingehalten werden und keine weiteren, nach vernünftigem Ermessen vorhersehbaren Gefährdungen zu berücksichtigen sind.*

[G 1] Abhängig z. B. von der getroffenen technischen Auswahl für die Gestaltung eines Systems, seiner Teilsysteme und Ausrüstungen könnten beim „Nachweis der Übereinstimmung mit den Sicherheitsanforderungen“ neue Gefährdungen erkannt werden (z. B. könnte die Verwendung einer bestimmten Lackfarbe zur Bildung toxischer Gase im Brandfall führen). Diese neuen Gefährdungen und mit ihnen verbundenen Risiken müssen als neue Eingabegrößen (Inputs) für eine neue Prozessschleife im iterativen Risikobewertungsverfahren berücksichtigt werden. Alage A.4.3 der Norm EN 50 129 gibt weitere Beispiele, wann neue Gefährdungen entstehen könnten und kontrolliert werden müssen.

## 2.2. Gefährdungsermittlung

*2.2.1. Der Vorschlagende ermittelt systematisch unter Rückgriff auf die umfassende Fachkenntnis eines qualifizierten Teams sämtliche nach vernünftigem Ermessen vorhersehbaren Gefährdungen für das gesamte zu bewertende System und gegebenenfalls für dessen relevante Funktionen sowie dessen Schnittstellen*

*Alle erkannten Gefährdungen werden gemäß Abschnitt 4 im Gefährdungsprotokoll erfasst.*

[G 1] Die Gefährdungen werden, soweit möglich, mit dem gleichem Detailgrad dargestellt. Bei den vorläufigen Gefährdungsanalysen kann es vorkommen, dass Gefährdungen mit unterschiedlichem Detailgrad erkannt werden (z. B. wenn Personen mit unterschiedlichen Erfahrungen im Rahmen einer HAZOP-Analyse zusammenarbeiten).
Der Detailgrad hängt auch von dem Risikoakzeptanzgrundsatz ab, der zur Kontrolle der ermittelten Gefährdung(en) ausgewählt wird. Wenn beispielsweise eine Gefährdung durch anerkannte Regeln der Technik oder durch ein ähnliches Referenzsystem vollständig kontrolliert werden kann, ist eine detailliertere Gefährdungsermittlung nicht notwendig.



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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] Alle während des Risikobewertungsverfahrens ermittelten Gefährdungen (einschließlich der Gefährdungen in Verbindung mit weitgehend akzeptablen Risiken) sowie die mit ihnen verbundenen Sicherheitsmaßnahmen und Risiken sind im Gefährdungsprotokoll einzutragen.

[G 3] Abhängig von der Art des zu analysierenden Systems können unterschiedliche Methoden bei der Gefährdungsermittlung verwendet werden:

(a) Es kann die empirische Gefährdungsermittlung unter Zuhilfenahme vergangener Erfahrungen verwendet werden (z. B. Checklisten oder Listen generischer Gefährdungen);
(b) für neue Bereiche kann die kreative Gefährdungsermittlung verwendet werden (proaktive Prognose, z. B. strukturierte „WAS-WENN"-Untersuchungen wie FMEA oder HAZOP).

[G 4] Die empirische Methode und die kreative Methode der Gefährdungsermittlung können gemeinsam in gegenseitiger Ergänzung verwendet werden, damit gewährleistet ist, dass die Liste der potenziellen Gefährdungen und die Sicherheitsmaßnahmen, soweit zutreffend, allumfassend sind.

[G 5] In einem vorläufigen Schritt könnte die Gefährdungsermittlung mit einem Brainstorming-Team beginnen, in dem Sachverständige unterschiedlicher Kompetenz zusammenarbeiten, die alle relevanten Aspekte der signifikanten Änderung behandeln. Wenn dieses Sachverständigengremium es für notwendig erachtet, können empirische Methoden für die Analyse einer spezifischen Funktion oder Betriebsart eingesetzt werden.

[G 6] Die für die Gefährdungsermittlung verwendeten Methoden sind abhängig von der Systemdefinition. Einige Beispiele finden sich im Alage B

[G 7] Weitere Informationen über die Techniken und Methoden der Gefährdungsermittlung sind in den Anhängen A.2 und E des Leitfadens EN 50 126-2 {Ref. 9} zu finden.

[G 8] Ein Beispiel für eine generische Gefährdungsliste ist in Abschnitt C.17 von Alage C enthalten.

*2.2.2. Mit dem Ziel, die Risikobewertung auf die wichtigsten Risiken zu konzentrieren, werden die Gefährdungen nach dem sich aus ihnen ergebenden geschätzten Risiko eingestuft. Auf der Grundlage eines Sachverständigenurteils müssen Gefährdungen, die mit einem weitgehend akzeptablen Risiko verbunden sind, nicht weiter analysiert, sondern lediglich im Gefährdungsprotokoll erfasst werden. Die Einstufung der Gefährdungen ist zu begründen, damit eine unabhängige Bewertung durch eine Bewertungsstelle vorgenommen werden kann.*

[G 1] Zur Unterstützung des Risikobewertungsverfahrens können die signifikanten Gefährdungen in verschiedene Kategorien weiter untergliedert werden. Beispielsweise können die signifikanten Gefährdungen abhängig vom zu erwartenden Schweregrad des Risikos und von der Eintrittshäufigkeit eingestuft oder geordnet werden. Eine Anleitung dazu findet sich in den CENELEC-Normen: siehe Abschnitt A.2 in Alage A

[G 2] Die in Abschnitt 2.1.4 beschriebene Risikoanalyse und Risikoevaluierung wird mit Prioritätensetzung angewendet, beginnend mit den höhergradigeren Gefährdungen.



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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. Aus Gefährdungen resultierende Risiken können beispielsweise dann als weitgehend akzeptabel eingestuft werden, wenn das Risiko so gering ist, dass die Einführung zusätzlicher Sicherheitsmaßnahmen nicht angemessen wäre. Das Sachverständigenurteil berücksichtigt, dass der Gesamtumfang aller weitgehend akzeptablen Risiken einen bestimmten Anteil am Gesamtrisiko nicht übersteigen darf.*

[G 1] Beispielsweise kann ein mit einer Gefährdung verbundenes Risiko als weitgehend akzeptabel betrachtet werden:

(a) wenn das Risiko unter einem angegebenen Prozentsatz (z. B. x%) vom maximal tragbaren Risiko für diesen Gefährdungstyp liegt. Der Wert x% kann auf einer Best-Practice und auf Erfahrungen mit mehreren Risikoanalyseansätzen beruhen, z. B. auf dem Klassifikationsverhältnis zwischen weitgehend akzeptablem Risiko und untragbarem Risiko als FN-Kurve oder Risikomatrix. Dies kann entsprechend Abbildung 7 dargestellt werden;

(b) oder wenn der mit dem Risiko verbundene Verlust so gering ist, dass die Implementierung einer sicherheitsbezogenen Gegenmaßnahme nicht vernünftig ist.

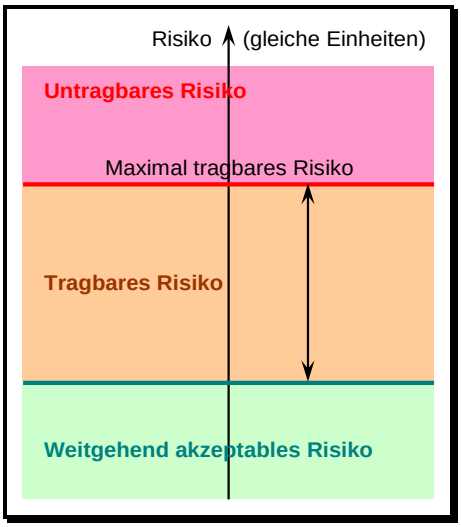


***Abbildung 7 : Weitgehend akzeptable Risiken***

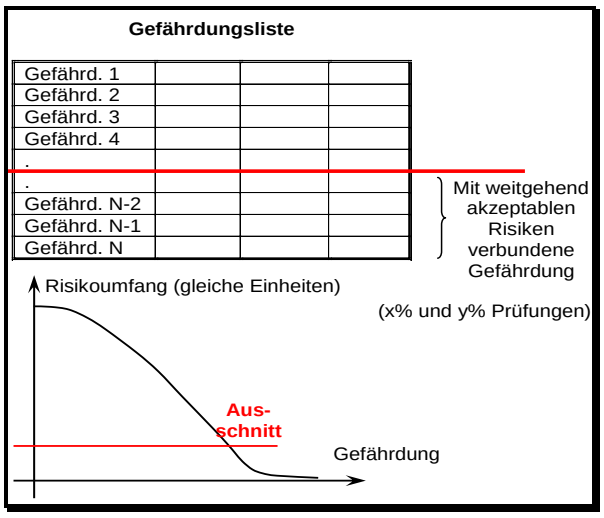


***Abbildung 8 : Filterung von Gefährdungen, die mit weitgehend akzeptablen Risiken verbunden sind***

[G 2] Wenn darüber hinaus Gefährdungen mit unterschiedlichen Detailgraden ermittelt werden (d. h. Gefährdungen der höheren Ebene einerseits und detaillierte Teilgefährdungen andererseits), müssen Vorkehrungsmaßnahmen getroffen werden, um eine falsche Einordnung in der Rubrik der mit weitgehend akzeptablen Risiken verbundenen Gefährdungen zu vermeiden. Der Beitrag aller mit weitgehend akzeptablen Risiken verbundenen Gefährdungen darf einen bestimmen Anteil (z. B. y%) des auf Systemebene bestehenden Gesamtrisikos nicht übersteigen. Diese Prüfung ist notwendig, um zu verhindern, dass der gedankliche Grundansatz durch ein Aufspalten der Gefährdungen in zu viele kleinteilige Gefährdungen ausgehöhlt wird. Wenn eine einzelne Gefährdung in zu vielen „kleineren“ Teilgefährdungen ausgedrückt wird, kann tatsächlich die einzelne Betrachtung jeder dieser Teilgefährdungen schnell dazu führen, dass eine Verbindung mit weitgehend akzeptablen Risiken ermittelt wird, während eine gemeinsame Beurteilung (d. h. die gemeinsame Betrachtung der Teilgefährdungen als eine Gefährdung höherer Ebene) im Ergebnis dazu führen kann, dass diese Gefährdung mit einem signifikanten Risiko verbunden ist. Der effektive Wert des prozentualen Anteils (z. B. y%) hängt davon ab,



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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

welche Risikoakzeptanzkriterien auf der Systemebene gelten. Er kann anhand von Betriebserfahrungen ähnlicher Referenzsysteme ermittelt bzw. geschätzt werden.

[G 3] Die beiden oben genannten Prüfungen (d. h. gegenüber x % und y %) ermöglichen die Bündelung der Risikobewertung auf die wesentlichsten Gefährdungen und sichern die Kontrolle signifikanter Risiken (siehe Abbildung 8).
Unbeschadet der rechtlichen Anforderungen eines Mitgliedstaates liegt es in der Verantwortung des Vorschlagenden, auf der Grundlage eines Sachverständigenurteils die Werte von x % und y % festzulegen und von der Bewertungsstelle unabhängig bewerten zu lassen. Die Werte können beispielsweise in der Größenordnung x = 1% und y = 10% liegen, wenn dies ausgehend vom Sachverständigenurteil für akzeptabel erachtet wird.

[G 4] Nach Abschnitt 2.2.2 bedarf die Einstufung in „weitgehend akzeptable Risiken“ einer unabhängigen Bewertung durch eine Bewertungsstelle.

*2.2.4. Bei der Gefährdungsermittlung können Sicherheitsmaßnahmen identifiziert werden. Diese werden gemäß Abschnitt 4 im Gefährdungsprotokoll erfasst.*

[G 1] Hauptziel der Aktivität ist die Ermittlung von Gefährdungen, die mit der Änderung verbunden sind. Sollten bereits Sicherheitsmaßnahmen festgestellt werden, sind diese in das Gefährdungsprotokoll einzutragen. Die Art der Maßnahmen ist abhängig von der Änderung; die Maßnahmen können verfahrensbezogener, technischer, betrieblicher oder organisatorischer Art sein.

*2.2.5. Die Gefährdungsermittlung muss nur so detailliert durchgeführt werden, dass bestimmt werden kann, in welchen Fällen davon auszugehen ist, dass durch Sicherheitsmaßnahmen die Risiken gemäß einem der in Ziffer 2.1.4 genannten Risikoakzeptanzgrundsätze kontrolliert werden können. Somit müssen die Phasen der Risikoanalyse und der Risikoevaluierung gegebenenfalls mehrfach durchlaufen werden, bis ein ausreichender Detaillierungsgrad für die Erkennung von Gefährdungen erreicht ist.*

[G 1] Selbst wenn ein Risiko auf einem akzeptablen Niveau kontrolliert wird, kann der Vorschlagende beschließen, dass eine detailliertere Gefährdungsermittlung notwendig ist. Ein Grund dafür könnte sein, dass die Durchführung einer detaillierteren Gefährdungsermittlung zu kosteneffektiveren Sicherheitsmaßnahmen für die Risikokontrolle führen dürfte.

*2.2.6. Wird zur Risikokontrolle auf anerkannte Regeln der Technik oder auf ein Referenzsystem zurückgegriffen, kann die Gefährdungsermittlung beschränkt werden auf:*

*(a) die Überprüfung der Relevanz der anerkannten Regeln der Technik bzw. des Referenzsystems.*
*(b) die Ermittlung der Abweichungen von den anerkannten Regeln der Technik bzw. vom Referenzsystem.*

[G 1] Eine zusätzliche Erläuterung erscheint nicht notwendig.



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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. Zugrundelegung der anerkannten Regeln der Technik und Risikoevaluierung

*2.3.1. Der Vorschlagende untersucht mit Unterstützung anderer beteiligter Akteure und auf der Grundlage der unter Ziffer 2.3.2 genannten Anforderungen, ob eine oder mehrere Gefährdungen durch die Anwendung der relevanten anerkannten Regeln der Technik angemessen abgedeckt werden.*

[G 1] Eine zusätzliche Erläuterung erscheint nicht notwendig.

*2.3.2. Die anerkannten Regeln der Technik müssen mindestens folgende Anforderungen erfüllen:*

*(a) Sie müssen im Eisenbahnsektor allgemein anerkannt sein. Ist dies nicht der Fall, müssen sie begründet werden und für die Bewertungsstelle akzeptabel sein;*
*(b) Sie müssen für die Kontrolle der betreffenden Gefährdungen in dem System, das der Bewertung unterzogen wird, relevant sein;*
*(c) Sie müssen für alle Akteure, die sie anwenden wollen, öffentlich zugänglich sein.*

[G 1] Eine zusätzliche Erläuterung erscheint nicht notwendig.

*2.3.3. In Fällen, in denen gemäß der Richtlinie 2008/57/EG die Einhaltung von TSI verlangt wird und die relevanten TSI nicht das durch diese Verordnung vorgeschriebene Risikomanagementverfahren vorsehen, können die TSI als anerkannte Regeln der Technik für die Kontrolle von Gefährdungen betrachtet werden, sofern die unter Ziffer 2.3.2 Buchstabe c genannte Anforderung erfüllt ist.*

[G 1] Eine zusätzliche Erläuterung erscheint nicht notwendig.

*2.3.4. Nationale Vorschriften, die gemäß Artikel 8 der Richtlinie 2004/49/EG und Artikel 17 Absatz 3 der Richtlinie 2008/57/EG notifiziert werden, können als anerkannte Regeln der Technik betrachtet werden, sofern die unter Ziffer 2.3.2 genannten Anforderungen erfüllt sind.*

[G 1] Eine zusätzliche Erläuterung erscheint nicht notwendig.

*2.3.5. Wenn eine oder mehrere Gefährdungen durch anerkannte Regeln der Technik kontrolliert werden, die die Anforderungen unter Ziffer 2.3.2 erfüllen, sind die mit diesen Gefährdungen verbundenen Risiken als vertretbar anzusehen. Dies bedeutet:*

*(a) dass die betreffenden Risiken nicht weiter analysiert werden müssen;*
*(b) dass die Anwendung der anerkannten Regeln der Technik im Gefährdungsprotokoll als Sicherheitsanforderung in Bezug auf die jeweiligen Gefährdungen erfasst wird.*

[G 1] Eine zusätzliche Erläuterung erscheint nicht notwendig.



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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

*2.3.6. Entspricht der verfolgte Ansatz den relevanten anerkannten Regeln der Technik nicht in vollem Umfang, hat der Vorschlagende nachzuweisen, dass der stattdessen verfolgte Ansatz mindestens dasselbe Sicherheitsniveau gewährleistet.*

[G 1] Eine zusätzliche Erläuterung erscheint nicht notwendig.

*2.3.7. Kann das aus einer bestimmten Gefährdung erwachsende Risiko nicht durch Anwendung anerkannter Regeln der Technik auf ein akzeptables Maß eingedämmt werden, werden zusätzliche Sicherheitsmaßnahmen ermittelt, bei denen einer der beiden anderen Risikoakzeptanzgrundsätze zur Anwendung kommt.*

[G 1] Eine zusätzliche Erläuterung erscheint nicht notwendig.

*2.3.8. Erfolgt die Kontrolle sämtlicher Gefährdungen durch Anwendung der anerkannten Regeln der Technik, kann das Risikomanagementverfahren beschränkt werden auf:*

*(a) die Gefährdungsermittlung gemäß Abschnitt 2.2.6;*
*(b) die Aufnahme eines Vermerks über die Anwendung der anerkannten Regeln der Technik im Gefährdungsprotokoll gemäß Abschnitt 2.3.5;*
*(c) die Dokumentation der Anwendung des Risikomanagementverfahrens gemäß Abschnitt 5;*
*(d) eine unabhängige Bewertung gemäß Artikel 6.*

[G 1] Eine zusätzliche Erläuterung erscheint nicht notwendig.

## 2.4. Heranziehung eines Referenzsystems und Risikoevaluierung

*2.4.1. Der Vorschlagende untersucht mit Unterstützung anderer beteiligter Akteure, ob eine oder mehrere Gefährdungen durch ein ähnliches System abgedeckt werden, das als Referenzsystem herangezogen werden könnte.*

[G 1] Weitere Informationen zu diesen Grundsätzen finden sich in Abschnitt § 8 des Leitfadens EN 50 126-2 {Ref. 9}.

*2.4.2. Ein Referenzsystem muss mindestens folgende Anforderungen erfüllen:*

*(a) Es hat sich bereits in der Praxis bewährt, weil es ein akzeptables Sicherheitsniveau gewährleistet, und es würde in dem Mitgliedstaat, in dem die Änderung eingeführt werden soll, nach wie vor eine Genehmigung erhalten;*
*(b) Es verfügt über ähnliche Funktionen und Schnittstellen wie das System, das der Bewertung unterzogen wird;*
*(c) Es wird unter ähnlichen Betriebsbedingungen eingesetzt wie das System, das der Bewertung unterzogen wird;*
*(d) Es wird unter ähnlichen Umweltbedingungen eingesetzt wie das System, das der Bewertung unterzogen wird.*

[G 1] Beispielsweise könnte ein altes Zugsteuerungs-/Zugsicherungssystem, das im praktischen Einsatz ein akzeptables Sicherheitsniveau nachgewiesen hat, durch ein anderes System mit



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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

neuerer Technologie und besserem Sicherheitsgrad ersetzt werden. Es ist also geboten, bei Anwendung eines Referenzsystems jedes Mal erneut zu prüfen, ob es weiterhin für den entsprechenden Akzeptanzgrad geeignet ist.

[G 2] Da bestimmte Aspekte der Tunnelsicherheit oder der Sicherheit von Gefahrguttransporten spezifischer Art und damit von Betriebs- und Umweltbedingungen abhängig sein könnten, ist zum Beispiel bei jedem einzelnen Projekt eine Prüfung notwendig, ob das System unter den gleichen Bedingungen verwendet wird.

*2.4.3. Erfüllt ein Referenzsystem die unter Ziffer 2.4.2 genannten Anforderungen, gilt für das zu bewertende System Folgendes:*

*(a) Die Risiken, die mit den vom Referenzsystem abgedeckten Gefährdungen verbunden sind, werden als vertretbar angesehen;*
*(b) Die Sicherheitsanforderungen im Falle von Gefährdungen, die von dem Referenzsystem abgedeckt werden, können aus Sicherheitsanalysen oder aus einer Bewertung der Sicherheitsdokumentation des Referenzsystems abgeleitet werden;*
*(c) Diese Sicherheitsanforderungen werden im Gefährdungsprotokoll als in Bezug auf die jeweiligen Gefährdungen geltende Sicherheitsanforderungen erfasst.*

[G 1] Eine zusätzliche Erläuterung erscheint nicht notwendig.

*2.4.4. Weicht das zu bewertende System vom Referenzsystem ab, muss aus der Risikoevaluierung hervorgehen, dass das bewertete System mindestens das gleiche Sicherheitsniveau erreicht wie das Referenzsystem. Die Risiken, die mit den vom Referenzsystem abgedeckten Gefährdungen verbunden sind, werden in diesem Fall als vertretbar angesehen.*

[G 1] Weitere Informationen zu Ähnlichkeitsanalysen finden sich in Abschnitt § 8.1.3. des Leitfadens EN 50 126-2 {Ref. 9}.

*2.4.5. Kann nicht nachgewiesen werden, dass das System das gleiche Sicherheitsniveau erreicht wie das Referenzsystem, werden für die Abweichungen zusätzliche Sicherheitsmaßnahmen ermittelt, bei denen einer der beiden anderen Risikoakzeptanzgrundsätze zur Anwendung kommt.*

[G 1] Eine zusätzliche Erläuterung erscheint nicht notwendig.

## 2.5. Explizite Risikoabschätzung und -evaluierung

*2.5.1. Wenn die Gefährdungen nicht von einem der beiden Risikoakzeptanzgrundsätze abgedeckt werden, die in den Abschnitten 2.3 und 2.4 beschrieben sind, wird der Nachweis über die Vertretbarkeit des Risikos in Form einer expliziten Risikoabschätzung und –evaluierung erbracht. Risiken, die sich aus diesen Gefährdungen ergeben, werden unter Berücksichtigung der vorhandenen Sicherheitsmaßnahmen quantitativ oder qualitativ beurteilt.*


European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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] Eine zusätzliche Erläuterung erscheint nicht notwendig.

*2.5.2. Die Vertretbarkeit der geschätzten Risiken wird anhand von Risikoakzeptanzkriterien bewertet, die aus in gemeinschaftlichen Rechtsvorschriften oder notifizierten nationalen Vorschriften niedergelegten gesetzlichen Anforderungen abgeleitet werden oder darauf beruhen. In Abhängigkeit von den Risikoakzeptanzkriterien kann die Vertretbarkeit des Risikos entweder für jede Gefährdung einzeln oder insgesamt für die Kombination aller bei der expliziten Risikoabschätzung berücksichtigten Gefährdungen bewertet werden.*

*Wenn das geschätzte Risiko nicht vertretbar ist, werden zusätzliche Sicherheitsmaßnahmen ermittelt und eingeführt, damit das Risiko auf ein vertretbares Maß gesenkt werden kann.*

[G 1] Für eine Beurteilung, ob die Risiken aus dem zu bewertenden System akzeptabel oder nicht akzeptabel sind, werden Risikoakzeptanzkriterien benötigt (siehe die Boxen „Risikoevaluierung“ in Abbildung 1). Dabei kann es sich entweder um implizite oder um explizite Risikoakzeptanzkriterien handeln:

(a) Implizite Risikoakzeptanzkriterien: Risiken, die gemäß den Abschnitten 2.3.5 und 2.4.3 durch Anwendung anerkannter Regeln der Technik und durch Vergleich mit Referenzsystemen abgedeckt werden, werden implizit als akzeptabel betrachtet, vorausgesetzt dass (siehe gepunkteten Kreis in Abbildung 1):

(1) die Anwendungsbedingungen der anerkannten Regeln der Technik nach Abschnitt 2.3.2 eingehalten werden; bzw.
(2) die Verwendungsbedingungen eines Referenzsystems nach Abschnitt 2.4.2 eingehalten werden.

(b) Explizite Risikoakzeptanzkriterien: Für eine Beurteilung, ob das bzw. die durch Anwendung einer expliziten Risikoabschätzung kontrollierten Risiken akzeptabel sind oder nicht, werden explizite Risikoakzeptanzkriterien benötigt (siehe Volllinienkreis in Abbildung 1 beim dritten Grundsatz). Diese können auf unterschiedlichen Ebenen eines Eisenbahnsystems festgelegt werden. Sie können als „Kriterienpyramide“ angesehen werden (siehe Abbildung 9) beginnend mit den Risikoakzeptanzkriterien der oberen Ebene (ausgedrückt beispielsweise als gesellschaftliches oder individuelles Risiko) bis hinunter zu den Teilsystemen und Komponenten (für die Behandlung technischer Systeme), einschließlich der menschlichen Bediener in den Betriebs- und Instandhaltungsaktivitäten des Systems und der Teilsysteme. Die Risikoakzeptanzkriterien leisten zwar einen Beitrag zur Erreichung der Systemsicherheit und sind deshalb mit den gemeinsamen Sicherheitszielen (CST) und nationalen Referenzwerten (NRV) verknüpft, aber der Aufbau eines mathematischen Modells zur Beschreibung ihrer Wechselwirkungen ist sehr schwer: Näheres dazu in {Ref. 12}.
Die Ebene, auf der die expliziten Risikoakzeptanzkriterien festgelegt werden, muss der Bedeutung und Komplexität der signifikanten Änderung entsprechen. Beispielsweise ist es bei Änderung eines Achsentyps in Schienenfahrzeugen nicht notwendig, das Risiko des gesamten Eisenbahnsystems zu evaluieren. Die Festlegung der Risikoakzeptanzkriterien kann sich ganz auf die Fahrzeugsicherheit konzentrieren. Hingegen sollten große Änderungen oder Ergänzungen in einem bestehenden Eisenbahnsystem nicht isoliert anhand des Sicherheitsgrades hinzukommender einzelner Funktionen oder Änderungen beurteilt werden. Hier sollte auch auf der Ebene des Eisenbahnsystems verifiziert werden, dass die Änderung im Ganzen akzeptabel ist.



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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

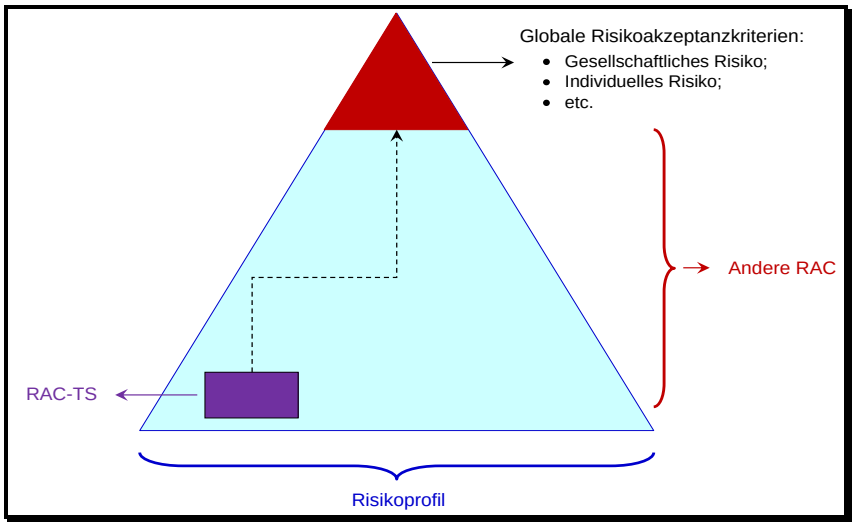


***Abbildung 9 : Pyramide der Risikoakzeptanzkriterien (RAC)***

[G 2] Die weitere Arbeit der Agentur an den Risikoakzeptanzkriterien wird die zur Förderung der gegenseitigen Anerkennung notwendigen expliziten Risikoakzeptanzkriterien zwischen den Mitgliedsstaaten harmonisieren. In dieses Dokument werden zusätzliche Informationen eingearbeitet, sobald diese vorliegen.

[G 3] Bis dahin können Risiken beispielsweise unter Zuhilfenahme der Risikomatrix evaluiert werden, die in Abschnitt § 4.6 der Norm EN 50 126-1 {Ref. 8} zu finden ist. Auch andere Arten geeigneter Kriterien können eingesetzt werden, soweit davon ausgegangen werden kann, dass diese Kriterien eine akzeptable Sicherheitsstufe im betreffenden Fall erzielen.

*2.5.3. Wird das mit einer Gefährdung oder mit einer Kombination mehrerer Gefährdungen verbundene Risiko als vertretbar angesehen, werden die ermittelten Sicherheitsmaßnahmen im Gefährdungsprotokoll erfasst.*

[G 1] Eine zusätzliche Erläuterung erscheint nicht notwendig.

*2.5.4. Wenn sich aus Ausfällen technischer Systeme Gefährdungen ergeben, die nicht von den anerkannten Regeln der Technik oder der Verwendung eines Referenzsystems abgedeckt werden, gilt für die Planung des technischen Systems folgendes Risikoakzeptanzkriterium:*

*Bei technischen Systemen, bei denen im Falle eines funktionellen Ausfalls von unmittelbaren katastrophalen Folgen auszugehen ist, muss das damit verbundene Risiko nicht weiter eingedämmt werden, wenn die Ausfallrate pro Betriebsstunde kleiner oder gleich $10^{-9}$ ist.*

[G 1] Weitere Einzelheiten über RAC-TS sowie dazu, für welche Aspekte und Funktionen des technischen Systems das Kriterium gilt, finden sich in einer separaten, mit dem vorliegenden Dokument verbundenen Mitteilung der Agentur: siehe Abschnitt A.3 von Alage A und Referenzdokument {Ref. 11}.



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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. Unbeschadet des in Artikel 8 der Richtlinie 2004/49/EG vorgesehenen Verfahrens kann im Interesse der Aufrechterhaltung eines nationalen Sicherheitsniveaus im Wege einer nationalen Vorschrift ein strengeres Kriterium festgelegt werden. Werden jedoch zusätzliche Genehmigungen für die Inbetriebnahme von Fahrzeugen verlangt, gelten die Verfahren der Artikel 23 und 25 der Richtlinie 2008/57/EG.*

[G 1] Eine zusätzliche Erläuterung erscheint nicht notwendig.

*2.5.6. Wird ein technisches System unter Zugrundlegung des unter Ziffer 2.5.4 festgelegten Kriteriums einer Ausfallrate von $10^{-9}$ entwickelt, findet das Prinzip der gegenseitigen Anerkennung gemäß Artikel 7 Absatz 4 dieser Verordnung Anwendung.*

*Weist der Vorschlagende jedoch nach, dass das nationale Sicherheitsniveau im betreffenden Mitgliedstaat sich auch bei einer Ausfallrate pro Betriebsstunde von über $10^{-9}$ aufrechterhalten lässt, kann das entsprechende Kriterium vom Vorschlagenden im betreffenden Mitgliedstaat angewandt werden.*

[G 1] Eine zusätzliche Erläuterung erscheint nicht notwendig.

*2.5.7. Die explizite Risikoabschätzung und -evaluierung muss mindestens folgende Anforderungen erfüllen:*

*(a) Die für die explizite Risikoabschätzung eingesetzten Methoden geben das System, das der Bewertung unterzogen wird, und seine Parameter (einschließlich aller Betriebsmodi) korrekt wieder;*

*(b) Die Ergebnisse sind ausreichend präzise, um als solide Entscheidungshilfe dienen zu können. Das bedeutet, dass geringfügige Änderungen bei den zugrunde gelegten Annahmen oder Voraussetzungen nicht zu erheblich unterschiedlichen Anforderungen führen dürfen.*

[G 1] Eine zusätzliche Erläuterung erscheint nicht notwendig.



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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. NACHWEIS DER ERFÜLLUNG DER SICHERHEITS-ANFORDERUNGEN

*3.1. Bevor die Sicherheit einer Änderung bescheinigt wird, ist – unter Aufsicht des Vorschlagenden – die Erfüllung der sich aus der Phase der Risikobewertung ergebenden Sicherheitsanforderungen nachzuweisen.*

[G 1] Wie in den Punkten [G 3] bis [G 6] in Abschnitt 2.1.1 erläutert, beinhaltet der „Nachweis der Übereinstimmung des Systems mit den Sicherheitsanforderungen“ die Phasen „6 bis 10“ der V-Darstellung nach CENELEC (siehe BOX 3 in Abbildung 5). Siehe Punkt [G 3] in Abschnitt 2.1.1.

[G 2] Siehe auch Punkt [G 4] in Abschnitt 2.1.1 des vorliegenden Dokuments.

*3.2. Dieser Nachweis wird von jedem der für die Erfüllung der gemäß Ziffer 1.1.5 bestimmten Sicherheitsanforderungen verantwortlichen Akteure erbracht.*

[G 1] Ein Beispiel für Sicherheitsbewertungen und Sicherheitsanalysen, die sich auf Teilsystemebene durchführen lassen, sind Kausalanalysen: siehe Abbildung 10. Es können aber auch andere Methoden herangezogen werden, um nachzuweisen, dass die Teilsysteme die Eingangs-Sicherheitsanforderungen erfüllen.

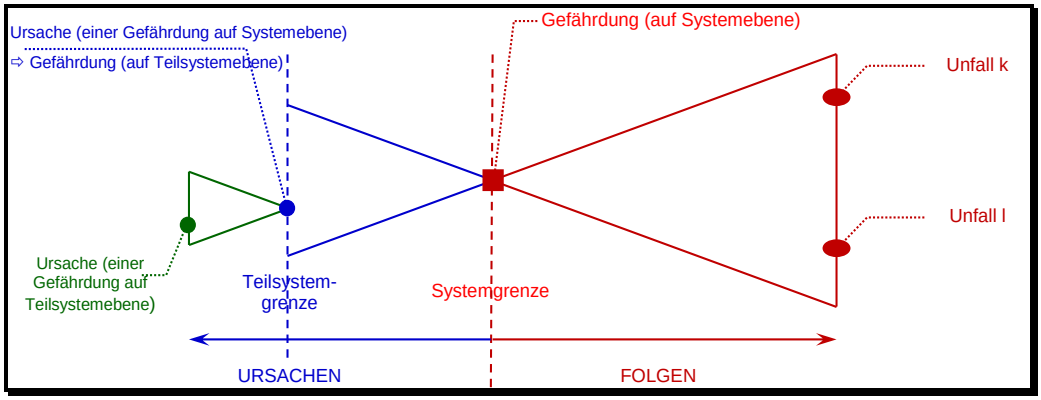


***Abbildung 10 : Bild A.4 der Norm EN 50 129: Gefährdungsdefinition in Bezug auf die Systemgrenzen***

[G 2] Die hierarchische Strukturierung von Gefährdungen und Gefährdungsursachen bezüglich von Systemen und Teilsystemen kann für jede weitere untergeordnete Phase der V-Darstellung von CENELEC nach Abbildung 5 wiederholt werden. Die Aktivitäten der Gefährdungsermittlung und Kausalanalyse (oder einer beliebigen anderen relevanten Methode) sowie die Verwendung von anerkannten Regeln der Technik, ähnlichen Referenzsystemen und expliziten Analysen und Beurteilungen können auch für jede Phase des Systementwicklungszyklus wiederholt werden, um von den auf Teilsystemebene ermittelten Sicherheitsmaßnahmen die von der nächsten Phase zu erfüllenden Sicherheitsanforderungen abzuleiten. Dies ist in Abbildung 11 dargestellt.

[G 3] Siehe auch Punkt [G 4] in Abschnitt 2.1.1 des vorliegenden Dokuments.


European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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

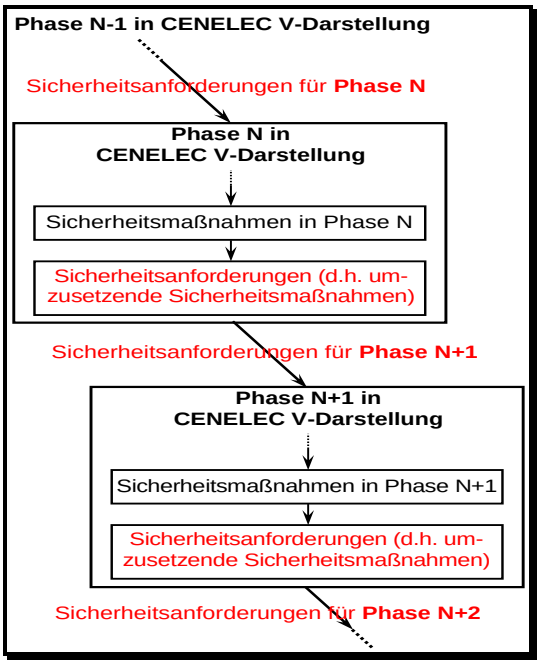


***Abbildung 11 : Ableitung der Sicherheitsanforderungen für Phasen nachgeordneter Ebenen***

*3.3. Die für den Nachweis der Erfüllung der Sicherheitsanforderungen gewählte Vorgehensweise sowie der Nachweis selbst werden einer unabhängigen Bewertung durch eine Bewertungsstelle unterzogen.*

[G 1] Alle Aktivitäten, die in der BOX 3[(12)] der V-Darstellung der CENELEC in Abbildung 5 dargestellt sind, werden deshalb auch unabhängig bewertet.

[G 2] Die Art und Detailliertheit der von den Bewertungsstellen durchgeführten unabhängigen Bewertung (z. B. detaillierte oder makroskopische Bewertung) wird in den Erläuterungen von Artikel 6 behandelt.

*3.4. Eine Unangemessenheit der Sicherheitsmaßnahmen, durch die die Sicherheitsanforderungen erfüllt werden sollen, oder eine Gefährdung, die beim Nachweis der Erfüllung der Sicherheitsanforderungen entdeckt wird, hat gemäß Abschnitt 2 eine erneute Bewertung und Evaluierung der damit verbundenen Risiken durch den Vorschlagenden zur Folge. Die neuen Gefährdungen werden gemäß Abschnitt 4 im Gefährdungsprotokoll festgehalten.*

[G 1] Beispielsweise kann die Art der Brandbekämpfung zu einer neuen Gefährdung (Erstickungsgefahr) führen, die neue Sicherheitsanforderungen verlangt (z. B. ein spezielles Verfahren für die Evakuierung der Passagiere). Ein anderes Beispiel ist die Verwendung von

(12) *Wie die Aktivitäten von CSM und Abbildung 5 (d. h. Bild 10 von CENELEC 50 126 V-Darstellung) einander entsprechen, ist in Abschnitt 2.1.1 beschrieben. Speziell in Punkt [G 3] von Abschnitt 2.1.1 werden die CENELEC-Aktivitäten aufgelistet, die die CSM-Phase „Nachweis der Übereinstimmung des Systems mit den Sicherheitsanforderungen“ umfasst.*


European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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

vorgespanntem Sicherheitsglas, um zu vermeiden, dass bei Unfällen Fenster zu Bruch gehen und Passagiere durch Glassplitter verletzt oder durch die Fenster aus dem Zug geschleudert werden. Daraus leitet sich als neue Gefährdung ab, dass in Notsituationen das Verlassen des Zuges durch die Fenster weitaus schwieriger ist, woraus Sicherheitsanforderungen dahingehend entstehen können, dass einige Fenster zur Ermöglichung des Fluchtwegs speziell konstruiert sein müssen.

[G 2] Beispiel für eine betriebliche Änderung: Es wird gefordert, dass Gefahrguttransporte nicht auf Strecken durch dicht besiedelte Gebiete vorgenommen werden dürfen. Stattdessen soll der Gefahrguttransport auf einer alternativen Route mit Tunneln erfolgen, was andere Arten von Gefährdungen verursacht.

[G 3] Weitere Beispiele neuer Gefährdungen, die im Zuge des Nachweises der Systemübereinstimmung mit den Sicherheitsanforderungen eventuell ermittelt werden, finden sich in Anhang A.4.3 der Norm EN 50 129.



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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. GEFÄHRDUNGSMANAGEMENT

## 4.1. Gefährdungsmanagementverfahren

*4.1.1. Im Verlauf der Planung und Durchführung werden – bis zur Genehmigung der Änderung oder der Vorlage des Sicherheitsbewertungsberichts – vom Vorschlagenden Gefährdungsprotokolle angelegt bzw. aktualisiert (sofern sie bereits bestehen). Im Gefährdungsprotokoll werden die Fortschritte in der Überwachung der aus den ermittelten Gefährdungen resultierenden Risiken aufgezeichnet. Gemäß Anhang III Ziffer 2 Buchstabe g der Richtlinie 2004/49/EG wird das Gefährdungsprotokoll, sobald das System genehmigt und in Betrieb genommen wurde, von dem Infrastrukturbetreiber oder dem Eisenbahnunternehmen, der bzw. das für den Betrieb des der Bewertung unterzogenen Systems verantwortlich ist, als integraler Bestandteil seines Sicherheitsmanagementsystems weitergeführt.*

[G 1] Die Verwendung eines Gefährdungsprotokolls für die Registrierung, Verwaltung und Kontrolle sicherheitsrelevanter Informationen ist auch in den Normen CENELEC 50 126-1 {Ref. 8} und 50 129 {Ref. 7} empfohlen.

[G 2] Je nach Komplexität des Systems, könnte beispielsweise ein Akteur ein oder mehrere Gefährdungsprotokolle führen. In beiden Fällen ist/sind das/die Gefährdungsprotokoll(e) von der/den Bewertungsstelle(n) unabhängig zu bewerten. Zum Beispiel wäre eine mögliche Lösung:

(a) Führen eines „internen Gefährdungsprotokolls“ zur Verwaltung aller internen Sicherheitsanforderungen, die für das Teilsystem gelten, für das der Akteur verantwortlich ist. Größe und Umfang der Verwaltungsarbeit hängen von der Struktur und natürlich von der Komplexität des Teilsystems ab. Da das Gefährdungsprotokoll nur internen Verwaltungszwecken dient, muss es nicht an andere Akteure übermittelt werden. Das interne Gefährdungsprotokoll enthält alle ermittelten Gefährdungen, die kontrolliert werden, sowie die damit verbundenen Sicherheitsmaßnahmen, die validiert werden;

(b) Führen eines „externen Gefährdungsprotokolls“, um Gefährdungen und verbundene Sicherheitsmaßnahmen (die der Akteur allein nicht vollständig implementieren kann) gemäß Abschnitt 1.2.2 an andere Akteure zu übertragen. Gewöhnlich ist dieses zweite Gefährdungsprotokoll nicht so umfangreich und erfordert weniger Verwaltungsaufwand (siehe Beispiel in Abschnitt C.16.4 von Alage C).

[G 3] Falls das Führen mehrerer Gefährdungsprotokolle kompliziert erscheint, besteht eine andere Lösung darin, alle in den Punkten (a) und (b) oben genannten Gefährdungen und verbundenen Sicherheitsmaßnahmen in einem einzigen Gefährdungsprotokoll zu verwalten, aber die Möglichkeit vorzusehen, daraus zwei verschiedene Gefährdungsberichte zu erstellen (siehe Beispiel in Abschnitt C.16.3 von Alage C):

(a) einen internen Gefährdungsbericht, der u. U. nicht notwendig ist, wenn das Gefährdungsprotokoll zur Sicherung der unabhängigen Bewertung gut durchstrukturiert ist;
(b) einen externen Gefährdungsbericht für die Übertragung von Gefährdungen und verbundenen Sicherheitsmaßnahmen an andere Akteure.

[G 4] Wie in Abschnitt 4.2 erläutert, gilt am Projektende bei Abnahme des Systems:

(a) Alle an andere Akteure übertragenen Gefährdungen werden in dem externen Gefährdungsprotokoll desjenigen Akteurs kontrolliert, der die Gefährdungen überträgt. Da diese in die internen Gefährdungsprotokolle der anderen Akteure überführt und dort



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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

geführt werden, müssen sie während des (Teil-)Systemlebenszyklus durch den entsprechenden Akteur nicht weiter verwaltet werden;

(b) alle verbundenen Sicherheitsmaßnahmen sollten jedoch aus den in Punkt [G 9] von Abschnitt 4.2 genannten Gründen im Gefährdungsprotokoll nicht validiert werden. Die Organisation, die die Verwendungsbeschränkungen exportiert, sollte zweckdienlicherweise in ihrem Gefährdungsprotokoll klar und deutlich darauf hinweisen, dass die verbundenen Sicherheitsmaßnahmen nicht validiert wurden.

[G 5] Hingegen werden alle internen Gefährdungsprotokolle über den gesamten (Teil-)Systemlebenszyklus hinweg geführt und verwaltet. Dies ermöglicht die Verfolgbarkeit des erzielten Fortschritts bei der Überwachung der mit den ermittelten Gefährdungen verbundenen Risiken im Zuge des Betriebs und der Instandhaltung des (Teil-)Systems, d. h. auch nach seiner Inbetriebsetzung: Siehe BOX 4 in der V-Darstellung CENELEC in Abbildung 5.

*4.1.2. Im Gefährdungsprotokoll sind alle Gefährdungen sowie alle entsprechenden Sicherheitsmaßnahmen und Systemannahmen aufgeführt, die im Zuge des Risikobewertungsverfahrens identifiziert wurden. Insbesondere enthält das Protokoll einen eindeutigen Verweis auf die Herkunft und die gewählten Risikoakzeptanzgrundsätze sowie genaue Angaben zu den Akteuren, die für die Kontrolle der einzelnen Gefährdungen verantwortlich sind.*

[G 1] Die von anderen Akteuren stammenden Informationen über Gefährdungen und verbundene Sicherheitsmaßnahmen (siehe Abschnitt 1.2.2) umfassen auch alle Annahmen[13] und Verwendungsbeschränkungen[15] (auch bezeichnet als sicherheitsbezogene Anwendungsbedingungen), die für die verschiedenen Teilsysteme sowie generischen Anwendungs- und Produktsicherheitsnachweise gelten, die von den Herstellern, soweit relevant, vorgelegt werden.

[G 2] Ein mögliches Beispiel für die Struktur eines Gefährdungsprotokolls ist in Abschnitt C.16 von Alage C beschrieben.

## 4.2. Informationsaustausch

*Alle Gefährdungen und damit zusammenhängenden Sicherheitsanforderungen, die nicht durch einen Akteur allein kontrolliert werden können, werden einem weiteren beteiligten Akteur gemeldet, damit gemeinsam eine angemessene Lösung gefunden werden kann. Die Gefährdungen, die im Gefährdungsprotokoll des Akteurs aufgezeichnet sind, der die Zuständigkeit auf einen anderen Akteur überträgt, gelten nur dann als „kontrolliert", wenn die Evaluierung der Risiken im Zusammenhang mit diesen Gefährdungen von dem anderen Akteur vorgenommen wird und sich alle Beteiligten auf eine Lösung einigen.*

(13) *Nähere Erläuterungen zur Terminologie der „generischen Nachweise" in Bezug auf „generisches Produkt" und „generische Anwendung" sowie „Annahmen und Verwendungsbeschränkungen" finden sich in Punkt [G 5] in Abschnitt 1.1.5 und den Fußnoten [9] und [10] auf Seite 30 des vorliegenden Dokuments".*


European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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] Beispielsweise kann beim odometrischen Teilsystem der fahrzeugseitigen ETCS-Ausrüstung der Hersteller im Labor die Algorithmen durch Simulierung der theoretischen Signale validieren, die von der verbundenen odometrischen Sensorik erzeugt werden könnten. Die komplette Validierung des odometrischen Teilsystems erfordert jedoch die Hilfe von EBU und FB zur Durchführung der Validierung mit Einsatz eines tatsächlichen Zuges mit tatsächlichem Rad-Schiene-Kontakt.

[G 2] Andere Beispiele wären die vom Hersteller an die Eisenbahnunternehmen vorgenommenen Übertragungen betrieblicher oder instandhaltungsbezogener Sicherheitsmaßnahmen für technische Ausrüstungen. Diese Sicherheitsmaßnahmen müssen durch das Eisenbahnunternehmen implementiert werden.

[G 3] Damit diese Gefährdungen, verbundenen Sicherheitsmaßnahmen und Risiken von den beteiligten Organisationen gemeinsam neubewertet werden können, ist es hilfreich, wenn die Organisation, die diese Gefährdungen, Sicherheitsmaßnahmen und Risiken ermittelt hat, alle für das eindeutige Verständnis des Problems notwendigen Erläuterungen mitliefert. So könnte es sein, dass der ursprüngliche Wortlaut der Gefährdungen, Sicherheitsmaßnahmen und Risiken geändert werden muss, damit diese verständlich werden, ohne dass eine erneute gemeinsame Erörterung notwendig ist. Die gemeinsame Neubewertung der Gefährdungen könnte zur Ermittlung neuer Sicherheitsmaßnahmen führen.

[G 4] Der für die Implementierung, Verifizierung und Validierung der an ihn übertragenen oder neuen Sicherheitsmaßnahmen verantwortliche Akteur verzeichnet alle entsprechenden Gefährdungen mit den verbundenen Sicherheitsmaßnahmen (sowohl die importierten als auch die gemeinsam ermittelten) in seinem eigenen Gefährdungsprotokoll.

[G 5] Wenn eine Sicherheitsmaßnahme nicht vollständig validiert ist, muss eine eindeutige Verwendungsbeschränkung (z. B. betriebliche Minderungsmaßnahmen) ausgearbeitet und im Gefährdungsprotokoll festgehalten werden. Es ist faktisch möglich, dass technische/konstruktive Sicherheitsmaßnahmen:

(a) nicht ordnungsgemäß implementiert werden oder
(b) nicht vollständig implementiert werden oder
(c) absichtlich nicht implementiert werden, beispielsweise weil andere als im Gefährdungsprotokoll verzeichnete Sicherheitsmaßnahmen implementiert werden (z. B. aus Kostengründen). Da solche Sicherheitsmaßnahmen nicht validiert werden, müssen sie im Gefährdungsprotokoll eindeutig kenntlich gemacht werden. Und es ist zu belegen/begründen, warum die ersatzweise implementierten Sicherheitsmaßnahmen[(14)] geeignet sind, sowie der Nachweis zu führen, dass das System mit den ersetzenden Sicherheitsmaßnahmen die Sicherheitsanforderungen erfüllt;
(d) usw.

In diesen Fällen können die entsprechenden technischen/konstruktiven Sicherheitsmaßnahmen im Zuge des Gefährdungsmanagements nicht verifiziert und validiert werden. Die diesbezügliche(n) Gefährdung(en) und Sicherheitsmaßnahmen müssen dann im Gefährdungsprotokoll offen bleiben, damit vermieden wird, dass die Sicherheitsmaßnahmen über die Anwendung des Risikoakzeptanzgrundsatzes „ähnliches Referenzsystem“ fälschlicherweise auf andere Systeme übertragen werden.

[G 6] Gewöhnlich werden die „nicht ordnungsgemäß“ und/oder „nicht vollständig“ implementierten Sicherheitsmaßnahmen im Systemlebenszyklus frühzeitig erkannt und vor der

(14) *Wenn andere als die ursprünglich angegebenen Sicherheitsmaßnahmen implementiert werden, sind auch diese abweichenden Sicherheitsmaßnahmen in das Gefährdungsprotokoll einzutragen.*



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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

Systemabnahme korrigiert. Falls die Erkennung jedoch für eine ordnungsgemäße und vollständige Implementierung technischer Sicherheitsmaßnahmen zu spät erfolgt, muss die für die Implementierung und Verwaltung zuständige Organisation eindeutige Verwendungsbeschränkungen für das zu bewertende System ermitteln und im Gefährdungsprotokoll eintragen. Diese Verwendungsbeschränkungen stellen oftmals betriebliche Anwendungszwänge für das zu bewertende System dar.

[G 7] Es könnte auch zweckdienlich sein, im Gefährdungsprotokoll festzuhalten, ob die verbundenen Sicherheitsmaßnahmen in einer späteren Phase des Systemlebenszyklus noch ordnungsgemäß implementiert werden oder ob das System weiter mit den ermittelten Verwendungsbeschränkungen verwendet wird. Nützlich wäre auch die Aufnahme einer Begründung in das Gefährdungsprotokoll, warum die verbundenen technischen Sicherheitsmaßnahmen nicht ordnungsgemäß/vollständig implementiert werden.

[G 8] Der die Verwendungsbeschränkungen erhaltende Akteur:

(a) importiert all diese Beschränkungen in sein eigenes Gefährdungsprotokoll;
(b) sorgt dafür, dass die Verwendungsbedingungen des zu bewertenden Systems alle Verwendungsbeschränkungen einhalten;
(c) verifiziert und validiert die Einhaltung dieser Verwendungsbeschränkungen durch das zu bewertende System.

[G 9] Abhängig von den vereinbarten Entscheidungen der beteiligten Organisationen:

(a) Entweder werden die entsprechenden technischen Sicherheitsmaßnahmen zu einem späteren Zeitpunkt ordnungsgemäß im Design implementiert.
Die die Verwendungsbeschränkungen exportierende Organisation verfolgt weiterhin die ordnungsgemäße technische Umsetzung der verbundenen Sicherheitsmaßnahmen. Demzufolge können im Gefährdungsprotokoll dieser Organisation die entsprechenden Sicherheitsmaßnahmen so lange nicht validiert und die mit ihnen verbundenen Gefährdungen so lange nicht kontrolliert werden, bis die entsprechenden technischen Sicherheitsmaßnahmen vollständig implementiert sind. Das ist auch dann weiter zu gewährleisten, wenn zwischenzeitlich die exportierten Verwendungsbeschränkungen eingerichtet wurden.

(b) Oder es werden die entsprechenden technischen Sicherheitsmaßnahmen später nicht im Design implementiert. Das System verwendet dann die verbundenen Verwendungsbeschränkungen während seines gesamten Lebenszyklus. In diesem Falle kann wie folgt verfahren werden:

(1) Die die Verwendungsbeschränkungen exportierende Organisation trägt die verbundenen Sicherheitsmaßnahmen nicht als „validiert“ in ihr Gefährdungsprotokoll ein. So werden die jeweiligen Sicherheitsbedenken nicht übersehen, sollte das System als Referenzsystem in anderen Projekten verwendet werden. Selbst wenn ein anderer Akteur bereit ist, die verbundenen Risiken abweichend zu verwalten, ist es günstig, wenn die die Verwendungsbeschränkungen exportierende Organisation in ihrem Gefährdungsprotokoll eindeutig darauf hinweist, dass die verbundenen Sicherheitsmaßnahmen nicht validiert wurden, oder

(2) die Systembeschreibung kann so geändert werden, dass die Verwendungsbeschränkungen fortan im Anwendungsbereich des Systems (d. h. Annahmen für das System) und in den Sicherheitsanforderungen enthalten sind. Dies ermöglicht die Kontrolle der Gefährdungen. Das bedeutet für den Fall, dass das System als Referenzsystem in einer anderen Anwendung verwendet wird:



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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) Das neue System muss unter den gleichen Bedingungen verwendet werden (d. h. es muss die mit diesen Annahmen verbundenen Verwendungs-beschränkungen erfüllen), oder

(ii) der Vorschlagende muss eine zusätzliche Risikobewertung für die Abweichungen von diesen Annahmen durchführen.



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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. DOKUMENTATION DER ANWENDUNG DES RISIKO-MANAGEMENTVERFAHRENS

*5.1. Das Risikomanagementverfahren, das für die Bewertung der Sicherheitsniveaus und der Erfüllung der Sicherheitsanforderungen angewandt wird, ist vom Vorschlagenden in einer Weise zu dokumentieren, dass einer Bewertungsstelle alle erforderlichen Nachweise über die ordnungsgemäße Anwendung des Risikomanagementverfahrens zugänglich sind. Die Bewertungsstelle hält ihre Schlussfolgerungen in einem Sicherheitsbewertungsbericht fest.*

[G 1] Das Sicherheitsmanagementsystem (SMS) von Fahrwegbetreiber und Eisenbahnunternehmen behandelt bereits diese Anforderungen. Die anderen an der signifikanten Änderung beteiligten Akteure des Eisenbahnsektors verfügen in der Regel, auch wenn das SMS nicht zwingend vorgeschrieben ist, zumindest auf der Projektebene über einen Qualitätsmanagementprozess (QMP) und/oder einen Sicherheitsmanagementprozess (SMP). Diese beiden Prozesse gründen sich auf eine strukturierte Dokumentationshierarchie entweder innerhalb des Unternehmens oder zumindest innerhalb des Projekts. Sie betreffen auch die dokumentarischen Erfordernisse des RAMS-Managements. Eine solche strukturierte Dokumentation kann grundsätzlich aus folgenden Dokumenten bestehen (siehe auch Abbildung 12):

(a) **Projektpläne** zur Beschreibung der Organisation, die für die Verwaltung einer Aktivität innerhalb eines Projekts einzurichten ist.

(b) **Projektverfahren** zur detaillierten Beschreibung der Verfahrensweise zur Ausführung einer bestimmten Aufgabe. Gewöhnlich gibt es im Unternehmen Verfahrensvorschriften und Verfahrensanweisungen und werden als solche angewendet. Neue Projektverfahren werden nur erarbeitet, wenn eine besondere Aufgabe im betrachteten Projekt zu beschreiben ist.

(c) **Projektentwicklungsdokumente**, die im Verlaufe des in Abbildung 5 dargestellten Lebenszyklus des Systems erarbeitet werden.

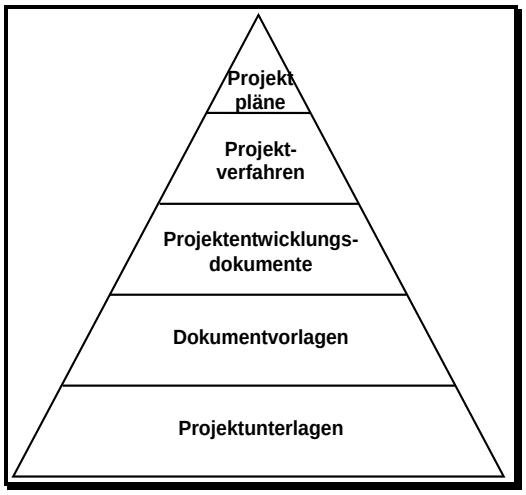


***Abbildung 12 : Strukturierte Dokumentationshierarchie***

(d) **Dokumentvorlagen des Unternehmens oder zumindest für das Projekt** gibt es für die verschiedenen vorzulegenden Arten von Dokumenten.

(e) **Projektunterlagen**, die im Verlaufe des Projektes erstellt werden und für den Nachweis der Einhaltung der Qualitätsmanagement- und Sicherheitsmanagementprozesse des Unternehmens notwendig sind.

Dies ist ein Weg zur Erreichung der erforderlichen dokumentarischen Nachweise. Andere Verfahrensweisen sind denkbar, so lang die Kriterien der CSM erfüllt werden.

[G 2] Die CENELEC-Normen empfehlen den Nachweis der Einhaltung der Funktions- und Sicherheitsanforderungen durch das System in einem Sicherheitsnachweisdokument (oder



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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

Sicherheitsbericht). Auch wenn dies nicht zwingend vorgeschrieben ist, erbringt ein Sicherheitsnachweis in einem strukturierten Sicherheitsdokument den Nachweis:

(a) für ein Qualitätsmanagement;
(b) für ein Sicherheitsmanagement;
(c) für die funktionale und technische Sicherheit.

Gleichzeitig liegt der Vorteil darin, dass dieser Sicherheitsnachweis die Bewertungsstelle(n) bei der unabhängigen Bewertung der ordnungsgemäßen Anwendung der CSM unterstützt und anleitet.

[G 3] Der Sicherheitsnachweis beschreibt und fasst zusammen, wie die Projektdokumente, die aus der Anwendung der unternehmenseigenen oder projektgebundenen Qualitäts- und/oder Sicherheitsmanagementprozesse hervorgehen, im Rahmen des Systementwicklungsprozesses für den Nachweis der Systemsicherheit miteinander zusammenhängen. Gewöhnlich enthält der Sicherheitsnachweis keine umfangreichen, detaillierten Nachweise und Begleitdokumentationen, sondern exakte Verweise auf solche Dokumente.

[G 4] **Sicherheitsnachweis für technische Systeme:** Die CENELEC-Normen können als Leitlinien für die Erstellung und/oder Struktur von Sicherheitsnachweisen verwendet werden.

(a) Siehe Norm EN 50 129 {Ref. 7} für „Bahnanwendungen – Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme – Sicherheitsrelevante elektronische Systeme für Signaltechnik“; auch in Anhang H.2 des Leitfadens EN 50 126-2 {Ref. 9} wird eine Struktur für den Sicherheitsnachweis von Signaltechnik vorgeschlagen;

(b) siehe Anhang H.1 des Leitfadens EN 50 126-2 {Ref. 9} für die Struktur des Sicherheitsnachweises von Fahrzeugen;

(c) siehe Anhang H.3 des Leitfadens EN 50 126-2 {Ref. 9} für die Struktur des Sicherheitsnachweises von Infrastrukturen.

Wie aus diesen Verweisen hervorgeht, sind die Struktur und der Inhalt der Sicherheitsnachweise für technische Systeme abhängig vom System, dessen Einhaltung der Sicherheitsanforderungen zu belegen ist.

Der in Anhang H des Leitfadens EN 50 126-*2* {Ref. 9} umrissene Sicherheitsnachweis gibt lediglich Beispiele und ist vermutlich nicht für alle Systeme der angegebenen Art geeignet. Deshalb ist diese umrissene Darstellung auf ihre Eignung für eine spezifische Anwendung mit entsprechendem Sachurteil zu betrachten.

[G 5] **Sicherheitsnachweis für organisatorische und betriebliche Aspekte in Eisenbahnsystemen:**

Gegenwärtig gibt es keine dedizierte Norm, die die Struktur, den Inhalt und eine Anleitung für das Verfassen des Sicherheitsnachweises für organisatorische und betriebliche Aspekte eines Eisenbahnsystems bereitstellt. Da der Zweck des Sicherheitsnachweises jedoch darin besteht, die Einhaltung der Sicherheitsanforderungen durch das System auf strukturierte Weise zu belegen, kann die gleiche Art von Sicherheitsnachweisstruktur wie bei technischen Systemen verwendet werden. Die Verweisliteratur in Punkt [G 4] von Abschnitt 5.1 gibt Empfehlungen und eine Checkliste zu behandelnder Elemente unabhängig von der Art des zu bewertenden Systems. Die Verwaltung organisatorischer und betrieblicher Änderungen erfordert die gleiche Art von Qualitäts- und Sicherheitsmanagementprozessen wie bei technischen Änderungen mit einem Nachweis, dass das System die spezifizierten Sicherheitsanforderungen einhält. Die Anforderungen der CENELEC-Normen, die nicht für organisatorische und betriebliche Aspekte gelten, sind jene Anforderungen mit ausschließlichem Bezug auf die konstruktive Anlage technischer Systeme wie beispielsweise hardwareinhärente Fail-Safe-Grundsätze, elektromagnetische Verträglichkeit (EMV) usw.



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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. Das vom Vorschlagenden gemäß Ziffer 5.1 erstellte Dokument enthält mindestens:*

*(a) eine Beschreibung der Organisation und Angaben zu den Sachverständigen, die benannt wurden, um das Risikobewertungsverfahren durchzuführen,*

*(b) die Ergebnisse der verschiedenen Phasen der Risikobewertung sowie eine Auflistung aller Sicherheitsanforderungen, die erfüllt werden müssen, damit das Risiko auf ein akzeptables Niveau gesenkt werden kann.*

[G 1] Je nach Komplexität des Systems, können diese Nachweise in einem oder mehreren Sicherheitsnachweisen zusammengefasst werden. Die Struktur des Sicherheitsnachweises für technische Systeme sowie für betriebliche und organisatorische Aspekte findet sich in Punkt [G 4] und [G 5] von Abschnitt 5.1.

[G 2] Mögliche Beispiele für Nachweise siehe auch Abschnitt A.4 in Alage A.

[G 3] Die erwartete Lebensdauer technischer Systeme und Teilsysteme im Eisenbahnsektor liegt in der Regel bei ca. 30 Jahren. Bei so langen Zeiträumen ist es plausibel, auch eine Reihe signifikanter Änderungen an diesen Systemen zu erwarten. Für diese Systeme und ihre Schnittstellen könnten demnach weitere Risikobewertungen mit der entsprechenden Begleitdokumentation durchgeführt werden, die mit Hilfe von Gefährdungsprotokollen geprüft, ergänzt und zwischen verschiedenen Akteuren und Organisation übertragen werden müssen. Dies erfordert relativ strenge Anforderungen an Dokumentationskontrolle und Konfigurationsmanagement.

[G 4] Ferner ist es hilfreich, wenn durch das Unternehmen, das alle Risikobewertungs- und Risikomanagementinformationen archiviert, gewährleistet wird, dass die Ergebnisse/Informationen auf einem physischen Datenträger gespeichert wird, der über die komplette Lebensdauer bzw. den kompletten Lebenszyklus des Systems (z. B. 30 Jahre) lesbar/zugänglich ist.

[G 5] Die Hauptgründe für diese Anforderungen sind unter anderem:

(a) Sicherstellung, dass alle Sicherheitsanalysen und Sicherheitsunterlagen des bewerteten Systems über die komplette Lebensdauer des Systems zugänglich bleiben. Also:

(1) für den Fall weiterer signifikanter Änderungen am gleichen System ist die letztgültige Systemdokumentation verfügbar;

(2) im Falle eines Problems während der Systemlebensdauer ist es günstig, wenn man auf die verbundenen Sicherheitsanalysen und Sicherheitsunterlagen zurückgreifen kann.

(b) Sicherstellung, dass die Sicherheitsanalysen und die Sicherheitsunterlagen des zu bewertenden Systems zugänglich sind, falls es in einer anderen Anwendung als ähnliches Referenzsystem verwendet werden soll.



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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

# ANHANG II DER CSM-VERORDNUNG

## Von den Bewertungsstellen zu erfüllende Kriterien

1. *Die Bewertungsstelle darf weder unmittelbar noch als Bevollmächtigte an der Planung, der Herstellung, dem Bau, dem Vertrieb, dem Betrieb oder der Instandhaltung des zu bewertenden Systems beteiligt sein. Ein Austausch technischer Informationen zwischen der Stelle und den beteiligten Akteuren wird hierdurch nicht ausgeschlossen.*

2. *Die Bewertungsstelle muss die Bewertung mit größter Gewissenhaftigkeit und höchster Fachkompetenz durchführen und darf keinerlei Druck oder Einflussnahme – vor allem finanzieller Art – auf ihr Urteil oder die Ergebnisse ihrer Bewertungen, insbesondere durch Personen oder Personengruppen, die von den Bewertungen betroffen sind, ausgesetzt sein.*

3. *Die Bewertungsstelle muss über die Mittel für die angemessene Erfüllung der technischen und administrativen Aufgaben verfügen, die mit der Durchführung der Bewertungen verbunden sind, und Zugang zu den für außergewöhnliche Bewertungen erforderlichen Geräten haben.*

4. *Das mit den Bewertungen beauftragte Personal muss über folgende Qualifikationen verfügen:*

   - *eine gute technische und berufliche Ausbildung,*
   - *eine ausreichende Kenntnis der Vorschriften für die von ihm durchgeführten Bewertungen und eine ausreichende praktische Erfahrung mit solchen Bewertungen,*
   - *die erforderliche Befähigung zur Erstellung der Sicherheitsbewertungsberichte, die die formellen Schlussfolgerungen der durchgeführten Bewertungen darstellen.*

5. *Die Unabhängigkeit des mit den unabhängigen Bewertungen beauftragten Personals muss gewährleistet sein. Die Vergütung der Mitarbeiter darf sich weder nach der Zahl der von ihm durchgeführten Bewertungen noch nach den Ergebnissen dieser Bewertungen richten.*

6. *Handelt es sich bei der Bewertungsstelle um eine externe Stelle außerhalb der Organisation des Vorschlagenden, muss die betreffende Stelle über eine Haftpflichtversicherung verfügen, es sei denn, dass der Mitgliedstaat aufgrund der nationalen Rechtsvorschriften haftet oder die Bewertungen selbst durchführt.*

7. *Handelt es sich bei der Bewertungsstelle um eine externe Stelle außerhalb der Organisation des Vorschlagenden, ist ihr Personal (außer gegenüber den zuständigen Verwaltungsbehörden des Staates, in dem es seine Tätigkeit ausübt) in Bezug auf alle Informationen, von denen es bei der Durchführung seiner Aufgaben im Rahmen dieser Verordnung Kenntnis erlangt, durch das Berufsgeheimnis gebunden.*

[G 1] Eine zusätzliche Erläuterung erscheint nicht notwendig.



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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

# ANLAGE A: ZUSÄTZLICHE KLARSTELLUNGEN

## A.1. Einleitung

A.1.1. Diese Alage soll das Lesen des vorliegenden Dokumentes unterstützen. Um das eigentliche Dokument nicht mit Informationen zu überfrachten, werden komplexere Themen im vorliegenden Alage näher erläutert.

## A.2. Gefährdungseinstufung

A.2.1. Hinweise zur Einstufung/Klassifikation von Gefährdungen finden sich in Abschnitt § 4.6.3. der Norm EN 50 126-1 {Ref. 8} sowie in Anhang B.2 des Leitfadens EN 50 126-2 {Ref. 9}.

## A.3. Risikoakzeptanzkriterium für technische Systeme (RAC-TS)

### A.3.1. Obergrenze der Risikozulässigkeit für technische Systeme

A.3.1.1. Das RAC-TS wird in Abschnitt 2.5.4. von {Ref. 4} beschrieben.

A.3.1.2. Das RAC-TS bezweckt die Vorgabe einer Obergrenze der Risikozulässigkeit für technische Systeme, für die die Sicherheitsanforderungen weder durch die Anwendung von anerkannten Regeln der Technik noch durch den Vergleich mit ähnlichen Referenzsystemen hergeleitet werden können. Dementsprechend wird hier ein Bezugspunkt definiert, von dem aus die Risikoanalysemethoden für die technischen Systeme kalibriert werden können. Wie in Abschnitt A.3.6. von Anlage A dieses Dokuments beschrieben, könnte dieser Bezugspunkt bzw. diese Obergrenze der Risikozulässigkeit auch dazu verwendet werden, die Risikoakzeptanzkriterien für andere Funktionsausfälle technischer Systeme zu definieren, bei denen kein unmittelbar vorstellbares Potenzial für eine katastrophale Folge vorliegt (d. h. für andere Schweregrade). Das RAC-TS ist jedoch keine Methode für die Risikoanalyse.

A.3.1.3. Das RAC-TS ist ein halbquantitatives Kriterium. Es gilt sowohl für zufällige Hardware-Ausfälle als auch die systematischen Ausfälle/Fehler des technischen Systems. Somit werden hier auch die systematischen Ausfälle/Fehler des technischen Systems erfasst, die sich potenziell aus menschlichen Fehlern im Zuge des Entwicklungsprozesses des technischen Systems (d. h. während der Spezifikation, Konstruktion, Implementierung und Validierung) ergeben können. Menschliche Fehler während des Betriebs und der Instandhaltung des technischen Systems sind hingegen im RAC-TS nicht erfasst.

A.3.1.4. Entsprechend den Anhängen A.3 und A.4 der CENELEC-Norm 50 129 sind die systematischen Ausfälle/Fehler nicht quantifizierbar und somit muss das quantitative Ziel nur für zufällige Hardwareausfälle nachgewiesen werden, während die systematischen Ausfälle/Fehler mit qualitativen Methoden[(15)] behandelt werden. „*Da eine Bewertung der systematischen Ausfallsicherheit durch quantitative Methoden nicht möglich ist, werden Safety-Integrity-Levels zur Gruppierung von Methoden, Werkzeugen und Techniken*

---

*(15)* *Gemäß den CENELEC-Normen 50 126, 50 128 und 50 129 muss die quantitative Zahl, die zufällige Hardware-Ausfälle behandelt, immer mit einem Safety-Integrity-Level verknüpft werden, um die systematischen Ausfälle/Fehler zu verwalten. Somit erfordert auch die Zahl $10^{-9}\,h^{-1}$ des RAC-TS die Einrichtung eines adäquaten Prozesses, mit dem auch die systematischen Ausfälle/Fehler ordnungsgemäß verwaltet werden. Zur besseren Lesbarkeit wird in der Mitteilung jedoch meist nur Bezug auf die zufälligen Hardware-Ausfälle des technischen Systems genommen.*



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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

*verwendet, bei denen davon auszugehen ist, dass sie bei effektivem Einsatz ein ausreichend hohes Vertrauen in die Realisierung eines Systems mit einem angegebenen Integritätsniveau erreichen."*

A.3.1.5. Analog dazu ist nach den CENELEC-Normen die Integrität der Software technischer Systeme nicht quantifizierbar. Die CENELEC-Norm 50 128 enthält Hinweise für den Entwicklungsprozess sicherheitsbezogener Software in Abhängigkeit von der geforderten Sicherheitsanforderungsstufe (Safety-Integrity-Level). Dazu gehören die Entwurfs-, Verifizierungs-, Validierungs- und Qualitätssicherungsprozesse für die Software.
Entsprechend der CENELEC-Norm 50 128 ist für ein programmierbares elektronisches Steuersystem mit implementierten Sicherheitsfunktionen die höchstmögliche Sicherheitsanforderungsstufe für den Softwareentwicklungsprozess die Integritätsstufe SIL 4, die einer quantitativen tolerierbaren Gefährdungsrate von $10^{-9}$ $h^{-1}$ entspricht.

A.3.1.6. Da sich also die systematischen Ausfälle/Fehler nicht quantifizieren lassen, müssen sie stattdessen durch die Einführung eines Qualitäts- und Sicherheitsprozesses verwaltet werden, der mit der für das zu bewertende System geforderten SIL-Stufe kompatibel ist.

(a) Zweck des Qualitätsprozesses ist *„die Minimierung der Auswirkung menschlicher Fehler in jeder Phase des Lebenszyklus und damit die Verminderung des Risikos systematischer Fehler im System"*;

(b) Zweck des Sicherheitsprozesses ist *„die weitere Verminderung der Auswirkung sicherheitsbezogener menschlicher Fehler im gesamten Lebenszyklus und damit die Minimierung des Restrisikos sicherheitsbezogener systematischer Fehler."*

A.3.1.7. Hinweise zur Verwaltung der Auswirkungen systematischer Ausfälle/Fehler sowie Hinweise zu möglichen konstruktiven Maßnahmen für den Schutz gegen Ausfälle durch gemeinsame Ursachen bzw. gemeinsamer Art (Common Cause/Mode Failures – CCF/CMF) und zur Gewährleistung, dass das technische System bei solchen Ausfällen/Fehler einen sicheren Zustand (Fail-Safe-State) einnimmt, finden sich in folgenden Normen:

(a) Die Norm CENELEC 50 126-1 {Ref. 8} und der dazugehörige Leitfaden 50 126-2 {Ref. 9} enthalten eine Aufstellung der Bestimmungen der CENELEC 50 129 und deren Anwendbarkeit für dokumentierte Nachweise für Systeme außer signalgebende Systeme: siehe Tabelle 9.1 in Leitfaden 50 126-2 {Ref. 9}. Diese Aufstellung enthält Verweise, wie die Fehler aus dem eigentlichen System und die Umgebungswirkung auf das zu bewertende System zu behandeln sind.

Beispielsweise finden sich Techniken/Maßnahmen für Konstruktionsmerkmale in *„Tabelle E.5: Konstruktive Merkmale (gemäß 5.4)"* der Norm CENELEC 50 129 {Ref. 7}, *„zur Vermeidung und Kontrolle von Fehlzuständen verursacht durch:*

(1) *„konstruktive Restfehler";*
(2) *„Umweltbedingungen";*
(3) *„Missbrauch oder Bedienfehler";*
(4) *„Restfehler in der Software";*
(5) *„menschliche Faktoren";"*

Die Anhänge D und E der Norm CENELEC 50 129 {Ref. 7} enthalten Techniken und Maßnahmen für die Vermeidung systematischer Fehlzustände und für die Kontrolle zufälliger Hardware- und systematischer Ausfälle/Fehler für sicherheitsbezogene elektronische Systeme in der Signalgebung. Eine ganze Reihe davon lässt sich über eine Verweisung auf diese Richtlinien in Tabelle 9.1 des Leitfadens 50 126-2 {Ref. 9} auf nicht signalgebende Systeme übertragen.



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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) Die Norm CENELEC 50 128 enthält Hinweise für den Entwicklungsprozess sicherheitsbezogener Software in Abhängigkeit von den Safety-Integrity-Levels (SIL 0 bis SIL 4), die für die Software des zu bewertenden Systems gefordert werden.

A.3.1.8. Das RAC-TS stellt darüber hinaus das höchste Integritätsniveau dar, das nach CENELEC- und IEC-Normen gefordert werden kann. Zur besseren Bezugnahme seien die Anforderungen aus den Normen IEC 61508-1 und CENELEC 50 129 hier zitiert:

(a) IEC 61508-1: *„Diese Norm setzt eine beanspruchbare niedrigere Grenze bei den vorgegebenen Ausfallwahrscheinlichkeiten fest. Diese werden als Untergrenzen für Safety-Integrity-Level 4 spezifiziert. Zwar können Konstruktionen sicherheitsbezogener Systeme mit niedrigeren Ausfallwahrscheinlichkeiten bei nicht komplexen Systemen erreichbar sein, aber es wird davon ausgegangen, dass die Zahlen in der Tabelle die Grenze dessen darstellen, was für relativ komplexe System (beispielsweise programmierbare elektronische sicherheitsbezogene Systeme) derzeit erreicht werden kann."*

(b) EN 50129: *„Eine Funktion mit quantitativen Anforderungen von mehr als $10^{-9}$ $h^{-1}$ ist auf einem der beiden folgenden Wege zu behandeln:*

(1) *Wenn eine Aufteilung der Funktion in funktional unabhängige Teilfunktionen möglich ist, kann die tolerierbare Gefährdungsrate (THR) auf diese Teilfunktionen aufgesplittet und jeder Teilfunktion eine SIL zugeordnet werden;*

(2) *Wenn die Funktion nicht aufteilbar ist, müssen zur Erreichung der notwendigen THR die für SIL 4 erforderlichen Maßnahmen und Methoden mindestens erfüllt sein und die Funktion in Kombination mit anderen technischen oder betrieblichen Maßnahmen verwendet werden."*

A.3.1.9. Alle technischen Systeme müssen dann die quantitative Sicherheitsanforderung auf diese Zahl begrenzen. Wird ein höheres Schutzniveau benötigt, kann dies nicht mit nur einem System erreicht werden. Die Architektur des Systems muss geändert werden, beispielsweise indem zwei unabhängige Systeme parallel verwendet werden, die über Cross-Checks sichere Outputs generieren. Dies erhöht jedoch definitiv die Kosten der technischen Systementwicklung.

**Bemerkung:** Falls Funktionen bestehen, z. B. rein mechanische Systeme, die anhand von Betriebserfahrungen einen höheren Integritätslevel erreicht haben, kann das Sicherheitsniveau durch besondere anerkannte Regeln der Technik beschrieben werden oder können die Sicherheitsanforderungen durch Ähnlichkeitsanalyse mit dem bestehenden System festgelegt werden. Im Anwendungsbereich der CSM muss das RAC-TS nur dann angewendet werden, wenn weder anerkannte Regeln der Technik noch ein Referenzsystem existieren.

A.3.1.10. Hierbei kann wie folgt zusammengefasst werden:

(a) Entsprechend den CENELEC-Normen 50 126, 50 128 und 50 129 sind die systematischen Ausfälle/Fehler bei der Entwicklung nicht quantifizierbar;

(b) Die Auswirkung systematischer Ausfälle/Fehler sowie ihr Restrisiko müssen durch die Anwendung geeigneter Qualitäts- und Sicherheitsprozesse kontrolliert und verwaltet werden, die mit der für das zu bewertende System verlangten Sicherheitsanforderungs-stufe (Safety-Integrity-Level) kompatibel sind;

(c) die höchste erreichbare Sicherheitsanforderungsstufe ist SIL 4 für die zufälligen Hardware-Ausfälle ebenso wie für die systematischen Ausfälle/Fehler technischer Systeme;

(d) die SIL-4-Grenze bedeutet, dass die maximale tolerierbare Gefährdungsrate (THR) (d. h. die maximale Ausfallrate) für technische Systeme auch auf $10^{-9}$ $h^{-1}$ zu begrenzen ist.



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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. Eine tolerierbare Gefährdungsrate von $10^{-9}\,h^{-1}$ kann ein technisches System entweder mit einer „Fail-Safe-Architektur“ (die per definitionem einen solchen Sicherheitsgrad gewährleistet) oder mit einer „redundanten Architektur“ (z. B. zwei unabhängige Verarbeitungskanäle mit gegenseitigem Cross-Check) erreichen.

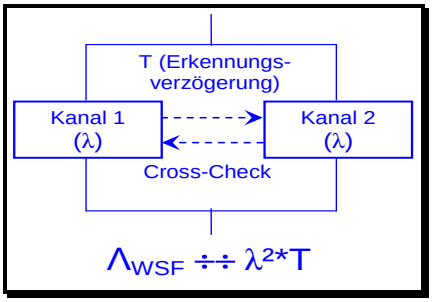


***Abbildung 13 : Redundante Architektur für ein technisches System.***

Für eine redundante Architektur kann gezeigt werden, dass die Gesamtrate gefährlicher Ausfälle ($\Lambda_{WSF}$) des technischen Systems proportional zu $\lambda^2*T$ ist, wobei gilt:

(a) $\lambda^2$ ist das Quadrat der gefährlichen Ausfallrate eines einzelnen Kanals;

(b) T ist die Zeit, die ein einzelner Kanal benötigt, um den bzw. die gefährlichen Ausfall/Ausfälle des anderen Kanals zu erkennen. Dies ist gewöhnlich ein Mehrfaches der Verarbeitungszeit bzw. des Verarbeitungszyklus eines Kanals. T ist gewöhnlich weitaus kleiner als 1 Sekunde.

A.3.1.12. Anhand dieser Formel ($\lambda^2*T$) kann theoretisch nachgewiesen werden (unter alleiniger Berücksichtigung der zufälligen Hardware-Ausfälle des technischen Systems – siehe auch Punkt A.3.1.13 in Anlage A), dass eine quantitative Anforderung von $10^{-9}\,h^{-1}$ für das RAC-TS erreichbar ist. Die systematischen Ausfälle/Fehler müssen durch einen entsprechenden Prozess verwaltet werden: siehe Punkt A.3.1.6 in Anlage A. Zum Beispiel:

(a) mit einer MTBF (mittleren Zeit zwischen Ausfällen) von 10 000 Stunden für die Zuverlässigkeitszahl eines Kanals und mit der vorsichtigen Annahme, dass jeder Kanalausfall zu einem unsicheren Zustand führt, liegt die gefährliche Ausfallrate des Kanals bei $10^{-4}\,h^{-1}$;

(b) selbst bei einer Zeitdauer von 10 Minuten (d. h. $\approx 2*10^{-3}$ Stunden) bis zur Entdeckung des bzw. der gefährlichen Ausfalls / Ausfälle des anderen Kanals, was gleichfalls eine vorsichtige Annahme ist;

Die Gesamtrate für gefährliche Ausfälle $\Lambda_{WSF} \approx 2 * 10^{-10}\,h^{-1}$

A.3.1.13. Bei einer solchen redundanten Architektur muss die Evaluierung der quantitativen gefährlichen Hardware-Gesamtausfälle in der Praxis die Maßnahmen berücksichtigen, die im Entwurf ergriffen werden, um den Schutz gegen Ausfälle durch gemeinsame Ursachen / Ausfälle gemeinsamer Art (Common Cause/Mode Failures – CCF/CMF) zu gewährleisten und sicherzustellen, dass das technische System im Falle eines CCF/CMF-Ausfalls/Fehlers einen Fail-Safe-Zustand annimmt. Diese Evaluierung der gefährlichen Gesamtausfallrate ($\Lambda_{WSF}$) muss ferner Folgendes berücksichtigen:

(a) die allen Kanälen gemeinen Komponenten, z. B. einzelne oder gemeinsame Eingänge zu allen Kanälen, gemeinsame Stromversorgung, Vergleichs- und Überwachungsglieder usw.;

(b) die erforderliche Zeit bis zur Erkennung von ruhenden oder latenten Ausfällen. Bei komplexen technischen Systemen kann diese Zeit um mehrere Größenordnungen größer als 1 Sekunde sein;

(c) die Auswirkung von CCF/CMF-Ausfällen.

Hinweise zu diesen Themen finden sich in Normen, die unter Punkt A.3.1.7 in Anlage A. von dieses Dokuments zusammengefasst werden.



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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. Ablaufdiagramm für den Gültigkeitstest des RAC-TS

A.3.2.1. Die Art und Weise der Anwendung des RAC-TS für Gefährdungen aufgrund von Ausfällen technischer Systeme kann gemäß Abbildung 14 dargestellt werden.

A.3.2.2. Ein Beispiel für die Anwendung dieses Diagramms findet sich in Abschnitt C.15 von Anlage C.

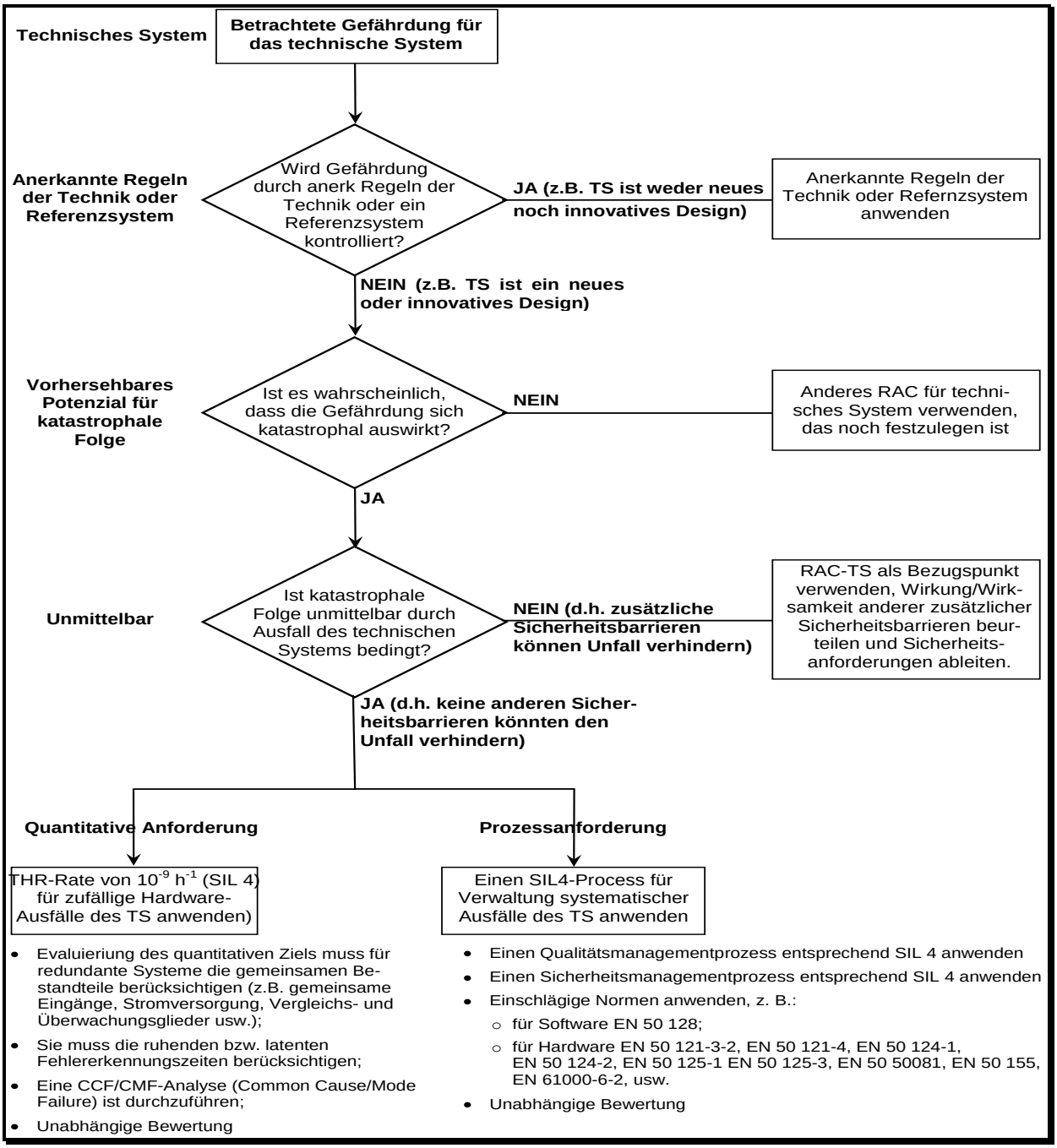


***Abbildung 14 : Ablaufdiagramm Gültigkeitstest des RAC-TS***


European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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.3.3. Definition eines technischen Systems ausgehend von der CSM

A.3.3.1. Das RAC-TS gilt ausschließlich für technische Systeme. „Technisches System“ ist in Artikel 3 Nummer 22 der CSM-Verordnung wie folgt definiert:

*„Technisches System“: das Bauteil oder die Baugruppe, einschließlich Planung, Realisierung und Begleitdokumentation; die Entwicklung eines technischen Systems beginnt mit der Festlegung der Anforderungen an das System und endet mit seiner Zulassung; auch wenn dabei die relevanten Schnittstellen zum menschlichen Verhalten berücksichtigt werden, sind das Personal und dessen Handlungen nicht Bestandteil eines technischen Systems; der Wartungsprozess wird in den Wartungshandbüchern beschrieben, ist aber selbst nicht Bestandteil des technischen Systems."*

## A.3.4. Erläuterung der Definition „Technisches System“

A.3.4.1. Diese Definition eines technischen Systems beschreibt den Geltungsumfang des technischen Systems: *„Technisches System beutet das Bauteil oder die Baugruppe, einschließlich Planung, Realisierung und Begleitdokumentation.“;* Dementsprechend umfasst und beinhaltet es:

(a) die das technische System bildenden physischen Teile;
(b) die damit verbundene Software (soweit vorhanden);
(c) die Planung und Realisierung des technischen Systems, einschließlich, soweit zutreffend, Konfiguration oder Parametrierung eines generischen Produkts entsprechend den spezifischen Anforderungen der spezifischen Anwendung;
(d) die notwendige Begleitdokumentation für:

(1) die Entwicklung des technischen Systems;
(2) den Betrieb und die Instandhaltung des technischen Systems;

A.3.4.2. In den mit dieser Definition verbundenen Anmerkungen wird der Geltungsumfang des technischen Systems weiter dargelegt:

(a) *„Die Entwicklung eines technischen Systems beginnt mit der Festlegung der Anforderungen an das System und endet mit seiner Zulassung.“* Dies umfasst die Phasen 1 bis 10 der V-Darstellung in Bild 10 der CENELEC-Norm 50 126-1 {Ref. 8};

(b) *„auch wenn dabei die relevanten Schnittstellen zum menschlichen Verhalten berücksichtigt werden, sind das Personal und dessen Handlungen nicht Bestandteil eines technischen Systems.“* Obwohl die humanfaktorbedingten Fehler während des Betriebs und der Instandhaltung des technischen Systems nicht Teil des eigentlichen Systems sind, muss die Gestaltung der Schnittstellen zu den menschlichen Bedienern diese in Betracht ziehen. Zweck ist die Minimierung der Wahrscheinlichkeit von menschlichen Fehlern, die auf eine mangelhafte Gestaltung der relevanten Schnittstellen zu den menschlichen Bedienern zurückgehen;

(c) *„der Wartungsprozess wird in den Wartungshandbüchern beschrieben, ist aber selbst nicht Bestandteil des technischen Systems.“* Das bedeutet, dass das RAC-TS nicht auf den Betrieb und die Instandhaltung des technischen Systems angewendet werden muss; diese beruhen zu einem Großteil auf Abläufen und Handlungen, die von menschlichem Personal durchgeführt werden.
Zur Unterstützung der Instandhaltung technischer Systeme muss die Definition des technischen Systems jedoch alle relevanten Anforderungen (z. B. regelmäßige vorbeugende Instandhaltung oder korrektive Instandhaltung im Falle von Ausfällen) mit ausreichendem Detailgrad einbeziehen. Wie die Instandhaltung am entsprechenden technischen System zu organisieren und zu erreichen ist, ist jedoch nicht Teil der



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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

Definition des technischen Systems, sondern Bestandteil der entsprechenden Instandhaltungshandbücher.

A.3.4.3. Siehe auch Abschnitt A.3.1 in Anlage A.

## A.3.5. Funktionen von technischen Systemen, für die das RAC-TS gilt

A.3.5.1. Das RAC-TS gilt entsprechend seiner Definition für gefährliche Ausfälle der vom technischen System zu erfüllenden Funktionen, wenn diese *"ein vorstellbares **unmittelbares** Potenzial für eine katastrophale Folge"* besitzen: Siehe Abschnitt 2.5.4. in {Ref. 4}.

A.3.5.2. Das RAC-TS kann auch für Funktionen angewendet werden, an denen technische Systeme beteiligt sind, bei denen aber im Falle eines Ausfalls **nicht** ***"von unmittelbaren** katastrophalen Folgen"* auszugehen ist. In diesem Fall muss das RAC-TS als Gesamtziel für die Ereignisreihe angewendet werden, die die katastrophale Folge hervorruft. Anhand dieses Gesamtzieles muss der tatsächliche Anteil jedes einzelnen Ereignisses und damit der Funktionsausfälle des am betrachteten Szenario beteiligten technischen Systems entsprechend Abschnitt A.3.6 in Anlage A abgeleitet werden.
Eine solche Verwendung des RAC-TS ist noch mit der CSM-Arbeitsgruppe zu erörtern und zu vereinbaren.

A.3.5.3. Für welche Funktionen des technischen Systems gilt das RAC-TS? Entsprechend der Norm IEC 61226:2005 gilt:

(a) Eine Funktion ist in diesem Kontext definiert als *„ein bestimmter Zweck oder ein Ziel, das es zu erreichen gilt und das ohne Bezug auf die physikalische Realisierung festgelegt und beschrieben werden kann“*;
(b) eine Funktion (als Blackbox betrachtet) überführt Eingangsparameter (z. B. Material, Energie, Informationen) in zielbezogene Ausgabeparameter (z. B. Material, Energie, Informationen);
(c) die Analyse der Funktion ist unabhängig von ihrer technischen Realisierung.

A.3.5.4. Das RAC-TS gilt für die folgenden Arten von Funktionen:

(a) Beispiele für das fahrzeugseitige ETCS-Teilsystem:

(1) „Den Triebfahrzeugführer mit Informationen versorgen, die es ihm ermöglichen, den Zug sicher zu führen und im Falle überhöhter Geschwindigkeit eine Bremsung auszulösen“. Anhand der streckenseitig gelieferten Informationen (erlaubte Geschwindigkeit) und der Zuggeschwindigkeitsberechnung der fahrzeugseitigen ETCS-Ausrüstung können der Triebfahrzeugführer und das fahrzeugseitige ETCS den Zug so überwachen, dass er die erlaubte Höchstgeschwindigkeit nicht übersteigt. Das RAC-TS gilt für die fahrzeugseitige Evaluierung der Zuggeschwindigkeit, denn:

(i) Es gibt keine zusätzliche (unmittelbare) Barriere, da die an den Triebfahrzeugführer gehenden Informationen auch unterevaluiert sind;
(ii) die Geschwindigkeitsüberschreitung des Zuges könnte zu einer Entgleisung führen, also zu einem Unfall mit katastrophalem Folgenpotenzial.

(2) „Den Triebfahrzeugführer mit Informationen versorgen, die es ihm ermöglichen, den Zug sicher zu führen und im Falle eines Verstoßes gegen die erlaubte Fahrbewegung eine Bremsung auszulösen“.

(b) Beispiel für einen Gleisstromkreis: „Gleisfreiheit des Streckenabschnitts erkennen“. Das RAC-TS kommt bei dieser Funktion nur dann zur Anwendung, wenn im Stellwerk keine sequentielle Überwachungsfunktion implementiert ist;


European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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) Beispiel für eine Weiche: „Weichenstellung kontrollieren“.

A.3.5.5. Einige Normen definieren auch Funktionen, für die das RAC-TS gelten könnte. Zum Beispiel:

(a) Die Norm prEN 0015380-4 {Ref. 13} (ModTrain) definiert in ihrem normativen Teil drei hierarchische Funktionsebenen (mit Erweiterung auf fünf Ebenen in informativen Anhängen). Insgesamt definiert die prEN 0015380-4 mehrere hundert zugbezogene Funktionen;
(b) in der Regel wird empfohlen, die Funktionen aus den ersten drei Ebenen der prEN 0015380-4 (aber nicht darunter) auszuwählen und dabei auch die Aufschlüsselungsstruktur des Produktes zu beachten;
(c) für Funktionen, die nicht in den Anwendungsbereich der prEN 0015380-4 fallen, muss über die geeignete Funktionsebene auf dem Vergleichswege unter Zuhilfenahme eines Sachverständigenurteils entschieden werden.

Diese Beispiele von Funktionen aus der Norm prEN 0015380-4 sind von der Agentur im Zuge der Bearbeitung der weitgehend akzeptablen Risiken und der Risikoakzeptanzkriterien weiter zu bearbeiten.

A.3.5.6. Das RAC-TS gilt beispielsweise auch für die folgende Funktion der prEN 0015380-4: *„Neigung steuern“* (Code = CLB). Die Funktion könnte auf der Systemebene auf zweierlei Art verwendet werden:

(a) Erster Fall: Der Zug soll sich in Bögen aus Gründen des Passagierkomforts neigen und muss die Übereinstimmung des Lichtraumprofils mit der streckenseitigen Infrastruktur überwachen;
(b) zweiter Fall: Der Zug soll sich in Bögen ausschließlich aus Gründen des Passagierkomforts neigen, muss aber die Übereinstimmung des Lichtraumprofils mit der streckenseitigen Infrastruktur nicht überwachen.

Im ersten Fall wird das RAC-TS angewendet, aber im zweiten Fall nicht, da der Ausfall der Neigungsfunktion keine katastrophale Folge hat.

A.3.5.7. Das Beispiel (b) in Punkt A.3.5.4 und die Beispiele in Punkt A.3.5.6 in Anlage A zeigen deutlich, dass der Aufbau einer vordefinierten Liste von Funktionen, für die das RAC-TS auf jeden Fall anzuwenden ist, nicht machbar ist. Dies wird immer davon abhängen, wie das System diese Teilsystemfunktionen verwendet.

A.3.5.8. Ein Beispiel der Anwendung des RAC-TS findet sich in Abschnitt C.15 von Anlage C.

## A.3.6. Anwendungsbeispiele für RAC-TS

### A.3.6.1. Einleitung

(a) Dieses Kapitel gibt Beispiele, wie die Ausfallrate für die anderen Gefährdungsstufen bestimmt werden kann and wie Sicherheitsanforderungen unter $10^{-9}\,h^{-1}$ abgeleitet werden können. Das vorliegende Dokument bevorzugt oder empfiehlt keine besondere Methode. Es werden nur Informationen gegeben, wie das RAC-TS für die Kalibrierung einiger oft verwendeter Methoden verwendet werden kann. Das Dokument bedarf einer weiteren Entwicklung im Zuge der Arbeiten der Agentur an den weitgehend akzeptablen Risiken und Risikoakzeptanzkriterien.

(b) Tatsächlich kann das RAC-TS nur in einer geringen Zahl von Fällen unmittelbar angewendet werden, da in der Praxis nicht viele Funktionsausfälle technischer Systeme unmittelbar zu Unfällen mit potenziell katastrophalen Folgen führen. Um das Kriterium auf Gefährdungen mit nicht katastrophalen Folgen anzuwenden und die Zielausfallrate zu bestimmen, können Vergleiche (z. B. durch Kalibrierung einer Risikomatrix mit


European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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

diesem Kriterium) zwischen unterschiedlichen Parametern, z. B. Folgenschwere gegenüber Häufigkeit, durchgeführt werden.

### A.3.6.2. Beispiel 1: Direkter Risikovergleich (Tradeoff)

(a) Das RAC-TS lässt sich leicht auf Szenarien anwenden, die sich nur in einigen wenigen unabhängigen Parametern von den Bezugsbedingungen unterscheiden, die im RAC-TS in Abschnitt 2.5.4. der CSM-Verordnung {Ref. 3} festgelegt sind;

(b) Angenommen, für einen besonderen Parameter p besteht ein multiplikatives Verhältnis zum Risiko. Angenommen, in der Bezugsbedingung liegt p* vor, während für das alternative Szenario p‘ gilt. In diesem Fall ist nur das Parameterverhältnis p*/p’ relevant und die Eintrittsrate kann vermindert werden. Wenn die Parameter unabhängig sind, kann dieses Verfahren wiederholt werden.

(c) Beispiel:

(1) Angenommen, das tatsächliche Potenzial für eine katastrophale Folge wurde durch ein Sachverständigenurteil zehn Mal niedriger bewertet als das Katastrophenpotenzial unter den Bezugsbedingungen nach Abschnitt 2.5.4 der CSM-Verordnung {Ref. 3}. Dann läge die Anforderung bei $10^{-8}\,h^{-1}$ statt bei $10^{-9}\,h^{-1}$.

(2) angenommen, es wird festgestellt, dass eine zusätzliche Sicherheitsbarriere durch ein anderes technisches System (unabhängig von den Folgen) besteht, die in 50 % der Fälle wirksam ist;

(3) dann läge die Sicherheitsanforderung bei $5*10^{-7}\,h^{-1}$ (d. h. $0{,}5*10^{-8}\,h^{-1}$) statt bei $10^{-9}\,h^{-1}$.

### A.3.6.3. Beispiel 2: Risikomatrix-Kalibrierung

(a) Zur sachgerechten Anwendung des RAC-TS in einer Risikomatrix muss die Matrix sich auf die richtige Systemebene beziehen (vergleichbar zur Angabe in Abschnitt A.3.5 in Anlage A).

(b) Das RAC-TS definiert ein Feld in der Risikomatrix als tolerierbar, das der Koordinate entspricht (Gefahrenstufe katastrophal; Unfallhäufigkeit $10^{-9}\,h^{-1}$): siehe rotes Feld in Tabelle 5. Alle Felder mit Bezug auf eine höhere Unfallhäufigkeit sind als „intolerabel“ zu kennzeichnen. Es ist zu beachten, dass nur im Falle eines vorstellbaren unmittelbaren Potenzials für eine katastrophale Folge die Häufigkeit von Unfällen gleich der Häufigkeit von Funktionsausfällen ist.

***Tabelle 5: Typisches Beispiel einer kalibrierten Risikomatrix***

| **Eintrittshäufigkeit eines Unfalls (infolge einer Gefahr)** | **Risikoniveau** | | | |
|---|---|---|---|---|
| Häufig ($10^{-4}$ pro Stunde) | Intolerabel | Intolerabel | Intolerabel | Intolerabel |
| Wahrscheinlich ($10^{-5}$ pro Stunde) | Intolerabel | Intolerabel | Intolerabel | Intolerabel |
| Gelegentlich ($10^{-6}$ pro Stunde) | Akzeptabel | Intolerabel | Intolerabel | Intolerabel |
| Selten ($10^{-7}$ pro Stunde) | Akzeptabel | Akzeptabel | Intolerabel | Intolerabel |
| Unwahrscheinlich ($10^{-8}$ pro Stunde) | Akzeptabel | Akzeptabel | Akzeptabel | Intolerabel |
| Unvorstellbar ($10^{-9}$ pro Stunde) | Akzeptabel | Akzeptabel | Akzeptabel | Akzeptabel |
| | Unbedeutend | Marginal | Kritisch | Katastrophal |
| | **Gefahrenstufe (d. h. Ausmaß der Folge von Unfällen)** | | | |

| **Risikoevaluierung** | **Risikoverminderung/Risikokontrolle** |
|---|---|
| Intolerabel | Das Risiko muss ausgeschlossen werden. |
| Akzeptabel | Das Risiko ist akzeptabel. Eine unabhängige Bewertung ist erforderlich. |



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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) Dann kann der Rest der Matrix ausgefüllt werden, wobei jedoch Effekte wie Risikoaversion oder Skalierung der Kategorien berücksichtigt werden müssen. Im einfachsten Falle einer linearen dekadischen Skalierung (wie in Tabelle 5 durch den Pfeil verdeutlicht) wird das durch RAC-TS als „akzeptabel“ bezeichnete Feld linear auf den Rest der Matrix extrapoliert. Das bedeutet, dass alle Felder in der gleichen Diagonale (oder unterhalb der Diagonale) auch als „akzeptabel“ ausgezeichnet werden. Auch die darunter stehenden Felder können als „akzeptabel“ ergänzt werden.

(d) Nachdem die Matrix ausgefüllt ist, kann sie auch auf nicht katastrophale Gefährdungen angewendet werden. Wenn beispielsweise ein anderer Funktionsausfall in die Gefahrenstufe „kritisch“ eingeordnet ist, dann sollte nach der kalibrierten Risikomatrix die tolerierbare Unfallhäufigkeit die Kategorie „unwahrscheinlich“„ nicht übersteigen (oder sogar darunter liegen).

(e) Es ist anzumerken, dass die Risikomatrix zu übervorsichtigen Ergebnissen führen kann, wenn sie für Eintrittshäufigkeiten von Funktionsausfällen angewendet wird (d. h. für Funktionsausfälle, die nicht unmittelbar zu Unfällen führen).

#### A.3.6.4. Grundsatz für die Kalibrierung anderer Risikoanalysemethoden

Auch andere Risikoanalysemethoden, beispielsweise die vorgeschlagene Risikoprioritätszahl oder das Risikodiagramm aus der VDV 331 oder IEC 61508, können durch ein ähnliches Verfahren, wie für die Risikomatrix dargestellt, kalibriert werden.

(a) Erster Schritt: Der Bezugspunkt aus dem RAC-TS wird als tolerierbar und Punkte mit höherer Häufigkeit oder Gefahrenstufe werden als intolerierbares RAC-TS klassifiziert.

(b) Zweiter Schritt: Verwendung der Vergleichsmechanismen (Tradeoff) der besonderen Methode zur Extrapolierung der Risikozulässigkeit auf nicht katastrophale Gefährdungen (ausgehend vom linearen Risikovergleich).

(c) Dritter Schritt: Für die nicht katastrophalen Gefährdungen kann daraufhin das RAC-TS aus der kalibrierten Risikoanalysemethode hergeleitet werden, indem die (Häufigkeit; Gefahrenstufe)-Koordinate mit der so erhaltenen FN-Kurve verglichen wird.

## A.3.7. Schlussfolgerungen für RAC-TS

A.3.7.1. In dem von der CSM vorgeschlagenen allgemeinen Risikobewertungsrahmen sind Risikoakzeptanzkriterien notwendig, um zu bestimmen, wann das Risikorestniveau akzeptabel wird und damit auch, wann die explizite Risikoabschätzung zu beenden ist.

A.3.7.2. Das RAC-TS ist ein Konstruktionsziel ($10^{-9}$ $h^{-1}$) für technische Systeme.

A.3.7.3. Hauptzwecke des RAC-TS sind:

(a) Festlegung einer Obergrenze für die Risikozulässigkeit und dementsprechend Festlegung eines Bezugspunktes, von dem ausgehend die Risikoanalysemethoden für die technischen Systeme kalibriert werden können;

(b) Ermöglichung der gegenseitigen Anerkennung technischer Systeme, da die verbundenen Risiko- und Sicherheitsbewertungen in allen MS anhand ein und desselben Risikoakzeptanzkriteriums evaluiert werden;

(c) Einsparung von Kosten, da nicht unnötig hohe quantitative Sicherheitsanforderungen verlangt werden;

(d) Vereinfachung des Wettbewerbs zwischen Herstellern. Die Verwendung unterschiedlicher Risikoakzeptanzkriterien je nach Vorschlagendem oder Mitgliedstaat würde dazu führen, dass die Industrie viele verschiedene Nachweise an den gleichen



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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

technischen Systemen durchführen würde. Das würde demzufolge die Wettbewerbsfähigkeit von Herstellern gefährden und Produkte unnötig verteuern.

A.3.7.4. Die im RAC-TS enthaltene halbquantitative Anforderung muss für technische Systeme nicht in jedem Falle nachgewiesen werden. Tatsächlich ist im Anwendungsbereich der CSM das RAC-TS nur für technische Systeme anzuwenden, bei denen die ermittelten Gefährdungen weder durch Verwendung anerkannter Regeln der Technik noch durch Vergleich mit Referenzsystemen ordnungsgemäß kontrolliert werden können. Somit können geringere Sicherheitsanforderungen gestellt werden, vorausgesetzt, dass das Gesamtsicherheitsniveau aufrechterhalten werden kann.

A.3.7.5. Nur wenn keine anerkannten Regeln der Technik existieren und es auch kein Referenzsystem gibt, ist ein harmonisiertes halbquantitatives Risikoakzeptanzkriterium für technische Systeme notwendig.

A.3.7.6. Die Sicherheitsanforderungsstufe (Safety-Integrity-Level) für systematische Ausfälle/Fehler ist auf SIL 4 begrenzt, entsprechend sind auch zufällige Hardware-Ausfälle technischer Systeme auf SIL 4 zu begrenzen. Dies entspricht einer maximalen tolerierbaren Gefährdungsrate (THR) von $10^{-9}\,h^{-1}$ (d. h. der maximalen Ausfallrate). Wenn höhere Sicherheitsanforderungen verlangt werden, kann dies entsprechend der Norm CENELEC 50 129 nicht mit nur einem System erreicht werden; die Architektur des Systems muss geändert werden, beispielsweise durch Verwendung von zwei Systemen, was unvermeidlich zu einer drastischen Erhöhung der Kosten des technischen Systems führt. Weitere Einzelheiten dazu finden sich in Abschnitt A.3.1 in Anlage A.

A.3.7.7. Schließlich wird in Abschnitt A.3.6 in Anlage A dargelegt, wie das RAC-TS als Bezugspunkt für die Kalibrierung besonderer Risikoanalysemethoden verwendet werden kann, wenn technische Systeme ein Potenzial für Folgen unterhalb der katastrophalen Gefahrenstufe aufweisen.

## A.4. Nachweis aus der Sicherheitsbewertung

A.4.1. Dieser Abschnitt gibt Hinweise zu Nachweisen, wie sie gewöhnlich einer Bewertungsstelle vorgelegt werden, um die unabhängige Bewertung zu ermöglichen und unbeschadet der in einem Mitgliedstaat geltenden nationalen Anforderungen die Abnahme des Systems zu erhalten. Dieser Abschnitt kann als Checkliste verwendet werden, um zu überprüfen, dass im Zuge der Anwendung der CSM, soweit relevant, alle verbundenen Aspekte erfasst und dokumentiert sind.

A.4.2. Sicherheitsplan: Die CENELEC empfiehlt, dass bei Projektbeginn ein Sicherheitsplan vorgelegt wird, oder, falls dies für das Projekt nicht angemessen ist, dass die damit verbundene Beschreibung in ein anderes relevantes Dokument aufgenommen wird. Wenn Bewertungsstellen bei Projektbeginn eingesetzt werden, kann diesen der Sicherheitsplan zur sachverständigen Begutachtung vorgelegt werden. Im Prinzip beschreibt der Sicherheitsplan:

(a) die vorgesehene Organisation und die Kompetenz der an der Entwicklung und an der Risikobewertung beteiligten Personen;

(b) alle sicherheitsbezogenen Aktivitäten, die in den verschiedenen Projektphasen geplant sind, sowie die erwarten Ergebnisse (Outputs).

A.4.3. Erforderliche Nachweise aus der Phase der Systemdefinition:

(a) Systembeschreibung:



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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) Festlegung des Geltungsbereichs und der Grenzen des Systems;
(2) Beschreibung von Funktionen;
(3) Beschreibung der Systemstruktur;
(4) Beschreibung von Betriebs- und Umgebungsbedingungen;

(b) Beschreibung externer Schnittstellen;
(c) Beschreibung interner Schnittstellen;
(d) Beschreibung von Lebenszyklusphasen;
(e) Beschreibung von Sicherheitsgrundsätzen;
(f) Beschreibung der Annahmen, die die Grenzen der Risikobewertung bestimmen.

A.4.4. Um die Durchführung der Risikobewertung zu ermöglichen, muss die Systemdefinition den Kontext der geplanten Änderung berücksichtigen:

(a) Wenn es sich bei der geplanten Änderung um eine Modifizierung eines bestehenden Systems handelt, beschreibt die Systemdefinition sowohl das vor der Änderung bestehende System als auch die geplante Änderung

(b) Wenn es sich bei der geplanten Änderung um den Aufbau eines neuen Systems handelt, ist die Beschreibung auf die Systemdefinition beschränkt, da es keine Beschreibung eines bestehenden Systems gibt.

A.4.5. Erforderliche Nachweise aus der Phase der Gefährdungsermittlung:

(a) Beschreibung und Begründung (einschließlich Begrenzungen) von Verfahren und Werkzeugen für die Gefährdungsermittlung (Top-down-Methode, Bottom-up-Methode, HAZOP, usw.);

(b) Ergebnisse:

(1) Liste der Gefährdungen:
(2) System-(Grenz-)Gefährdungen;
(3) Teilsystemgefährdungen;
(4) Schnittstellengefährdungen;
(5) Die Sicherheitsmaßnahmen, die in dieser Phase ermittelt werden konnten.

A.4.6. Die folgenden Nachweise werden ferner aus Phase der Risikoanalyse benötigt:

(a) Wenn anerkannte Regeln der Technik für die Gefährdungskontrolle verwendet werden: Nachweis darüber, dass alle relevanten Anforderungen aus diesen Regeln der Technik für das zu bewertende System erfüllt werden. Dazu gehört der Nachweis über die ordnungsgemäße Anwendung der einschlägigen Regeln der Technik.

(b) Wenn ähnliche Referenzsysteme für die Gefährdungskontrolle verwendet werden:

(1) Festlegung der Sicherheitsanforderungen aus dem relevanten Referenzsystem für das zu bewertende System;
(2) Nachweis, dass das zu bewertende System unter ähnlichen Umweltbedingungen wie das relevante Referenzsystem verwendet wird. Falls dies nicht möglich ist, ist der Nachweis darüber erbringen, dass die Abweichungen vom Referenzsystem ordnungsgemäß bewertet werden;
(3) Nachweis, dass die Sicherheitsanforderungen aus Referenzsystemen im zu bewertenden System ordnungsgemäß implementiert werden.

(c) Wenn die explizite Risikoabschätzung für die Gefährdungskontrolle verwendet wird:

(1) Beschreibung und Begründung (einschließlich Begrenzungen) von Methoden und Werkzeugen für die Risikoanalyse (qualitative, quantitative, halbquantitative, Non-Regression-Analyse usw.);
(2) Angabe bestehender Sicherheitsmaßnahmen und Risikominderungsfaktoren für jede Gefährdung (einschließlich Aspekte des menschlichen Faktors);



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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) Risikoevaluierung und Risikoeinstufung (Ranking) für jede Gefährdung:

(i) Abschätzung der Gefährdungsfolgen und Begründung (mit Annahmen und Bedingungen);
(ii) Abschätzung der Gefährdungshäufigkeit und Begründung (mit Annahmen und Bedingungen);
(iii) Einstufung der Gefährdungen nach ihrer Folgenschwere und Eintrittshäufigkeit;

(4) Angabe zusätzlicher geeigneter Sicherheitsmaßnahmen für jede Gefährdung die zu akzeptablen Risiken führen (iterativer Prozess nach der Phase der Risikoevaluierung).

A.4.7. Erforderliche Nachweise aus der Risikoevaluierung:

(a) Wenn eine explizite Risikoabschätzung durchgeführt wird:

(1) Festlegung und Begründung von Risikoevaluierungskriterien für jede Gefährdung;
(2) Nachweis/Begründung, dass die Sicherheitsmaßnahmen und Sicherheitsanforderungen für jede einzelne Gefährdung ein akzeptables Niveau bewirken (entsprechend dem oben genannten Risikoevaluierungskriterium);

(b) Gemäß den Abschnitten 2.3.5 und 2.4.3 der CSM-Verordnung werden Risiken, die durch die Anwendung von anerkannten Regen der Technik und durch Vergleich mit Referenzsystemen behandelt werden, implizit als akzeptabel betrachtet, unter der Voraussetzung: (siehe gepunkteten Kreis in Abbildung 1):

(1) dass die Anwendungsbedingungen der anerkannten Regeln der Technik gemäß Abschnitt 2.3.2 erfüllt sind;
(2) dass die Verwendungsbedingungen eines Referenzsystems nach Abschnitt 2.4.2 erfüllt sind.

Die Risikoakzeptanzkriterien gelten implizit für diese beiden Risikoakzeptanzgrundsätze.

A.4.8. Nachweise aus dem Gefährdungsmanagement:

(a) Eintragung aller Gefährdungen in einem Gefährdungsprotokoll mit folgenden Inhaltselementen:

(1) ermittelte Gefährdung;
(2) Sicherheitsmaßnahmen zur Verhinderung des Eintritts der Gefährdung oder zur Minderung der Gefährdungsfolgen;
(3) Sicherheitsanforderungen an die Maßnahmen;
(4) relevanter Teil des Systems;
(5) für Sicherheitsmaßnahmen verantwortlicher Akteur;
(6) Gefährdungsstatus (z. B. offen, gelöst, gelöscht, übertragen, kontrolliert, usw.);
(7) Datum der Eintragung, Überprüfung und Kontrolle jeder einzelnen Gefährdung;

(b) Beschreibung, wie Gefährdungen während des gesamten Lebenszyklus wirksam verwaltet werden;
(c) Beschreibung des Informationsaustausches zwischen den Parteien in Bezug auf Schnittstellengefährdungen und Zuweisung von Verantwortlichkeiten.

A.4.9. Nachweise zur Qualität des Risikoevaluierungs- und Risikobewertungsverfahrens:

(a) Beschreibung von verfahrensbeteiligten Personen und ihrer Kompetenz;
(b) Für explizite Risikoabschätzungen: Beschreibung von im Verfahren verwendeten Informationen, Daten und anderen Statistiken sowie Begründung ihrer Angemessenheit (z. B. Sensitivitätsstudie der verwendeten Daten).

A.4.10. Nachweise der Einhaltung der Sicherheitsanforderungen:



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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) Liste verwendeter Normen;
(b) Beschreibung der konstruktiven Gestaltung und von Betriebsgrundsätzen;
(c) Nachweise über die Anwendung eines sachgerechten Qualitäts- und Sicherheitsmanagementsystems für das Projekt: siehe Punkt [G 3] in Abschnitt 1.1.2;
(d) Zusammenfassung von Sicherheitsanalyseberichten (z. B. Analyse der Gefährdungsursache) als Beleg für die Einhaltung von Sicherheitsanforderungen;
(e) Beschreibung und Begründung von Methoden und Werkzeugen (FMECA, FTA, usw.), die für die Analyse der Gefährdungsursache verwendet werden;
(f) Zusammenfassung der Tests für die Sicherheitsverifizierung und -validierung.

A.4.11. Sicherheitsnachweise: CENELEC empfiehlt die Zusammenführung aller vorstehend genannten Belege und Nachweise in einem zusammenfassenden Dokument, das der Bewertungsstelle vorgelegt wird: siehe Punkte [G 4] und [G 5] in Abschnitt 5.1.



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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

# ANLAGE B: BEISPIELE FÜR TECHNIKEN UND WERKZEUGE ZUR UNTERSTÜTZUNG DES RISIKOBEWERTUNGS-VERFAHRENS

B.1. Beispiele für Techniken und Werkzeuge zur Ausführung der Risikobewertungsaktivitäten entsprechend der CSM finden sich in Anhang E des Leitfadens EN 50126-2 {Ref. 9}. Eine zusammenfassende Übersicht über Techniken und Werkzeuge befindet sich in Tabelle E.1. Jede einzelne Technik ist dort beschrieben und bei Bedarf wird auf andere Normen für weiterführende Informationen verwiesen.



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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

# ANLAGE C: BEISPIELE

## C.1. Einleitung

C.1.1. Diese Anlage soll das Lesen des vorliegenden Dokumentes erleichtern. Er vereint alle gesammelten Beispiele mit dem Ziel, die Anwendung der CSM zu unterstützen.

C.1.2. Die in dieser Anlage enthaltenen Beispiele für Risiko- und Sicherheitsbewertungen sind nicht durch die Anwendung des CSM-Prozesses entstanden, sondern wurden vor der Existenz der CSM-Verordnung durchgeführt. Die Beispiele lassen sich untergliedern in:

(a) Beispiele mit Herkunftsangabe, die von Fachleuten der CSM-Arbeitsgruppe eingebracht wurden;
(b) Beispiele mit absichtlich weggelassener Herkunftsangabe, die ebenso von Fachleuten der CSM-Arbeitsgruppe eingebracht wurden, bei denen jedoch um Vertraulichkeit gebeten wurde.
(c) Beispiele ohne Herkunftsangabe, die von Mitgliedern der Agentur auf Grundlage ihrer früheren Berufserfahrung eingebracht wurden.

Für jedes Beispiel gibt es eine Zuordnung des angewendeten Verfahrens zum geforderten CSM-Prozess sowie Argumentation und Wertbetrachtung für die Durchführung von CSM-seitig geforderten zusätzlichen Schritten (soweit zutreffend).

## C.2. Anwendungsbeispiele für signifikante Änderungskriterien in Artikel 4 Absatz 2

C.2.1. Die Agentur arbeitet derzeit an einer Definition, was als „signifikante Änderung“ anzusehen ist. Ein Beispiel aus dieser Arbeit findet sich im vorliegenden Abschnitt in Bezug auf die Anwendungsweise der Kriterien aus Artikel 4 Absatz 2.

C.2.2. Die Änderung bei einem manuell betriebenen Bahnübergang besteht in der Änderung der Art und Weise der Übermittlung von Richtungsinformationen über einen nahenden Zug vom Stellwärter an den Schrankwärter. Die Änderung ist in Abbildung 15 dargestellt.

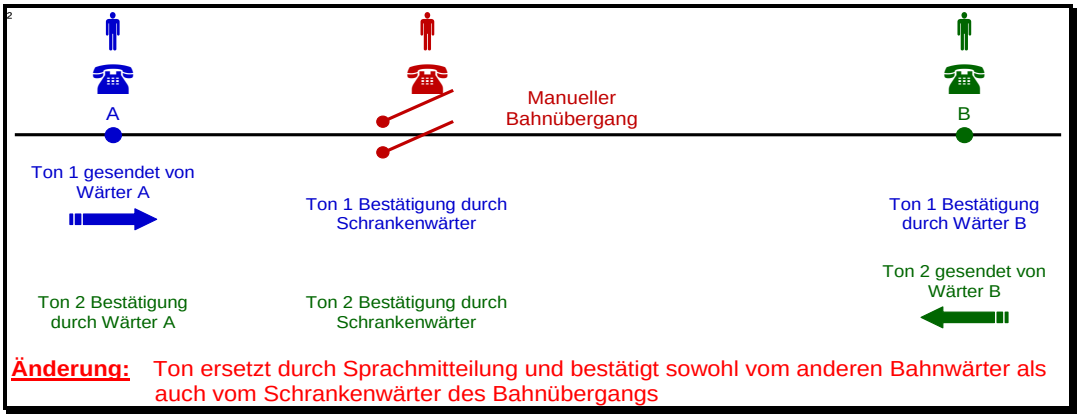


***Abbildung 15 : Beispiel für eine nicht signifikante Änderung – Telefonische Mitteilung für die Bahnübergangskontrolle***

C.2.3. Bestehendes System: Vor der Einführung der geplanten Änderung wurde die Information über die Richtung eines nahenden Zuges dem Schrankenwärter automatisch durch den


European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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

Klingelton des Telefons mitgeteilt. Der Klingelton war unterschiedlich, je nachdem, woher der Anruf kam.

C.2.4. Geplante Änderung: Da das alte Telefonsystem nicht mehr dem heutigen Stand entspricht und durch eine digitale Anlage ersetzt werden muss, können die entsprechenden Informationen technisch nicht mehr durch den Klingelton umgesetzt werden. Der Rufton ist der gleiche, unabhängig davon, von welchem Stellwärter die Mitteilung kommt. Somit wird beschlossen, die gleiche Funktion über ein Betriebsverfahren zu regeln:

(a) Bei Abfahrt des Zuges informiert der Stellwärter den Schrankenwärter verbal über die Fahrtrichtung des nahenden Zuges;
(b) Die Information wird anhand des Fahrplans gegengeprüft und sowohl vom Schrankenwärter als auch vom anderen Stellwärter bestätigt, damit jegliches Missverständnis durch den Schrankenwärter am Bahnübergang vermieden wird.

Die geplante Änderung und die mir ihr verbundene betriebliche Verfahrensweise sind in Abbildung 15 illustriert.

C.2.5. Obwohl die Änderung anscheinend eine mögliche Sicherheitsauswirkung hat (Risiko des nicht rechtzeitigen Schließens der Bahnschranke), deuten andere Kriterien aus Artikel 4 Absatz 2 wie:

(a) geringe Komplexität
(b) fehlende Innovation und
(c) leichte Überwachung.

eher daraufhin, dass es sich bei der geplanten Änderung nicht um eine signifikante Änderung handelt.

C.2.6. Im vorliegenden Beispiel ist jedoch ohnehin ein bestimmter Umfang an Sicherheitsanalyse bzw. Argumentation notwendig, um zu zeigen, dass für diese sicherheitskritische Aufgabe der Ersatz eines alten technischen Systems durch ein Betriebsverfahren (mit Cross-Check zwischen Mitarbeitern) zu einem gleichartigen Sicherheitsniveau führen wird. Die Frage besteht nunmehr darin, ob hier die Anwendung des kompletten CSM-Prozesses mit Gefährdungsprotokoll, unabhängiger Bewertung durch eine Bewertungsstelle usw. gefordert wäre. Im vorliegenden Fall ist es fraglich, ob dies einen Mehrwert hätte, was impliziert, dass eine solche Änderung nicht als signifikante Änderung behandelt werden könnte.

## C.3. Beispiele für Schnittstellen zwischen Akteuren des Eisenbahnsektors

C.3.1. Es folgen einige Beispiele von Schnittstellen und Gründen für die Zusammenarbeit zwischen Akteuren im Eisenbahnsektor:

(a) FB – FB: Zum Beispiel sollen beide Infrastrukturen Sicherheitsmaßnahmen vorsehen, um eine sichere Zugüberführung von einer Infrastruktur zur anderen zu gewährleisten;

(b) FB – EBU: Zum Beispiel könnte es je nach Infrastruktur spezielle Betriebsvorschriften geben, die vom Triebfahrzeugführer zu beachten sind;

(c) FB – Hersteller: Zum Beispiel könnte es für Teilsysteme eines Herstellers Verwendungsbeschränkungen geben, die vom FB einzuhalten sind;

(d) FB – Dienstleister: Zum Beispiel könnte es für die Infrastruktur spezielle Instandhaltungszwänge geben, die vom im Unterauftrag handelnden Instandhaltungsunternehmen zu erfüllen sind;


European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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) EBU – Hersteller: Zum Beispiel könnte es für Teilsysteme eines Herstellers Verwendungsbeschränkungen geben, die vom EBU einzuhalten sind;

(f) EBU – Dienstleister: Zum Beispiel könnte es für die Infrastruktur spezielle Instandhaltungszwänge geben, die vom im Unterauftrag handelnden Instandhaltungsunternehmen zu erfüllen sind;

(g) EBU – Halter: Zum Beispiel könnte es für Fahrzeuge Verwendungsbeschränkungen geben, die vom Eisenbahnunternehmen beim Betrieb dieser Fahrzeuge einzuhalten sind;

(h) Hersteller – Hersteller: Zum Beispiel die Verwaltung von sicherheitsbezogenen technischen Schnittstellen zwischen Teilsystemen zweier unterschiedlicher Hersteller;

(i) Hersteller – Dienstleister: Zum Beispiel die Verwaltung des Gefährdungsprotokolls durch den Hersteller, wenn er einen gewissen Leistungsumfang im Unterauftrag an ein Unternehmen vergibt, das zu klein ist, um eine Sicherheitsorganisation im entsprechenden Projekt zu haben;

(j) Dienstleister – Dienstleister: Analog zu Punkt (i) oben.

C.3.2. Dienstleister übernehmen alle entweder vom FB oder EBU oder Hersteller unterbeauftragten Aktivitäten wie Instandhaltung, Personenabfertigung, Ingenieurleistungen, etc.

C.3.3. Das folgende Beispiel soll das Schnittstellenmanagement und die damit verbundene Gefährdungsermittlung illustrieren. Es behandelt eine Schnittstelle zwischen einem Zughersteller und einem Vorschlagenden (EBU) und beschreibt dann, wie die in Punkt [G 3] von Abschnitt 1.2.1 angegebenen Hauptkriterien erfüllt werden könnten:

(a) Leitung: der Vorschlagende (RU);

(b) Eingaben (Inputs):

(1) Liste(n) relevanter Gefährdungen aus ähnlichen Projekten;
(2) Beschreibung aller Eingaben und Ausgaben (Inputs/Outputs) für die Schnittstelle einschließlich der Leistungsmerkmale;

(c) Methoden: siehe Anhang A.2 des Leitfadens EN 50 126-2 {Ref. 9};

(d) Erforderliche Teilnehmer:

(1) Sicherheitsmanager (Safety Assurance Manager) des Vorschlagenden (EBU);
(2) Sicherheitsmanager (Safety Assurance Manager) des Zugherstellers;
(3) Technischer Projektleiter (Design Authority) des Zug-Vorschlagenden;
(4) Technischer Projektleiter (Design Authority) des Zugherstellers;
(5) Instandhaltungspersonal des Zug-Vorschlagenden (teilweise abhängig von den analysierten Eingaben/Ausgaben);
(6) Triebfahrzeugführer (teilweise abhängig von den analysierten Eingaben/Ausgaben);

(e) Ausgaben (Outputs):

(1) Gemeinsam vereinbarter Bericht über die Gefährdungsermittlung;
(2) Sicherheitsmaßnahmen für das Gefährdungsprotokoll mit einer eindeutigen Beschreibung der Verantwortlichkeiten.



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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. Beispiele für Methoden zur Bestimmung weitgehend akzeptabler Risiken

## C.4.1. Einleitung

C.4.1.1. Weitgehend akzeptable Risiken („*broadly acceptable risks*“) sind in der CSM-Verordnung definiert als Risiken, die *„so gering sind, dass die Einführung zusätzlicher Sicherheitsmaßnahmen (zur weiteren Verminderung des Risikos) nicht angemessen wäre“*. Werden in der Phase der Gefährdungsermittlung ermittelte Gefährdungen so eingestuft, dass sie mit weitgehend akzeptablen Risiken verbunden sind, müssen sie im Risikobewertungsverfahren nicht weiter analysiert werden. Die oben zitierte Definition der weitgehend akzeptablen Risiken lässt einen gewissen Interpretationsspielraum. Deshalb sagt die Verordnung, dass die Entscheidung darüber, ob Gefährdungen mit weitgehend akzeptablen Risiken verbunden sind, durch Sachverständigenurteil zu treffen ist.

C.4.1.2. Es ist in der Tat schwierig, für weitgehend akzeptable Risiken ein expliziteres Kriterium zu finden, das auf alle Systemebenen zutrifft, in denen solche Gefährdungen ermittelt werden könnten, und das auch die für verschiedene Anwendungen unterschiedlichen Risikoaversionsfaktoren berücksichtigt. Da es jedoch wichtig ist, dass das von Sachverständigen getroffene Urteil leicht verständlich und nachvollziehbar ist, sind Hinweise und Anweisungen darüber geboten, wie Risiken als weitgehend akzeptabel zu definieren sind. Kriterien zur Findung weitgehend akzeptabler Risiken können quantitativer, qualitativer oder halbqualitativer Art sein. Unten folgen einige Beispiele für die Herleitung von Kriterien, die die Beurteilung weitgehend akzeptabler Risiken auf quantitative oder halbquantitative Art und Weise ermöglichen.

C.4.1.3. Die nachfolgenden Beispiele illustrieren den genannten Grundsatz. Sie stammen aus dem Artikel: *„Die Gefährdungseinstufung im ERA-Risikomanagementprozess“, Kurz, Milius, Signal +Draht (100) 9/2008.*

## C.4.2. Herleitung eines quantitativen Kriteriums

C.4.2.1. Man könnte weitgehend akzeptable Risiken als Risiken definieren, die für eine gegebene Gefährdungsklasse weitaus kleiner sind als das akzeptable Risiko. Unter Zuhilfenahme statischer Daten könnte es möglich sein, das derzeitige Risikoniveau für Eisenbahnsysteme zu berechnen und somit das berechnete Niveau als akzeptabel zu erklären. Wird das Risikoniveau durch die Anzahl (N) von Gefährdungen geteilt (beispielsweise kann man annehmen, dass es ca. N = 100 Hauptkategorien von Gefährdungen im Eisenbahnsystem gibt), erhält man ein akzeptables Risikoniveau pro Gefährdungsstufe. Anschließend könnte man sagen, dass eine Gefährdung mit einem Risiko zwei Größenordnungen niedriger als das akzeptable Risikoniveau pro Gefährdung (d. h. Parameter x % in Punkt [G 1] von Abschnitt 2.2.3) als weitgehend akzeptables Risiko betrachtet wird.

C.4.2.2. Es ist jedoch zu prüfen, dass der Gesamtbeitrag aller Gefährdungen, die mit (einem) weitgehend akzeptablen Risiko/Risiken verbunden sind, einen bestimmten Anteil (z. B. y%) am Gesamtrisiko auf Systemebene nicht übersteigen darf: Siehe Abschnitt 2.2.3 und Erläuterung in Punkt [G 2] von Abschnitt 2.2.3.

## C.4.3. Beurteilung weitgehend akzeptabler Risiken

C.4.3.1. Mit den in den obigen Beispielen abgeleiteten Grenzwerten für weitgehend akzeptable Risiken können anschließend qualitative Werkzeuge wie eine Risikomatrix, ein Risikodiagramm oder Risikoprioritätszahlen kalibriert werden, um den Sachverständigen bei


European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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

seiner Entscheidung zu unterstützen, ein Risiko als weitgehend akzeptabel einstufen. Hierbei muss unbedingt betont werden, dass der Umstand, dass quantitative Werte als Kriterien für weitgehend akzeptable Risiken vorliegen, nicht zwangsläufig bedeutet, dass eine exakte Risikoabschützung oder Risikoanalyse durchgeführt werden muss, um zu einer Entscheidung zu gelangen, ob das Risiko weitgehend akzeptabel ist. Genau hier kommt das Sachverständigenurteil für eine grobe Abschätzung in der Gefährdungsermittlungsphase zum Tragen.

C.4.3.2. Wichtig ist auch die Prüfung, dass der Gesamtbeitrag aller Gefährdungen, die mit (einem) weitgehend akzeptablen Risiko/Risiken verbunden sind, einen bestimmten Anteil (z. B. y%) am Gesamtrisiko auf Systemebene nicht übersteigen darf: Siehe Abschnitt 2.2.3 und Erläuterung in Punkt [G 2] von Abschnitt 2.2.3.

## C.5. Beispiel der Risikobewertung einer signifikanten organisatorischen Änderung

C.5.1 **Anmerkung:** Diese beispielhafte Risikobewertung geht nicht auf die Anwendung des CSM-Prozesses zurück; sie wurde vor dem Bestehen der CSM durchgeführt. Das Beispiel soll:

(a) die Ähnlichkeiten zwischen den bestehenden Risikobewertungsmethoden und dem CSM-Prozess aufzeigen;
(b) die Verfolgbarkeit zwischen dem bestehenden Prozess und dem von der CSM geforderten Prozess herausarbeiten;
(c) den wertschöpferischen Charakter der Durchführung der von der CSM (ggf.) geforderten zusätzlichen Schritte begründen.

Hierbei ist zu betonen, dass dieses Beispiel lediglich zu Informationszwecken gegeben wird. Es soll dem Leser das Verständnis des CSM-Prozesses erleichtern. Das Beispiel selbst jedoch darf nicht auf eine andere signifikante Änderung übertragen oder als Referenzsystem für eine andere signifikante Änderung eingesetzt werden. Für jede signifikante Änderung muss die Risikobewertung gemäß CSM-Verordnung durchgeführt werden.

C.5.2. Das Beispiel richtet sich auf eine organisatorische Änderung, die vom entsprechenden Vorschlagenden für signifikant erachtet wurde. Zur Beurteilung der Änderung wurde ein Risikobewertungsansatz gewählt.

C.5.3. Ein Zweig der Fahrwegbetreiberorganisation, der bis zur Änderung bestimmte Instandhaltungsaktivitäten ausführte (außer Signalgebung und Telematik), musste in den Wettbewerb mit Fremdunternehmen treten, die im gleichen Bereich tätig waren. Dies führte unmittelbar zur Verringerung des Personals und Umlagerung von Mitarbeitern und Aufgaben innerhalb des in den Wettbewerb überführten separaten Zweiges der FB-Organisation.

C.5.4. Problempunkte für den davon betroffen Fahrwegbetreiber:

(a) Das von der Änderung betroffene FB-Personal war mit Sofortwartungsarbeiten und Notreparaturen beim Auftreten plötzlicher Fehler am Fahrweg betraut. Das Personal führte auch bestimmte geplante oder projektbezogene Wartungs- und Instandhaltungsarbeiten aus wie Gleisstopfen, Gleisbettreinigung, Vegetationskontrolle;

(b) Diese Aufgaben wurden als kritisch für die Sicherheit und Pünktlichkeit des Betriebs angesehen. Folglich war eine Analyse notwendig, um die richtigen Maßnahmen zur Vermeidung einer Verschlechterung der Situation zu finden, da viele Mitarbeiter mit sicherheitsbezogenen Aufgaben aus der FB-Organisation ausscheiden.

(c) Das gleiche Sicherheitsniveau und die gleiche Pünktlichkeit des Zugverkehrs müssen während und nach der Organisationsänderung aufrechterhalten bleiben.



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

C.5.5. Im Vergleich zum CSM-Prozess wurden die folgenden Schritte angewendet (siehe auch Abbildung 1):

(a) Systembeschreibung [Abschnitt 2.1.2]:

(1) Beschreibung der von der bestehenden Organisation (d. h. von der FB-Organisation vor der Änderung) ausgeführten Aufgaben;
(2) Beschreibung der in der FB-Organisation geplanten Änderungen;
(3) die Schnittstellen des „abzutrennenden Zweiges“ mit anderen umgebenden Organisationen oder mit dem physischen Umfeld konnten nur knapp beschrieben werden. Die Grenzen ließen sich nicht 100%-ig darstellen.

(b) Gefährdungsermittlung [Abschnitt 2.2]:

(1) Intensive Ermittlungsarbeit (Brainstorming) durch Sachverständigengruppe:

(i) Feststellung aller durch die beabsichtigte organisatorische Änderung hervorgebrachten Gefährdungen mit einschlägiger Risikowirkung;
(ii) Feststellung möglicher Maßnahmen zur Kontrolle des Risikos.

(2) Gefährdungseinstufung:

(i) nach dem Grad des verbundenen Risikos: hohes, mittleres, geringes Risiko;
(ii) nach der Wirkung der Änderung: erhöhtes, unverändertes, vermindertes Risiko.

(c) Verwendung eines Referenzsystems [Abschnitt 2.4]:

Das System vor der Änderung wurde so eingeschätzt, dass es über ein akzeptables Sicherheitsniveau verfügte. Es wurde also als „Referenzsystem“ verwendet, um die Risikoakzeptanzkriterien (RAC) für die Organisationsänderung herzuleiten.

(d) Explizite Risikoabschätzung und Risikoevaluierung [Abschnitt 2.5]:

Für jede organisationsänderungsbedingte Gefährdung mit erhöhtem Risiko werden Risikominderungsmaßnahmen ermittelt. Das Restrisiko wird mit dem RAC des Referenzsystems verglichen, um festzustellen, ob zusätzliche Maßnahmen vorzusehen sind.

(e) Nachweis der Erfüllung der Sicherheitsanforderungen durch das System [Abschnitt 3]:

(1) Die Risikoanalyse und das Gefährdungsprotokoll zeigen, dass Gefährdungen erst kontrollierbar sind, nachdem sie verifiziert wurden und die Implementierung der Sicherheitsanforderungen (d. h. ausgewählten Sicherheitsmaßnahmen) nachgewiesen ist;
(2) die Risikoanalyse und das Gefährdungsprotokoll waren dynamische Dokumente. Die Wirksamkeit der beschlossenen Maßnahmen wurde regelmäßig überwacht, um festzustellen, ob sich die Bedingungen geändert hatten und Risikoanalyse und Risikoevaluierung einer Aktualisierung bedurften;
(3) falls die implementierten Maßnahmen nicht effektiv genug waren, wurden die Risikoanalyse, die Risikoevaluierung und das Gefährdungsprotokoll aktualisiert und erneut überwacht.

(f) Gefährdungsmanagement [Abschnitt 4.1]:

Die ermittelten Gefährdungen und Sicherheitsmaßnahmen wurden in ein Gefährdungsprotokoll eingetragen und verwaltet. Eine der Schlussfolgerungen im Beispiel bestand in einer kontinuierlichen Aktualisierung der Risikoanalyse und des Gefährdungsprotokolls, da im Zuge der Organisationsänderung Entscheidungen und Maßnahmen getroffen wurden. Auch das Risiko an Schnittstellen z. B. mit Subunternehmern und Auftragnehmern war Teil der Risikoanalyse.

Die Struktur und für das Gefährdungsprotokoll verwendeten Bereiche sowie ein kurzer Auszug finden sich Abschnitt C.16.2 von Anlage C.



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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) Unabhängige Bewertung [Artikel 6]:

Außerdem wurde eine unabhängige Bewertung durch eine Drittstelle durchgeführt:

(1) um zu überprüfen, dass das Risikomanagement und die Risikobewertung ordnungsgemäß durchgeführt wurden;
(2) um zu überprüfen, dass die organisatorische Änderung zweckgeeignet ist und das gleiche Sicherheitsniveau wie vor der Änderung aufrechterhalten kann.

C.5.6. Das Beispiel zeigt, dass es sich bei den für die gemeinsame Sicherheitsmethode erforderlichen Grundsätzen um Methoden handelt, die im Eisenbahnsektor bereits bestehen und bereits für die Bewertung von Risiken bei organisatorischen Änderungen angewendet werden. Die Risikobewertung im Beispiel erfüllt alle Anforderungen aus der CSM. Sie verwendet zwei der drei Risikoakzeptanzkriterien, die im harmonisierten CSM-Ansatz zugelassen sind:

(a) Ein „Referenzsystem“ wird für die Bestimmung der Risikoakzeptanzkriterien verwendet, die für die Evaluierung der Risikoakzeptanz der organisatorischen Änderung notwendig sind;
(b) „Explizite Risikoabschätzung und Risikoevaluierung“ zur:

(1) Analyse der Abweichungen der Änderung gegenüber dem Referenzsystem;
(2) Feststellung von Risikominderungsmaßnahmen für änderungsbedingte erhöhte Risiken;
(3) Beurteilung, ob ein akzeptables Risikoniveau erreicht wird.

## C.6. Beispiel der Risikobewertung einer signifikanten betrieblichen Änderung – Änderung der Fahrstundenzahl

C.6.1. **Anmerkung:** Diese beispielhafte Risikobewertung geht nicht auf die Anwendung des CSM-Prozesses zurück; sie wurde vor dem Bestehen der CSM durchgeführt. Das Beispiel soll:

(a) die Ähnlichkeiten zwischen den bestehenden Risikobewertungsmethoden und dem CSM-Prozess aufzeigen;
(b) die Verfolgbarkeit zwischen dem bestehenden Prozess und dem von der CSM geforderten Prozess herausarbeiten;
(c) den wertschöpferischen Charakter der Durchführung der von der CSM (ggf.) geforderten zusätzlichen Schritte begründen.

Hierbei ist zu betonen, dass dieses Beispiel lediglich zu Informationszwecken gegeben wird. Es soll dem Leser das Verständnis des CSM-Prozesses erleichtern. Das Beispiel selbst jedoch darf nicht auf eine andere signifikante Änderung übertragen oder als Referenzsystem für eine andere signifikante Änderung eingesetzt werden. Für jede signifikante Änderung muss die Risikobewertung gemäß CSM-Verordnung durchgeführt werden.

C.6.2. Das Beispiel betrifft eine betriebliche Änderung, bei der das Eisenbahnunternehmen den Triebfahrzeugführern neue Fahrtrouten und eventuell neue Arbeitszeiten (einschließlich Rotations- und Schichtbetrieb) zuweisen wollte.

C.6.3. Im Vergleich zum CSM-Prozess wurden folgende Schritte angewendet (siehe auch Abbildung 1):

(a) Signifikanz der Änderung [Artikel 4]:

Das Eisenbahnunternehmen führte eine vorläufige Risikobewertung durch, die zu dem Schluss führte, dass die es sich bei der betrieblichen Änderung um eine signifikante Änderung handelte. Da die Triebfahrzeugführer neue Strecken und eventuell außerhalb



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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

ihrer üblichen Arbeitszeiten fahren mussten, konnten mögliche Überfahrungen von Haltsignalen, überhöhte Geschwindigkeiten oder Nichtbeachtung temporärer Geschwindigkeitsbeschränkungen nicht vernachlässigt werden.

Ein Vergleich dieser vorläufigen Risikobewertung mit den Kriterien in Artikel 4 Absatz 2 der CSM-Verordnung zeigt, dass die Änderung auch anhand der folgenden Kriterien als signifikante Änderung eingestuft werden könnte:

(1) Sicherheitsrelevanz: Die Änderung ist sicherheitsrelevant, da sich die Änderung des Arbeitsablaufs der Triebfahrzeugführer katastrophal auswirken könnte;
(2) Folgenschwere: Die oben genannten Fehler der Triebfahrzeugführer haben das Potenzial zur Auslösung von katastrophalen Folgen;
(3) Neuheitsgrad: Potenziell könnte das EBU neue Arbeitsweisen für die Triebfahrzeugführer einführen;
(4) Komplexität der Änderung: Die Veränderung der Fahrstundenzahl kann komplex sein, da dies eine umfassende Bewertung und Modifizierung bestehender Arbeitsbedingungen erforderlich machen könnte.

(b) Systemdefinition [Abschnitt 2.1.2]:

Die ursprüngliche Systemdefinition beschrieb:

(1) Die bestehenden Arbeitsbedingungen: Fahrstundenzahl, Schichtbetrieb usw.;
(2) die Änderungen der Fahrstundenzahlen;
(3) die Schnittstellenproblematik (z. B. Schnittstelle mit Fahrwegbetreiber).

Im Zuge der verschiedenen Wiederholungsläufe wurde die Systemdefinition entsprechend den aus dem Risikobewertungsverfahren stammenden Sicherheitsmaßnahmen aktualisiert. Wesentliche Personalvertreter waren an diesem iterativen Prozess bei der Gefährdungsermittlung und Aktualisierung der Systemdefinition beteiligt.

(c) Gefährdungsermittlung [Abschnitt 2.2]:

Die Gefährdungen und möglichen Sicherheitsmaßnahmen für neue Fahrstrecken und Schichtbetriebsmuster wurden durch Brainstorming einer Sachverständigengruppe ermittelt, zu der auch Vertreter der Triebfahrzeugführer gehörten. Die von den Triebfahrzeugführern unter den neuen Bedingungen zu übernehmenden Aufgaben wurden dahingehend geprüft und bewertet, ob sie die Triebfahrzeugführer, ihr Arbeitspensum, den geografischen Raum und die Arbeitszeit des Schichtsystems beeinflussen.
Das EBU wandte sich auch an die Gewerkschaften zur eventuellen Beibringung zusätzlicher Informationen und überprüfte das Risiko von Übermüdung und Krankenständen, das sich aus einer Erhöhung der infolge längerer Fahrten auf unbekannten Strecken zu leistenden Überstunden möglicherweise ergeben könnte.
Die einzelnen Gefährdungen wurden nach Risikoschwere und Risikofolgen eingestuft (hoch, mittel, gering) und daran wurde die Auswirkung der vorgesehenen Änderung gemessen (erhöhtes, unverändertes, vermindertes Risiko).

(d) Verwendung von anerkannten Regeln der Technik [Abschnitt 2.3]:

Anerkannte Regeln der Technik in Bezug auf Arbeitsstunden und menschliche Ermüdungsrisiken wurden eingesetzt, um die bestehenden Arbeitsbedingungen zu überarbeiten und die neuen Sicherheitsanforderungen zu ermitteln. Die notwendigen Betriebsvorschriften für das neue System der Schichtarbeit wurden entsprechend den anerkannten Regeln der Technik verfasst. Alle wichtigen Parteien waren an den überarbeiteten Betriebsverfahrensvorschriften und an der Einigung über die Durchführung der Änderung beteiligt.

(e) Nachweis der Einhaltung der Sicherheitsanforderungen durch das System [Abschnitt 3]:



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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

Die überarbeiteten Betriebsverfahren wurden in das Sicherheitsmanagementsystem des EBU übernommen. Sie wurden überwacht und ein Prüfverfahren wurde eingerichtet, um sicherzustellen, dass die ermittelten Gefährdungen während des Betriebs des Eisenbahnsystems weiter ordnungsgemäß kontrolliert werden.

(f) Gefährdungsmanagement [Abschnitt 4.1]:

Siehe vorhergehenden Punkt, da bei Eisenbahnunternehmen das Gefährdungs-managementverfahren ein Teil ihres Sicherheitsmanagementsystems für die Aufzeichnung und Verwaltung von Risiken sein kann. Die ermittelten Gefährdungen wurden in ein Gefährdungsprotokoll mitsamt den zur Kontrolle des verbundenen Risikos vorgesehenen Sicherheitsanforderungen (d. h. Verweis auf die überarbeiteten Betriebsverfahrensvorschriften) eingetragen.
Die überarbeiteten Verfahrensvorschriften wurden überwacht und bei Bedarf überprüft, um sicherzustellen, dass die ermittelten Gefährdungen während des Betriebs des Eisenbahnsystems weiterhin ordnungsgemäß kontrolliert werden können.

(g) Unabhängige Bewertung [Artikel 6]:

Das Risikobewertungs- und Risikomanagementverfahren wurde durch eine vom Bewertungsverfahren unabhängige kompetente Person der Gesellschaft des EBU bewertet. Die kompetente Person bewertete sowohl das Verfahren als auch die Ergebnisse, d. h. die ermittelten Sicherheitsanforderungen.

Das EBU berief sich bei seiner Entscheidung zur Inkraftsetzung des neuen Systems auf den von der kompetenten Person vorgelegten unabhängigen Bewertungsbericht.

C.6.4. Das Beispiel zeigt, dass die vom Eisenbahnunternehmen verwendeten Grundsätze und das verwendete Verfahren im Einklang mit der gemeinsamen Sicherheitsmethode stehen. Das Risikomanagement- und Risikobewertungsverfahren erfüllte alle Anforderungen der CSM.

## C.7. Beispiel der Risikobewertung einer signifikanten technischen Änderung (ZZS)

C.7.1. **Anmerkung:** Diese beispielhafte Risikobewertung geht nicht auf die Anwendung des CSM-Prozesses zurück; sie wurde vor dem Bestehen der CSM durchgeführt. Das Beispiel soll:

(a) die Ähnlichkeiten zwischen den bestehenden Risikobewertungsmethoden und dem CSM-Prozess aufzeigen;
(b) die Verfolgbarkeit zwischen dem bestehenden Prozess und dem von der CSM geforderten Prozess herausarbeiten;
(c) den wertschöpferischen Charakter der Durchführung der von der CSM (ggf.) geforderten zusätzlichen Schritte begründen.

Hierbei ist zu betonen, dass dieses Beispiel lediglich zu Informationszwecken gegeben wird. Es soll dem Leser das Verständnis des CSM-Prozesses erleichtern. Das Beispiel selbst jedoch darf nicht auf eine andere signifikante Änderung übertragen oder als Referenzsystem für eine andere signifikante Änderung eingesetzt werden. Für jede signifikante Änderung muss die Risikobewertung gemäß CSM-Verordnung durchgeführt werden.

C.7.2. Das Beispiel bezieht sich auf eine technische Änderung des Zugsteuerungs/Zugsicherungs-systems. Sie wurde vom entsprechenden Hersteller für signifikant erachtet. Zur Beurteilung der Änderung wurde ein Risikobewertungsansatz angewendet.

C.7.3. Beschreibung der Änderung: Bei der Änderung wird eine gleisseitige Schleife vor einem Signal durch ein Teilsystem des Typs „Radio Infill + GSM“ (siehe Abbildung 16) ersetzt.



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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.7.4. Sorge: Aufrechterhaltung des Sicherheitsniveaus des Systems nach der Änderung.

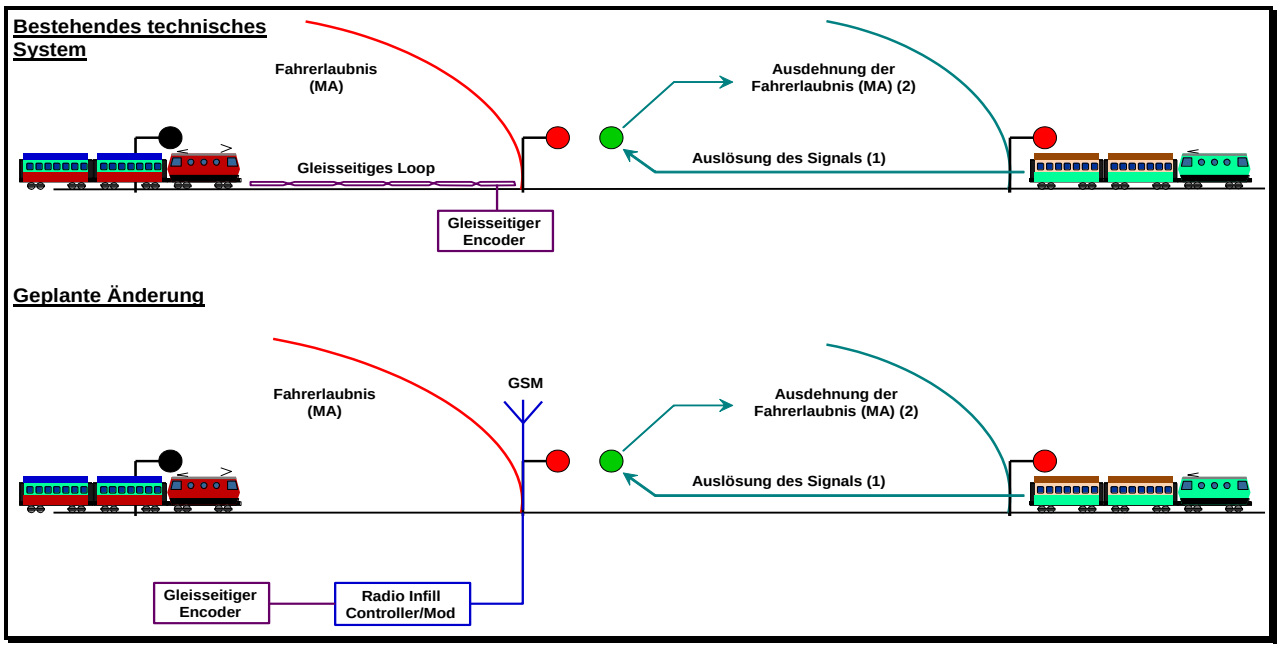


***Abbildung 16 : Änderung eines Loop durch ein Radio-Infill-Teilsystem.***

C.7.5. Im Vergleich zum CSM-Prozess werden folgende Schritte verwendet (siehe auch Abbildung 1):

(a) Bewertung der Signifikanz der Änderung [Artikel 4]

Zur Bewertung der Signifikanz einer Änderung werden die Kriterien aus Artikel 4 Absatz 2 angewendet. Die Entscheidung über die Signifikanz der Änderung beruhte hauptsächlich auf der Komplexität und dem Neuheitsgrad.

(b) Systembeschreibung [Abschnitt 2.1.2]:

(1) Beschreibung des bestehenden Systems: Loop und Loop-Funktionen im Zugsteuerungs-/Zugsicherungssystem;
(2) Beschreibung der vom Vorschlagenden und vom Hersteller geplanten Änderung;
(3) Beschreibung der funktionalen und physischen Schnittstellen des Loop mit dem restlichen System.

Die Funktion „Loop+Encoder“ im bestehenden System gilt der Auslösung des Signals beim Nahen eines Zuges, wenn der Streckenabschnitt hinter dem Signal (d. h. vor dem sich nähernden Zug) frei wird: siehe Abbildung 16.

(c) Gefährdungsermittlung [Abschnitt 2.2]:

Das iterative Risikobewertungsverfahren und die Gefährdungsermittlung (siehe Abschnitt 2.1.1) werden ausgehend von einem Brainstorming einer Sachverständigengruppe angewendet zur:

(1) Ermittlung von Gefährdungen mit einem relevanten Einfluss auf das durch die geplante Änderung eingebrachte Risiko;
(2) Ermittlung möglicher Maßnahmen zur Kontrolle des Risikos.

Da durch den Loop und somit das Radio-Infill das Signal auslöst wird, besteht das Risiko der Erteilung einer unsicheren Fahrerlaubnis (MA - “movement authority”) für den


European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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

sich nähernden Zug, während der vorausfahrende Zug noch den Gleisabschnitt vor dem Signal belegt. Das Risiko muss auf ein akzeptables Niveau gesenkt werden.

(d) Verwendung eines Referenzsystems [Abschnitt 2.4]:

Das System vor der Änderung (Loop) wird so eingeschätzt, dass es ein akzeptables Sicherheitsniveau besitzt. Es wird somit als „Referenzsystem“ verwendet, um die Sicherheitsanforderungen für das Radio-Infill-Teilsystem abzuleiten.

(e) Explizite Risikoabschätzung und Risikoevaluierung [Abschnitt 2.5]:

(1) Die Unterschiede zwischen dem „Loop“-Teilsystem und dem Teilsystem „Radio-Infill+GSM“ werden durch eine explizite Risikoabschätzung und -evaluierung untersucht. Für das Teilsystem „Radio-Infill + GSM“ werden die folgenden neuen Gefährdungen festgestellt:

(i) Einschleusung unsicherer Informationen durch eindringende Hacker in der Luftstrecke, da das Teilsystem „Radio-Infill+GSM“ mit offener Übertragung arbeitet;
(ii) verzögerte Übertragung oder Übertragung gespeicherter Datenpakete in der Luftstrecke.

(2) Explizite Risikoabschätzung und Verwendung des RAC-TS für den Controller-Teil des Radio-Infill-Teilsystems.

(f) Verwendung von anerkannten Regeln der Technik [Abschnitt 2.3]:

(1) Die Norm EN 50159-2 (*„Bahnanwendungen: Teil 2: Sicherheitsrelevante Kommunikation in offenen Übertragungssystemen“*) gibt die Sicherheitsanforderungen für die Kontrolle der neuen Gefährdungen auf akzeptablem Niveau vor, z. B.:

(i) Datenverschlüsselung und Datenschutz;
(ii) Sequenzierung und Zeitstempel.

(2) Verwendung z. B. der Norm EN 50 128 für die Software-Entwicklung des Radio-Infill-Controllers.

(g) Nachweis der Einhaltung der Sicherheitsanforderungen durch das System [Abschnitt 3]:

(1) Nachkontrolle der Implementierung der Sicherheitsmaßnahmen durch den Entwicklungsprozess des Teilsystems „Radio Infill + GSM“;
(2) Verifizierung, dass das System im Konstruktions- und Einbauzustand den Sicherheitsanforderungen genügt.

(h) Gefährdungsmanagement [Abschnitt 4.1]:

Die ermittelten Gefährdungen, die Sicherheitsmaßnahmen und die sich ergebenden Sicherheitsanforderungen aus der Risikobewertung und der Anwendung der drei Risikoakzeptanzgrundsätze werden in einem Gefährdungsprotokoll erfasst und verwaltet.

(i) Unabhängige Bewertung [Artikel 6]:

Eine unabhängige Fremdbewertung wird ebenfalls ausgeführt:

(1) um zu überprüfen, dass das Risikomanagement und die Risikobewertung ordnungsgemäß ausgeführt werden;
(2) um zu überprüfen, dass die technische Änderung zweckgeeignet ist und das gleiche Sicherheitsniveau erfüllt wie vor der Änderung.

C.7.6. Das Beispiel zeigt, dass die drei von der gemeinsamen Sicherheitsmethode geforderten Risikoakzeptanzgrundsätze zur Festlegung der Sicherheitsanforderungen für das zu



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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

bewertende System ergänzend verwendet werden. Die Risikobewertung im Beispiel erfüllt alle Anforderungen aus der CSM, wie in Abbildung 1 zusammenfassend dargestellt, einschließlich Verwaltung des Gefährdungsprotokolls und unabhängige Sicherheitsbewertung durch eine Drittstelle.

## C.8. Beispiel der schwedischen Leitlinie BVH 585.30 für die Risikobewertung von Eisenbahntunneln

C.8.1. **Anmerkung:** Diese beispielhafte Risikobewertung geht nicht auf die Anwendung des CSM-Prozesses zurück; sie wurde vor dem Bestehen der CSM durchgeführt. Das Beispiel soll:

(a) die Ähnlichkeiten zwischen den bestehenden Risikobewertungsmethoden und dem CSM-Prozess aufzeigen;
(b) die Verfolgbarkeit zwischen dem bestehenden Prozess und dem von der CSM geforderten Prozess herausarbeiten;
(c) den wertschöpferischen Charakter der Durchführung der von der CSM (ggf.) geforderten zusätzlichen Schritte begründen.

Hierbei ist zu betonen, dass dieses Beispiel lediglich zu Informationszwecken gegeben wird. Es soll dem Leser das Verständnis des CSM-Prozesses erleichtern. Das Beispiel selbst jedoch darf nicht auf eine andere signifikante Änderung übertragen oder als Referenzsystem für eine andere signifikante Änderung eingesetzt werden. Für jede signifikante Änderung muss die Risikobewertung gemäß CSM-Verordnung durchgeführt werden.

C.8.2. Das Beispiel soll den Prozess in der CSM mit der Leitlinie BVH 585.30 vergleichen, die vom schwedischen Fahrwegbetreiber Banverket für die Gestaltung und Überprüfung der Erreichung eines ausreichenden Sicherheitsniveaus bei der Planung und dem Bau neuer Eisenbahntunnel verwendet wird. Es folgt eine Aufstellung von Gemeinsamkeiten und Unterschieden mit der CSM; die detaillierten Anforderungen an die Risikobewertung sind in der Leitlinie BVH 585.30 zu finden.

C.8.3. Vergleich mit dem CSM-Prozess laut Abbildung 1:

(a) die Leitlinie BVH 585.30 weist die folgenden Gemeinsamkeiten auf:

(1) Systembeschreibung [Abschnitt 2.1.2]:

Die Leitlinie fordert eine detaillierte Systembeschreibung, die Folgendes umfasst:

(i) eine Beschreibung des Tunnels;
(ii) eine Beschreibung der Gleisstrecke;
(iii) eine Beschreibung des Fahrzeugtyps (einschließlich Bordpersonal);
(iv) eine Beschreibung des Verkehrs und des geplanten Betriebs;
(v) eine Beschreibung externer Unterstützungsleistungen (einschließlich Rettungs- und Bergungsdienst).

(2) Gefährdungsermittlung [Abschnitt 2.2]:

Eine Gefährdungsermittlung wird von der Leitlinie nicht ausdrücklich gefordert. Verlangt werden eine Risikoermittlung und ein „Unfallkatalog“ mit den Arten bzw. Typen ermittelter potenzieller Unfälle, bei denen davon ausgegangen wird, dass sie einen signifikanten Einfluss auf das Risikoniveau des Tunnels haben, und die in der nachfolgenden Bewertung zu erfassenden sind. Beispiele für Unfälle:

(i) „Entgleisung eines personenbefördernden Zuges“;
(ii) „Entgleisung eines Güterzuges“;
(iii) „Unfall im Zusammenhang mit Gefahrgut“;



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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

(iv) „Brand im Fahrzeug“;
(v) „Zusammenprall von personenbeförderndem Zug mit leichtem/schwerem Gegenstand“;
(vi) usw.

(3) Es gibt keine Bestimmung für die Anwendung von anerkannten Regeln der Technik oder ähnlichen Referenzsystemen. Es wird davon ausgegangen, dass eine Risikoanalyse in jedem Fall vorzunehmen ist.

(4) Explizite Risikoabschätzung und Risikoevaluierung [Abschnitt 2.5]:

(i) Im Allgemeinen empfiehlt die Leitlinie für jeden Unfalltyp die Durchführung einer kompletten Ereignisbaumanalyse anhand einer quantitativen Risikoanalyse. Da der Zweck der Risikoanalyse jedoch darin besteht, das globale Sicherheitsniveau des Tunnels zu untersuchen und keine Einzelanalyse der Sicherheit auf detaillierterer Ebene vorzunehmen, werden die Ergebnisse aller Szenarien zusammengenommen, um daraus das Gesamt-Risikoniveau für den Tunnel zu bestimmen;

(ii) der Akzeptanzgrad dieses globalen Risikoniveaus für den Tunnel ist mit dem nachfolgenden expliziten quantitativen Risikoakzeptanzkriterium zu vergleichen. *„Der Bahnverkehr pro Kilometer Tunnelstrecke muss genauso sicher sein wie der Bahnverkehr pro Kilometer auf offener Strecke, mit Ausnahme von Bahnübergängen“*. Dieses Kriterium wird anhand von historischen Daten schwedischer Eisenbahnunfälle in eine F-N-Kurve umgewandelt und auf Folgeergebnisse extrapoliert, die in den Statistiken nicht vorhanden sind;

(iii) neben diesem Kriterium des globalen Risikoniveaus des Tunnels gibt es auch zusätzlich zu erfüllende Anforderungen speziell für die Evakuierung in Tunneln und für Möglichkeiten der Rettungs- und Bergungsdienste:

- Verifizierung, dass in einem Zug im Brandfall die Selbstrettung bei einem „größten annehmbaren Unfall“ (Worst-Case-Szenario) möglich ist (es werden auch Bewertungskriterien hierfür angegeben);
- Der Tunnel sollte es von der Planung her ermöglichen, dass Rettungs- und Bergungseinsätze für eine Reihe gegebener Szenarien möglich sind.

(5) Ausgabe (Output) der Risikobewertung [Abschnitt 2.1.6]:

Die Ausgabeelemente der Risikobewertung sind:

(i) eine Liste von Sicherheitsmaßnahmen ausgehend vom Mindeststandard auf Grundlage der TSI-SRT und nationaler Vorschriften, die für die Konstruktion des Tunnels verwendet werden müssen; und
(ii) alle durch die Risikoanalyse als notwendig erkannten zusätzlichen Sicherheitsmaßnahmen unter Angabe ihres jeweiligen Zwecks. Es ist angegeben, dass Maßnahmen in folgender Reihenfolge beschlossen werden sollten:

- Vermeidung von Unfällen;
- Verminderung von Unfallfolgen;
- Erleichterung der Evakuierung;
- Erleichterung von Rettungseinsätzen.

(6) Gefährdungsmanagement [Abschnitt 4.1]:

Das Führen eines Gefährdungsprotokolls wird in der Leitlinie nicht ausdrücklich verlangt. Das hängt damit zusammen, dass es sich um eine globale Bewertung handelt und Gefährdungen deshalb nicht einzeln beurteilt und kontrolliert werden. Die Akzeptanzbeurteilung des globalen Tunnelrisikos erfolgt ohne tiefer gehende



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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

Aufteilung des globalen Risikoakzeptanzkriteriums auf einzelne Unfalltypen oder zugrunde liegende Gefährdungen.

Es gibt jedoch eine Liste aller Sicherheitsmaßnahmen, die einerseits vom „Mindeststandard“ herrühren und andererseits in der Risikoanalyse als notwendig ermittelt wurden: siehe oben Punkt (a)(5)(ii). In der Liste der Sicherheitsmaßnahmen ist anzugeben, ob sie die Tunnel-Infrastruktur, die Gleisstrecke, den Betrieb oder die Fahrzeuge betreffen, und welche Wirkung sie entsprechend der nummerierten Liste in Punkt (a)(5)(ii) beabsichtigen. Die Leitlinie verlangt jedoch keine ausdrückliche Auskunft darüber, welche Gefährdungen von den Sicherheitsmaßnahmen kontrolliert werden und wer für welche Maßnahmen verantwortlich ist.

(7) Unabhängige Bewertung [Artikel 6]:

Eine unabhängige Bewertung durch eine Drittstelle ist Pflicht:

(i) um zu prüfen, dass das von der Leitlinie BVH 585.30 empfohlene Risikobewertungsverfahren ordnungsgemäß durchgeführt wird;
(ii) für eine als akzeptabel betrachtete Risikoanalyse;
(iii) um zu prüfen, dass eindeutig angegeben ist, wie das zukünftige Sicherheitsmanagement im Projekt durchzuführen ist.

Das endgültige Risikoanalyse-Dokument wird vom unabhängigen Begutachter sowie vom Sicherheitskoordinator des Projekts unterzeichnet.

(b) Die Leitlinie BVH 585.30 zeigt Abweichungen in folgenden Aspekten:

(1) Nachweis der Einhaltung der Sicherheitsanforderungen durch das System [Abschnitt 3]:

Die Leitlinie BVH 585.30 verlangt weder eine Verfolgung der Art und Weise, wie die ermittelten Sicherheitsanforderungen umgesetzt werden, noch eine Verifizierung, dass der endgültige Tunnelentwurf die angegebenen Sicherheitsanforderungen erfüllt. Sie beschreibt nur die Art und Weise, wie diese Anforderung zu übertragen ist, um sicherzustellen, dass sie in der Bauphase implementiert wird.

Die Leitlinie gibt die zu verwendenden Sicherheitsanforderungen an, mit denen überprüft wird, dass die Risikoanalyse auf geeignete und transparente Weise durchgeführt wurde und dass sie vom Projekt akzeptiert werden kann.

C.8.4. Zusammenfassend ergibt der Vergleich mit der CSM:

(a) Die BVH 585.30 erfüllt die relevanten Teile der CSM, auch wenn der Anwendungsbereich und Zweck nicht exakt der gleiche ist;
(b) die BVH 585.30 bewertet das Gesamt-Risikoniveau des Bahntunnels;
(c) die Gefährdungen werden nicht einzeln kontrolliert und das Gefährdungsmanagement steht weniger im Mittelpunkt;
(d) der Nachweis der Übereinstimmung mit allen Sicherheitsmaßnahmen und deren ordnungsgemäßer Implementierung ist nicht so ausdrücklich angegeben. In der Leitlinie ist jedoch angegeben, dass die Rolle des Sicherheitskoordinators im Projekt (mit in der BVH 585.30 definierter Funktion und Kompetenz) darin besteht, zu überprüfen, dass die Schlussfolgerungen der Risikoanalyse in den Entwurfsunterlagen und Zeichnungen umgesetzt werden, und ihre ordnungsgemäße Implementierung in der Bauphase zu kontrollieren.

C.8.5. Die CSM sind dahingehend allgemeiner als die BVH 585.30, dass sie die Anwendung dreier unterschiedlicher Risikoakzeptanzgrundsätze anbieten. Die Anwendung der BVH 585.30 im Rahmen der CSM bringt jedoch keine Probleme mit sich, da sie mit der Anwendung des dritten Risikoakzeptanzgrundsatzes, d. h. der expliziten Risikoabschätzung, vereinbar ist.



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● BP 20392 ● F-59307 Valenciennes Cedex ● France ● Tel. +33 (0)3 27 09 65 00 ● Fax +33 (0)3 27 33 40 65 ● http://www.era.europa.eu

## C.9. Beispiel einer Risikobewertung auf Systemebene für die Metro von Kopenhagen

C.9.1. **Anmerkung:** Diese beispielhafte Risikobewertung geht nicht auf die Anwendung des CSM-Prozesses zurück; sie wurde vor dem Bestehen der CSM durchgeführt. Das Beispiel soll:

(a) die Ähnlichkeiten zwischen den bestehenden Risikobewertungsmethoden und dem CSM-Prozess aufzeigen;
(b) die Verfolgbarkeit zwischen dem bestehenden Prozess und dem von der CSM geforderten Prozess herausarbeiten;
(c) den wertschöpferischen Charakter der Durchführung der von der CSM (ggf.) geforderten zusätzlichen Schritte begründen.

Hierbei ist zu betonen, dass dieses Beispiel lediglich zu Informationszwecken gegeben wird. Es soll dem Leser das Verständnis des CSM-Prozesses erleichtern. Das Beispiel selbst jedoch darf nicht auf eine andere signifikante Änderung übertragen oder als Referenzsystem für eine andere signifikante Änderung eingesetzt werden. Für jede signifikante Änderung muss die Risikobewertung gemäß CSM-Verordnung durchgeführt werden.

C.9.2. Das Beispiel betrifft ein komplettes komplexes, führerloses Metrosystem, darin inbegriffen die grundlegenden technischen Teilsysteme (z. B. Automatische Zugsicherung [ATP] und Fahrzeuge) sowie Betrieb und Instandhaltung des Systems. Zur Beurteilung des Systems und der grundlegenden Teilsysteme kam ein Risikobewertungsansatz zur Anwendung. Das Projekt betraf auch die Zertifizierung des SMS der Betreibergesellschaft. Dies soll es dem EBU und dem FB ermöglichen, das Gesamtsystem während seines gesamten Lebenszyklus sicher zu betreiben und instand zu halten.

C.9.3. Im Vergleich zum CSM-Prozess wurden folgende Schritte angewendet (siehe auch Abbildung 1):

(a) Systembeschreibung [Abschnitt 2.1.2]:

(1) Beschreibung der Leistungsanforderungen des Systems;
(2) Beschreibung der Betriebsvorschriften;
(3) eindeutige Beschreibung der Schnittstellen und Verantwortlichkeiten zwischen den verschiedenen Akteuren, insbesondere zwischen den technischen Teilsystemen;
(4) Festlegung von Systemanforderungen auf höherer Ebene (in punkto akzeptabler Unfallhäufigkeit und Festlegung eines ALARP-Bereichs).

(b) Gefährdungsermittlung [Abschnitt 2.2]:

(1) vorläufige Gefährdungsanalyse auf Systemebene;
(2) Funktionsanalyse auf Systemebene unter Berücksichtigung sämtlicher, nicht nur der eindeutig sicherheitskritischen Teilsysteme (z. B. Automatische Zugsicherung und Fahrzeuge), die an den Sicherheitsfunktion teilhaben und eine aktive Rolle bei der Sicherung der Passagier- und Personalsicherheit spielen;
(3) Intensive Koordination zwischen den Akteuren (Auftragnehmern, Teilsystemlieferanten der technischen Teilsysteme und Bauleistungen):

(i) zur systematischen Erkennung aller nach vernünftigem Ermessen vorhersehbaren Gefährdungen;
(ii) zur Ermittlung möglicher Maßnahmen, durch die alle mit den ermittelten Gefährdungen verbundenen Risiken auf ein akzeptables Niveau gesenkt werden.

(c) Verwendung von anerkannten Regeln der Technik [Abschnitt 2.3]:


European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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

Verschiedene Regeln der Technik, Normen und Vorschriften wurden verwendet, z. B.:

(1) BOStrab-Verordnung über den Bau und Betrieb der Straßenbahnen (deutsche Verordnung mit Geltung für Stadtbahnen) und über führerlosen Betrieb;
(2) VDV-Schriften (deutsche Regeln der Technik) zu ausrüstungstechnischen Anforderungen zur Gewährleistung der Passagiersicherheit in Bahnhöfen für führerlosen Betrieb;
(3) CENELEC-Normen für Bahnsysteme (EN 50 126, 50 128 und 50 129). Diese Normen behandeln insbesondere technische Bahnsysteme. Da sie jedoch einen methodologischen Ansatz von allgemeiner Gültigkeit enthalten, wurden sie für die Kopenhagener Metro in starkem Maße übernommen:

    (i) EN 50 126 wurde für die Sicherheitsmanagement- und Risikobewertungs-aktivitäten des kompletten Bahnsystems verwendet;
    (ii) EN 50 129 wurde für das komplette Signalgebungssystem verwendet;
    (iii) EN 50 128 wurde für die Entwicklung der Software (einschließlich Verifizierung und Validierung) der technischen Teilsysteme verwendet.

(4) Brandschutznormen für Tunnel (NEPA 130).
(5) Normen für Bauleistungen (Eurocodes).

(d) Verwendung eines Referenzsystems [Abschnitt 2.4]:

Die Metro musste das Sicherheitsniveau entsprechender moderner Anlagen in Deutschland, Frankreich oder Großbritannien erreichen. Diese bestehenden Systeme wurden als ähnliche Referenzsysteme verwendet, um die Risikoakzeptanzkriterien in punkto akzeptabler Unfallhäufigkeiten für Kopenhagens Metro abzuleiten.

(e) Explizite Risikoabschätzung und Risikoevaluierung [Abschnitt 2.5]:

(1) zur Abschätzung von Risiken in Bezug auf spezifische Gefährdungen;
(2) zur Kontrolle der Tunnelnotbelüftung (einschließlich menschlicher Faktoren in Bezug auf die Feuerwehreinsatzkräfte);
(3) zur Ermittlung von Risikominderungsmaßnahmen;
(4) zur Beurteilung, ob für das gesamte System ein akzeptables Risikoniveau erreicht wird.

(f) Nachweis der Einhaltung der Sicherheitsanforderungen durch das System [Abschnitt 3]:

(1) Führungspersoneller und technischer Arbeitsaufwand entsprechend der Komplexität des Systems zum Nachweis der Systemsicherheit;
(2) Aufteilung von Sicherheitsanforderungen an das System auf die technischen Teilsysteme und Bauleistungen sowie auf alle sicherheitsbezogenen Metrofunktionen;
(3) Nachweis, dass jedes Teilsystem im Endbauzustand seine Sicherheitsanforderungen erfüllt;
(4) für Sicherheitsfunktionen, die von mehr als einem Teilsystem wahrgenommen werden, konnte der Nachweis der Einhaltung der Sicherheitsanforderungen nicht auf Teilsystemebene erbracht werden. Er wurde auf Systemebene durch Einbindung der verschiedenen Teilsysteme, Werkzeuge und Verfahren geführt;
(5) Nachweis, dass das gesamte System den Sicherheitsanforderungen der höheren Ebene erfüllt.

(g) Gefährdungsmanagement [Abschnitt 4.1]:

Die ermittelten Gefährdungen, die verbundenen Sicherheitsmaßnahmen und die daraus resultierenden Sicherheitsanforderungen wurden über ein zentrales Gefährdungsprotokoll registriert und verwaltet. Die Verantwortung für dieses Gefährdungsprotokoll hatte der Sicherheitsleiter des Gesamtprojekts. Auch die während der Konstruktion und Montage festgestellten betrieblichen Gefährdungen sowie die



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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

betriebs- und instandhaltungsbezogenen Gefährdungen wurden in das Gefährdungsprotokoll aufgenommen;

(h) Nachweise aus Risikomanagement und Risikobewertung [Abschnitt 5]:

Die Ergebnisse der Risikobewertung wurden förmlich dokumentiert und durch einen Sicherheitsnachweis entsprechend den Anforderungen der CENELEC-Normen belegt:

(1) Sicherheitsnachweis für Gesamtsystem;
(2) Sicherheitsnachweis für jedes technische Teilsystem (einschließlich Signalgebungsteilsystem und Bauwerke);
(3) Sicherheitsnachweis für Bauwerke (Bahnhöfe, Tunnel, Viadukte, Dämme);
(4) Sicherheitsnachweis für Installation/Montage;
(5) Sicherheitsnachweis für Fahrzeuge;
(6) Sicherheitsnachweis für Betreiber (als Beleg der Zertifizierung des SMS von EBU und FB, d. h. Befähigungsnachweis des Vorschlagenden zum sicheren Betreiben und Instandhalten des Systems).

(i) Unabhängige Bewertung [Artikel 6]:

Der Gesamtprozess wurde nachkontrolliert und von einem unabhängigen Sicherheitsbegutachter im Zusammenwirken mit einer Delegation der Technischen Überwachungsbehörde (d. h. des dänischen Verkehrsministeriums) bewertet. Die Rollen des unabhängigen Sicherheitsbegutachters sind in einschlägigen Regeln der Technik definiert. Dazu gehörten:

(1) Überprüfung der Ordnungsmäßigkeit von Risikomanagement und Risikobewertung;
(2) Überprüfung, dass das System zwecktauglich ist und über den gesamten Lebenszyklus sicher betrieben und instand gehalten wird;
(3) Genehmigungsempfehlung an die Technische Überwachungsbehörde.

C.9.4. Das vollständige Projekt wurde von einem geeigneten Qualitätsmanagementprozess begleitet.

C.9.5. Im Rahmen des Projekts wurden dem Sicherheitsleiter des Vorschlagenden die Nachweise der Zulieferer (d. h. Sicherheitsnachweise und detaillierte Dokumentation für technische Teilsysteme und Bauleistungen) vorgelegt. Diese Nachweise wurden anschließend von der Sicherheitsmanagementorganisation sowie vom unabhängigen Sicherheitsbegutachter überprüft, der seine Schlussfolgerungen in einem Bewertungsbericht darlegte.
Der Bericht des unabhängigen Sicherheitsbegutachters wurde von der Sicherheitsleitung des Vorschlagenden überprüft und dem Vorschlagenden vorgelegt, der der Technischen Überwachungsbehörde (d. h. dem dänischen Verkehrsministerium) alle Akten zur endgültigen Genehmigung vorlegte.

C.9.6. Das Beispiel zeigt, dass die von der gemeinsamen Sicherheitsmethode geforderten Grundsätze als Methoden im Eisenbahnsektor bereits bestehen. Die Risikobewertung im genannten Beispiel erfüllt alle Anforderungen aus der CSM. Insbesondere verwendet sie alle drei Risikoakzeptanzgrundsätze, die vom harmonisierten Ansatz der CSM zugelassen sind.

## C.10. Beispiel des OTIF-Leitfadens für die Berechnung von Risiken durch die Eisenbahnbeförderung gefährlicher Güter

C.10.1. **Anmerkung:** Diese beispielhafte Risikobewertung geht nicht auf die Anwendung des CSM-Prozesses zurück; sie wurde vor dem Bestehen der CSM durchgeführt. Das Beispiel soll:



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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) die Ähnlichkeiten zwischen den bestehenden Risikobewertungsmethoden und dem CSM-Prozess aufzeigen;
(b) die Verfolgbarkeit zwischen dem bestehenden Prozess und dem von der CSM geforderten Prozess herausarbeiten;
(c) den wertschöpferischen Charakter der Durchführung der von der CSM (ggf.) geforderten zusätzlichen Schritte begründen.

Hierbei ist zu betonen, dass dieses Beispiel lediglich zu Informationszwecken gegeben wird. Es soll dem Leser das Verständnis des CSM-Prozesses erleichtern. Das Beispiel selbst jedoch darf nicht auf eine andere signifikante Änderung übertragen oder als Referenzsystem für eine andere signifikante Änderung eingesetzt werden. Für jede signifikante Änderung muss die Risikobewertung gemäß CSM-Verordnung durchgeführt werden.

C.10.2. Der OTIF-Leitfaden steht von seiner Gesamtphilosophie her im Einklang mit dem Zweck der CSM, hat jedoch einen geringeren Geltungsumfang. Die Zielstellung des OTIF-Leitfadens besteht darin, *„einen einheitlicheren Ansatz für die Risikobewertung der Gefahrgutbeförderung in den COTIF-Mitgliedstaaten und demzufolge eine Vergleichbarkeit der einzelnen Risikobewertungen zu erreichen“*. Er unterstützt damit die gegenseitige Anerkennung von Risikobewertungen der Eisenbahnbeförderung gefährlicher Güter im Rahmen der COTIF-Mitgliedstaaten.

C.10.3. Vergleich mit der CSM und dem Ablauf nach Abbildung 1:

(a) Der OTIF-Leitfaden weist die folgenden Übereinstimmungen auf:

(1) Es handelt sich um einen gemeinsamen Ansatz der Risikobewertung; er beruht jedoch ausschließlich auf der expliziten Risikoabschätzung (d. h. auf dem dritten Risikoakzeptanzgrundsatz der CSM).
(2) Die Risikobewertung nach OTIF umfasst:

(i) eine Phase der Risikoanalyse mit:

- einer Phase der Gefährdungsermittlung;
- einer Phase der Risikoabschätzung;

(ii) eine Phase der Risikobeurteilung anhand von derzeit noch nicht harmonisierten Risiko-(Akzeptanz-)Kriterien. Diese Kriterien können von zahlreichen nationalen Spezifika beeinflusst sein.

(j) Der OTIF-Leitfaden zeigt folgende Unterschiede:

(1) Der Geltungsbereich ist unterschiedlich. Während die Geltung der CSM nur signifikante Änderungen am Eisenbahnsystem betrifft, ist der OTIF-Leitfaden für die Bewertung von Risiken des Gefahrguttransports auf der Schiene anzuwenden, unabhängig davon, ob eine signifikante Änderung des Schienensystems vorliegt oder nicht.

(2) Es gibt keine Wahlmöglichkeit zwischen drei Risikoakzeptanzkriterien zur Kontrolle des Risikos bzw. der Risiken. Zugelassen ist nur der dritte Grundsatz, d. h. die explizite Risikoabschätzung. Ferner muss die Bewertung ausschließlich anhand einer quantitativen, nicht qualitativen Abschätzung erfolgen. Die qualitative Risikoanalyse kann nur für den Vergleich von alternativen (Sicherheits-) Maßnahmen zur Risikominderung in Frage kommen.

(3) Es wird die Anwendung des ALARP-Grundsatzes verlangt, um zu bestimmen, ob zusätzliche Sicherheitsmaßnahmen das bewertete Risiko mit vernünftigem Aufwand weiter vermindern könnten.

(4) Es gibt kein Konzept der Verbindung von „Gefährdungen mit weitgehend akzeptablen Risiken“, was eine Konzentration der Risikobewertung auf die


European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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

relevantesten Gefährdungen ermöglichen würde. Dennoch wird im Leitfaden empfohlen, die Anzahl möglicher Unfallszenarien auf eine angemessene Anzahl von grundlegenden Szenarien zu reduzieren (siehe Abschnitt § 3.2 in {Ref. 10}).

(5) Das Verfahren konzentriert sich auf die Risikobewertung, beinhaltet aber nicht:

(i) das Verfahren für die Auswahl und Umsetzung von (Sicherheits-)Maßnahmen zur Änderung des Risikos;
(ii) das Verfahren für die Risikoakzeptanz;
(iii) das Verfahren für den Nachweis der Einhaltung der Sicherheitsanforderungen;
(iv) das Verfahren für die Mitteilung des Risikos an andere betroffene Akteure (siehe nachfolgenden Punkt).

(6) Der Leitfaden enthält keine Richtlinien über die vom Risikobewertungsverfahren vorzulegenden Nachweisunterlagen.
(7) Gefährdungsmanagement wird nicht verlangt.
(8) Nicht verlangt wird die unabhängige Bewertung der ordnungsgemäßen Anwendung des gemeinsamen Verfahrensansatzes durch einen Dritten.

C.10.4. Der Vergleich zwischen dem OTIF-Leitfaden und der CSM zeigt, dass beide miteinander kompatibel sind, auch wenn Anwendungsbereich und Zweck nicht exakt identisch sind. Die CSM ist allgemeiner, im Sinne von flexibler, als der OTIF-Leitfaden. Andererseits umfasst die CSM auch mehr Risikomanagement-Aktivitäten:

(a) Sie erlaubt die Verwendung von drei Risikoakzeptanzgrundsätzen, die sich auf bestehende Eisenbahnpraxis gründen: siehe Abschnitt 2.1.4;
(b) ihre Anwendung wird nur für signifikante Änderungen gefordert und eine weitergehende Risikoanalyse wird nur für Gefährdungen verlangt, die nicht mit einem weitgehend akzeptablen Risiko verbunden sind;
(c) sie beinhaltet die Auswahl und Implementierung der Sicherheitsmaßnahmen, die die ermittelten Gefährdungen und die verbundenen Risiken kontrollieren sollen;
(d) sie harmonisiert das Risikomanagementverfahren, u. a.:

(1) Harmonisierung der Risikoakzeptanzkriterien im Rahmen der weiteren Behandlung von weitgehend akzeptablen Risiken und Risikoakzeptanzkriterien durch die Agentur;
(2) Nachweis der Einhaltung der Systemanforderungen durch das System;
(3) Ergebnisse und Nachweise aus dem Risikobewertungsverfahren;
(4) Austausch von sicherheitsbezogenen Informationen zwischen den an Schnittstellen beteiligten Akteuren;
(5) Verwaltung aller ermittelten Gefährdungen und verbundenen Sicherheitsmaßnahmen in einem Gefährdungsprotokoll;
(6) unabhängige Bewertung der ordnungsgemäßen Anwendung der CSM durch eine Drittstelle.

C.10.5. Die Anwendung des OTIF-Leitfadens innerhalb der CSM (falls die Gefahrgutbeförderung eine signifikante Änderung für einen FB oder ein EBU darstellt) ist jedoch problemlos möglich, da er mit dem dritten Grundsatz der expliziten Risikoabschätzung vereinbar ist.

## C.11. Beispiel der Risikobewertung einer Anwendung zur Genehmigung eines neuen Fahrzeugtyps

C.11.1. **Anmerkung:** Diese beispielhafte Risikobewertung geht nicht auf die Anwendung des CSM-Prozesses zurück; sie wurde vor dem Bestehen der CSM durchgeführt. Das Beispiel soll:



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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) die Ähnlichkeiten zwischen den bestehenden Risikobewertungsmethoden und dem CSM-Prozess aufzeigen;
(b) die Verfolgbarkeit zwischen dem bestehenden Prozess und dem von der CSM geforderten Prozess herausarbeiten;
(c) den wertschöpferischen Charakter der Durchführung der von der CSM (ggf.) geforderten zusätzlichen Schritte begründen.

Hierbei ist zu betonen, dass dieses Beispiel lediglich zu Informationszwecken gegeben wird. Es soll dem Leser das Verständnis des CSM-Prozesses erleichtern. Das Beispiel selbst jedoch darf nicht auf eine andere signifikante Änderung übertragen oder als Referenzsystem für eine andere signifikante Änderung eingesetzt werden. Für jede signifikante Änderung muss die Risikobewertung gemäß CSM-Verordnung durchgeführt werden.

C.11.2. Dieses Beispiel einer Risikobewertung richtet sich auf eine Anwendung zur Genehmigung eines neuen Fahrzeugtyps. Es wurde eine Risikoanalyse durchgeführt, um die Risiken in Bezug auf die Einführung eines neuen Güterwagens zu beurteilen.

C.11.3. Zweck der Änderung war die Erhöhung von Effektivität, Kapazität, Leistung und Zuverlässigkeit für die Beförderung von Schüttgütern auf einer speziellen Güterstrecke. Da die Wagen für den grenzüberschreitenden Schienenverkehr bestimmt waren, wurde auch eine Zulassung von zwei verschiedenen NSA benötigt. Der Vorschlagende war der Frachtbetreiber, der im Eigentum der Gesellschaft stand, die die zu befördernden Güter produzierte.

C.11.4. Die Projektentwicklung umfasste den Bau, die Herstellung, die Montage, die Inbetriebnahme und die Verifizierung der neuen Fahrzeuge. Die Risikoanalyse erfolgte zur Verifizierung, dass der neue Entwurf die Sicherheitsanforderungen für jedes einzelne Teilsystem ebenso wie für das Gesamtsystem erfüllt.

C.11.5. In der Risikoanalyse wird auf die Verfahren und Definitionen der CENELEC EN 50126 verwiesen und die Risikoevaluierung erfolgt gemäß dieser Norm.

C.11.6. Im Vergleich zum CSM-Prozess wurden folgende Schritte angewendet:

(a) Systembeschreibung [Abschnitt 2.1.2]:

Für die einzelnen Entwurfs- und Konstruktionsphasen gab es Anforderungen an die Dokumentation der Sicherheitsverifizierung und an die Beschreibung des Systementwurfs:

(1) Konzeptionsphase: vorläufige Beschreibung der Betriebsanforderungen des Betreibers;
(2) Spezifikationsphase: funktionale Spezifikation, geltende technische Normen und Standards, Prüfungs- und Verifizierungsplan. Betreiberseitige Anforderungen an die Verwendung und Wartung des Wagens wurden eingearbeitet;
(3) Fertigungsphase: technische Dokumentation der Herstellers einschließlich Zeichnungen, Normen, Berechnungen, Analyse usw. Eine detaillierte Risikoanalyse für neue oder innovative Entwürfe oder neue Einsatzbereiche;
(4) Verifizierungsphase:

(i) Herstellerseitige Verifizierung des technischen Leistungsvermögens des Güterwagens (Prüfberichte, Berechnungen, Verifizierungen entsprechend den Normen und Funktionsanforderungen);
(ii) Dokumentierung von Risikominderungsmaßnahmen und Prüfberichte für den Nachweis der Übereinstimmung des Wagens mit der Bahninfrastruktur;
(iii) Instandhaltungs- und Schulungsunterlagen, Nutzerhandbücher usw.



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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) Abnahmephase:

(i) Sicherheitserklärung des Herstellers und Sicherheitsnachweis;
(ii) Abnahme des Güterwagens und seiner Dokumentation durch den Betreiber.

(b) Gefährdungsermittlung [Abschnitt 2.2]:

Die Gefährdungsermittlung wurde in allen Entwurfs- und Konstruktionsphasen kontinuierlich durchgeführt. Zuerst wurde ein „Bottom-up"-Verfahren verwendet, bei dem die verschiedenen Hersteller Risikoabfolgen im Falle des Ausfalls von Komponenten ihres Teilsystems beurteilten. Die Aufgliederung in Teilsysteme war folgende:

(1) Chassis;
(2) Bremssystem;
(3) Zentralkupplung;
(4) usw.

Anschließend wurde ein ergänzendes „Top-down"-Verfahren zur Feststellung von Fehlstellen oder fehlenden Informationen angewendet. Risiken, die nicht unmittelbar akzeptiert werden konnten, wurden zur weiteren Bearbeitung und Einstufung in das Gefährdungsprotokoll überführt.

(c) Verwendung von Risikoakzeptanzgrundsätzen [Abschnitt 2.1.4]:

Das System als Ganzes wurde einer expliziten Risikoabschätzung unterzogen. Zur Bewertung einzelner Gefährdungen konnten jedoch anerkannte Regeln der Technik oder ähnliche Referenzsysteme verwendet werden. Der Grundsatz besteht darin, dass jedes neue Teilsystem mindestens ebenso sicher sein muss wie das von ihm ersetzte Teilsystem, was letztlich dazu führt, dass das neue komplette System ein höheres Sicherheitsniveau aufweist als das vorhergehende. Ermittelte Gefährdungen wurden mit der Risikomatrix EN 50126 dargestellt. Darüber hinaus wurden verschiedene zusätzliche Risikoakzeptanzkriterien angewendet, unter anderem:

(1) Ein Einzelausfall darf nicht zu einer Situation führen, in der Menschen, Material oder Umwelt schwerwiegend beeinträchtigt werden;
(2) falls durch technische bauliche Mittel nicht vermeidbar, ist dies durch Betriebsvorschriften oder Instandhaltungsanforderungen zu verhindern. Dies galt nur für Gefährdungen, bei denen der eingetretene Fehler erkannt werden kann, bevor er eine gefährliche Situation bewirkt;
(3) für Komponenten, die eine hohe Ausfallwahrscheinlichkeit haben oder bei denen Ausfälle durch Instandhaltungs- oder Betriebsvorschriften nicht vorab erkennbar oder vermeidbar sind, sind zusätzliche Sicherheitsfunktionen und Sicherheitsbarrieren zu berücksichtigen;
(4) redundante Systeme mit Komponenten, bei denen sich während des Betriebs unerkennbare Ausfälle entwickeln können, sind durch Instandhaltungsmaßnahmen zu schützen, damit eine verminderte Redundanz vermieden wird;
(5) das daraus resultierende endgültige Sicherheitsniveau war ein Leitungsbeschluss anhand einer quantitativen und qualitativen Risikoanalyse.

(d) Nachweis der Einhaltung der Sicherheitsanforderungen durch das System [Abschnitt 3]:

Alle ermittelten Risiken und Gefährdungen wurden in einem Verzeichnis aufgelistet, das ständig konsultiert und aktualisiert wurde. Verbleibende Gefährdungen wurden gemeinsam mit der entsprechenden Liste von bei Bau, Betrieb und Instandhaltung zu ergreifenden Risikoreduzierungsmaßnahmen in das Gefährdungsprotokoll aufgenommen. Auf dieser Grundlage wurde ein abschließender Sicherheitsbericht mit Verifizierung der erfolgten Implementierung der Sicherheitsanforderungen erstellt;



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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) Gefährdungsmanagement [Abschnitt 4.1]:

Wie oben angegeben, wurden die Gefährdungen und ihre entsprechenden Sicherheitsmaßnahmen in ein Gefährdungsprotokoll eingetragen, das rückverfolgbaren Aufschluss über alle ermittelten Gefährdungen und Sicherheitsmaßnahmen gibt. Gefährdungen in Bezug auf Risiken, die ohne Gegenmaßnahmen akzeptabel waren, wurden jedoch nicht in das Gefährdungsprotokoll aufgenommen;

(f) Unabhängige Bewertung [Artikel 6]:

Eine unabhängige Bewertung war in den übergebenen Dokumenten dieser signifikanten Änderung nicht erwähnt.

C.11.7. Das Risikobewertungsbeispiel gründet sich auf die CENELEC-Norm EN 50126 und zeigt deshalb eine gute Übereinstimmung mit dem CSM-Prozess. Die im Beispiel genannte Risikobewertung erfüllt alle Anforderungen aus der CSM, abgesehen von der Anforderung einer unabhängigen Bewertung, was aus den übergebenen Dokumenten nicht eindeutig hervorging. Explizite Risikoakzeptanzkriterien wurden verwendet und waren eindeutig angegeben.

## C.12. Beispiel der Risikobewertung einer signifikanten betrieblichen Änderung – Übergang zu Einmannbetrieb

C.12.1. **Anmerkung:** Diese beispielhafte Risikobewertung geht nicht auf die Anwendung des CSM-Prozesses zurück; sie wurde vor dem Bestehen der CSM durchgeführt. Das Beispiel soll:

(a) die Ähnlichkeiten zwischen den bestehenden Risikobewertungsmethoden und dem CSM-Prozess aufzeigen;
(b) die Verfolgbarkeit zwischen dem bestehenden Prozess und dem von der CSM geforderten Prozess herausarbeiten;
(c) den wertschöpferischen Charakter der Durchführung der von der CSM (ggf.) geforderten zusätzlichen Schritte begründen.

Hierbei ist zu betonen, dass dieses Beispiel lediglich zu Informationszwecken gegeben wird. Es soll dem Leser das Verständnis des CSM-Prozesses erleichtern. Das Beispiel selbst jedoch darf nicht auf eine andere signifikante Änderung übertragen oder als Referenzsystem für eine andere signifikante Änderung eingesetzt werden. Für jede signifikante Änderung muss die Risikobewertung gemäß CSM-Verordnung durchgeführt werden.

C.12.2. Das Beispiel betrifft eine betriebliche Änderung, bei der das Eisenbahnunternehmen zu dem Entschluss kam, dass auf einer Strecke, wo bis dato der Triebfahrzeugführer von einem Zugbegleiter/Zugführer in der Zugabfertigung unterstützt wurde, der Zug künftig vom Triebfahrzeugführer im Einmannbetrieb zu fahren ist (Driver Only Operated – DOO).

C.12.3. Im Vergleich zum CSM-Prozess wurden folgende Schritte angewendet (siehe auch Abbildung 1):

(a) Signifikanz der Änderung [Artikel 4]:

Das Eisenbahnunternehmen führte eine vorläufige Risikobewertung mit dem Ergebnis durch, dass es sich bei der betrieblichen Änderung um eine signifikante Änderung handelte. Da der Triebfahrzeugführer den Zug ohne Unterstützung allein führen musste, konnte die potenzielle Gefahr, dass Passagiere in den Türen eingeklemmt werden oder auf das Gleis stürzen (z. B. beim Öffnen der Türen auf der falschen Seite), nicht vernachlässigt werden.



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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

Beim Vergleich dieser vorläufigen Risikobewertung mit den Kriterien in Artikel 4 der CSM-Verordnung könnte die Änderung auch anhand der folgenden Kriterien als signifikant eingestuft werden:

(1) Sicherheitsrelevanz: Die Änderung ist sicherheitsrelevant, da die Anforderung einer vollkommen anderen Art der Betriebsführung des Zugfahrdienstes sich katastrophal auswirken könnte;
(2) Folgenschwere: das Verhalten des Triebfahrzeugführers könnte potenziell katastrophale Folgen haben, wenn der Betrieb nicht effektiv kontrolliert wird;
(3) Neuheitsgrad: Der Einmannbetrieb des Zuges kann innovative Zugbetriebsarten erfordern, deren Risiken bewertet werden müssen.

(b) Systemdefinition [Abschnitt 2.1.2]:

In der Systemdefinition waren beschrieben:

(1) das bestehende System mit eindeutiger Angabe, welche Aufgaben vom Triebfahrzeugführer und welche anderen Aufgaben vom Zugpersonal (oder Zugbegleiter) in Unterstützung des Triebfahrzeugführers durchgeführt wurden;
(2) die Änderung des Aufgabenspektrums des Triebfahrzeugführers aufgrund des Verzichts auf das Zugbegleitpersonal;
(3) die technischen Anforderungen an das System zur Aufnahme der Betriebsänderungen;
(4) die bestehenden Schnittstellen zwischen dem Zugbegleitpersonal, dem Triebfahrzeugführer und dem Streckenpersonal des Fahrwegbetreibers.

Im Zuge der Wiederholungsabläufe wurde die Systemdefinition mit den Sicherheitsanforderungen aus dem Risikobewertungsverfahren aktualisiert. Wesentliche Personen (einschließlich Triebfahrzeugführer, Personalvertreter und Fahrwegbetreiber) waren an diesem iterativen Prozess der Gefährdungsermittlung and Aktualisierung der Systemdefinition beteiligt.

(c) Gefährdungsermittlung [Abschnitt 2.2]:

Die Gefährdungen und möglichen Sicherheitsmaßnahmen wurden durch ein Brainstorming einer Sachverständigengruppe ermittelt, zu der unter anderem gehörten:

(1) Triebfahrzeugführer- und Personalvertreter wegen ihrer Betriebserfahrungen;
(2) Vertreter des FB, da auch die Infrastruktur von der Änderung betroffen sein könnte, beispielsweise durch Änderungen in den Bahnhöfen (z. B. Montage von Spiegeln/Videoüberwachungsanlagen [CCTV] auf Bahnsteigen).

Die vom Triebfahrzeugführer auszuführenden zusätzlichen Aufgaben wurden eingehend geprüft, um alle vorhersehbaren Gefährdungen zu ermitteln, die nach Verzicht auf das Zugbegleitpersonal eintreten könnten. Die Gefährdungsermittlung richtete sich insbesondere auf die wesentlichen betrieblichen Gefährdungen an Bahnhöfen, an bestehenden Strecken mit bisheriger Unterstützung durch Begleit- und streckenseitigem Personal, einschließlich der sicheren Zugabfertigung, spezifische Fragen in Bezug auf den Triebfahrzeugführer, das Fahrzeug (z. B. Kontrolle der Öffnung/Schließung der Türen), Instandhaltungsanforderungen usw.

Den einzelnen ermittelten Gefährdungen wurde ein Risikoniveau mit Folgenschwere zugewiesen (hoch, mittel, niedrig), in Bezug auf welches die Auswirkung der geplanten Änderung eingestuft wurde (erhöhtes, unverändertes, vermindertes Risiko).

(d) Verwendung anerkannter Regeln der Technik [Abschnitt 2.3] und Verwendung ähnlicher Referenzsysteme [Abschnitt 2.4]:

Sowohl anerkannte Regeln der Technik (d. h. ein Normensatz für Einmannbetrieb) als auch ähnliche Referenzsysteme wurden verwendet, um die Sicherheitsanforderungen



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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

für die ermittelten Gefährdungen festzulegen. Diese Sicherheitsanforderungen beinhalteten u. a.:

(1) die überarbeiteten Betriebsverfahrensvorschriften für den Triebfahrzeugführer, die für den sicheren Betrieb der Züge ohne Unterstützung von Zugbegleitungspersonal erforderlich sind;
(2) notwendige zusätzliche fahrzeugseitige oder streckenseitige Ausrüstungen zur Gewährleistung sicherer und zuverlässiger Mittel der Zugabfertigung;
(3) eine Checkliste zur Eignungskontrolle der Führerkabine unter Berücksichtigung der Schnittstelle zwischen dem Eisenbahnsystem (sowohl fahrzeugseitig als auch streckenseitig) und dem Triebfahrzeugführer.

Die notwendigen Betriebsvorschriften wurden in Übereinstimmung mit den geltenden Regeln der Technik und den relevanten Referenzsystemen überarbeitet. Alle wesentlichen Parteien waren an der Überarbeitung der Betriebsverfahrensvorschriften und an der Einigung über die Durchführung der Änderung beteiligt.

(e) Nachweis der Einhaltung der Sicherheitsanforderungen durch das System [Abschnitt 3]:

Das System wurde in Übereinstimmung mit den ermittelten Sicherheitsanforderungen implementiert (zusätzliche Ausrüstungen und geänderte Verfahrensweisen). Diese wurden als geeignete Mittel zur Gewährleistung eines ausreichenden Sicherheitsniveaus des bewerteten Systems verifiziert.

Die überarbeiteten Betriebsverfahrensvorschriften wurden in das Sicherheits-managementsystem des EBU übernommen. Sie wurden überwacht und bei Bedarf überprüft, um sicherzustellen, dass die ermittelten Gefährdungen während des Betriebs des Eisenbahnsystems weiter ordnungsgemäß kontrolliert werden.

(f) Gefährdungsmanagement [Abschnitt 4.1]:

Siehe obigen Punkt, da bei Eisenbahnunternehmen das Gefährdungsmanagement-verfahren Teil ihres Sicherheitsmanagementsystems zur Aufzeichnung und Verwaltung Risiken sein kann. Die ermittelten Gefährdungen wurden in einem Gefährdungsprotokoll gemeinsam mit den Sicherheitsanforderungen verzeichnet, die das verbundene Risiko kontrollieren, d. h. mit Verweis auf zusätzliche fahrzeug- und streckenseitige Ausrüstungen sowie Verweis auf die überarbeiteten Betriebsverfahrensvorschriften.
Die überarbeiteten Betriebsverfahren wurden überwacht und bei Bedarf überprüft, um sicherzustellen, dass die ermittelten Gefährdungen während des Betriebs des Eisenbahnsystems weiter ordnungsgemäß kontrolliert werden.

(g) Unabhängige Bewertung [Artikel 6]:

Das Risikobewertungsverfahren und das Risikomanagementverfahren wurden durch eine kompetente, vom Bewertungsverfahren unabhängige Person aus der EBU-Gesellschaft bewertet. Die kompetente Person bewertete sowohl das Verfahren als auch die Ergebnisse, d. h. die ermittelten Sicherheitsanforderungen.

Das EBU gründete seine Entscheidung für das Inkrafttreten des neuen Systems auf den von der kompetenten Person vorgelegten unabhängigen Bewertungsbericht.

C.12.4. Das Beispiel zeigt, dass die vom Eisenbahnunternehmen verwendeten Grundsätze und Prozesse mit der gemeinsamen Sicherheitsmethode übereinstimmen. Das Risikomanagement- und Risikobewertungsverfahren erfüllte alle Anforderungen der CSM.



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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. Beispiel für die Verwendung eines Referenzsystems zur Ableitung von Sicherheitsanforderungen für neue elektronische Stellwerksysteme in Deutschland

C.13.1. **Anmerkung:** Diese beispielhafte Risikobewertung geht nicht auf die Anwendung des CSM-Prozesses zurück; sie wurde vor dem Bestehen der CSM durchgeführt. Das Beispiel soll:

(a) die Ähnlichkeiten zwischen den bestehenden Risikobewertungsmethoden und dem CSM-Prozess aufzeigen;
(b) die Verfolgbarkeit zwischen dem bestehenden Prozess und dem von der CSM geforderten Prozess herausarbeiten;
(c) den wertschöpferischen Charakter der Durchführung der von der CSM (ggf.) geforderten zusätzlichen Schritte begründen.

Hierbei ist zu betonen, dass dieses Beispiel lediglich zu Informationszwecken gegeben wird. Es soll dem Leser das Verständnis des CSM-Prozesses erleichtern. Das Beispiel selbst jedoch darf nicht auf eine andere signifikante Änderung übertragen oder als Referenzsystem für eine andere signifikante Änderung eingesetzt werden. Für jede signifikante Änderung muss die Risikobewertung gemäß CSM-Verordnung durchgeführt werden.

C.13.2. Zur Herleitung von Standardsicherheitsanforderungen für zukünftige elektronische Stellwerksysteme hatte die Deutsche Bahn eine Risikoanalyse eines bereits zugelassenen elektronischen Systems durchgeführt. Dieses System war bereits nach deutschem Regelwerk (Mü 8004) genehmigt.

C.13.3. Die Risikoanalyse erfolgte entsprechend den CENELEC-Normen (EN 50126 und EN 50129) and umfasste die folgenden Schritte:

(a) Systemdefinition;
(b) Gefährdungsermittlung;
(c) Gefährdungsanalyse und -quantifizierung.

C.13.4. Bei der Systemdefinition wurde darauf geachtet, die Grenzen des Systems sowie seine Funktionen und Schnittstellen zu definieren. Die größte Herausforderung bestand darin, das System so zu definieren, dass es unabhängig von der internen Architektur eines Stellwerks war und dabei mit bestehenden Stellwerken kompatibel blieb. Besondere Aufmerksamkeit erlangte folglich die eindeutige Definition der Schnittstellen zwischen Stellwerk und eingreifenden äußeren Systemen unter Verzicht auf eine detaillierte Beschreibung der inneren Stellwerksfunktionen.

C.13.5. Die Gefährdungen wurden nur an den Schnittstellen bestimmt, damit der generische Grundansatz gewahrt blieb (d. h. um Abhängigkeiten von spezifischen Architekturen zu vermeiden). Berücksichtigt wurden nur Gefährdungen aus technischen Fehlern. Für jede Schnittstelle wurden somit zwei generische Gefährdungen ermittelt:

(a) Falsche Ausgabe des Stellwerks wird an Schnittstelle übermittelt
(b) (Korrekte) Eingabe wird an der Schnittstelle verfälscht

C.13.6. Für jede Schnittstelle wurden den ermittelten generischen Gefährdungen anschließend spezifische Merkmale zugeordnet.

C.13.7. In der anschließenden Phase wurde der Beitrag der bestehenden Systemkomponenten zu den einzelnen ermittelten Gefährdungen analysiert und in einem Fehlerbaum zusammengefasst. Anhand der geschätzten Ausfallraten der Komponenten konnte dann für jede Gefährdung eine Eintrittshäufigkeit berechnet werden, die für zukünftige Generationen



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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

elektronischer Stellwerke als tolerierbare Gefährdungsrate (Tolerable Hazard Rate – THR) verwendet werden können.

C.13.8. Die Risikoanalyse wurde durch die nationale Sicherheitsbehörde (EBA) nachgeprüft und bewertet.

C.13.9. Im Rahmen der Risikoanalyse wurden auch die Steuer- und Anzeigefunktionen im elektronischen System analysiert. Erneut wurde ein bestehendes, zugelassenes elektronisches Stellwerksystem als Referenzsystem herangezogen, um daraus Sicherheitsanforderungen an die Funktionen der Mensch-Maschine-Schnittstelle (MMS) zur Kontrolle zufälliger Ausfälle und Fehler ebenso wie zur Kontrolle systematischer Fehler abzuleiten. Im Ergebnis wurden die SIL-Stufen (Safety Integrity Level) für verschiedene Funktionen bestimmt: für MSS-Funktionen im Regelbetrieb, für MMS-Funktionen im Kommandofreigabeverfahren (herabgesetzte Arbeitsweise) und für Anzeigefunktionen.

C.13.10. Auch diese Risikoanalyse wurde von der nationalen Sicherheitsbehörde (EBA) nachgeprüft und bewertet.

C.13.11. Diese Risikobewertungsbeispiele illustrieren, wie der zweite Risikoakzeptanzgrundsatz (Referenzsystem) der CSM für die Herleitung von Sicherheitsanforderungen neuer Systeme verwendet werden kann. Weitere Grundlagen waren die CENELEC-Normen, so dass eine gute Übereinstimmung mit dem CSM-Prozess vorliegt. Die Risikobewertung in den Beispielen erfüllt die Anforderungen der CSM in Bezug auf die einzelnen Teilschritte (Phasen). Da hier jedoch keine Entwurfsaktivitäten durchgeführt wurden, gibt es weder einen Verweis auf die Verwaltung von Gefährdungsprotokollen noch einen Nachweis über die Einhaltung der ermittelten Sicherheitsanforderungen durch das zu bewertende System.

C.13.12. Weitere Informationen über diese Risikoanalysen finden sich in:

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

(b) Bock, H., Braband, J., und Harborth, M.: *"Safety Assessment of Vital Control and Display Functions in Electronic Interlockings, in Proc. AAET2005 Automation, Assistance and Embedded Real Time Platforms for Transportation"*, GZVB, Braunschweig, 2005, 234-253.

## C.14. Beispiel eines expliziten Risikoakzeptanzkriteriums für den Funkfahrbetrieb in Deutschland

C.14.1. **Anmerkung:** Diese beispielhafte Risikobewertung geht nicht auf die Anwendung des CSM-Prozesses zurück; sie wurde vor dem Bestehen der CSM durchgeführt. Das Beispiel soll:

(a) die Ähnlichkeiten zwischen den bestehenden Risikobewertungsmethoden und dem CSM-Prozess aufzeigen;
(b) die Verfolgbarkeit zwischen dem bestehenden Prozess und dem von der CSM geforderten Prozess herausarbeiten;
(c) den wertschöpferischen Charakter der Durchführung der von der CSM (ggf.) geforderten zusätzlichen Schritte begründen.

Hierbei ist zu betonen, dass dieses Beispiel lediglich zu Informationszwecken gegeben wird. Es soll dem Leser das Verständnis des CSM-Prozesses erleichtern. Das Beispiel selbst jedoch darf nicht auf eine andere signifikante Änderung übertragen oder als Referenzsystem



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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

für eine andere signifikante Änderung eingesetzt werden. Für jede signifikante Änderung muss die Risikobewertung gemäß CSM-Verordnung durchgeführt werden.

C.14.2. Für ein vollkommen neues Betriebsverfahren, das in Deutschland für konventionelle Bahnstrecken geplant war (aber nie eingeführt wurde), wurde eine Risikoanalyse entsprechend den CENELEC-Normen durchgeführt. Das Konzept sah einen sicheren Zugbetrieb durch ausschließliche Funksteuerung vor (Strecke und Zug). Da es keine bestehenden Regelwerke (anerkannte Regeln der Technik) und keine Referenzsysteme für so ein neues System gab, wurde eine explizite Risikoabschätzung durchgeführt, um die Sicherheit des neuen Verfahrens nachzuweisen. Es musste aufgezeigt werden, dass das Risikoniveau für einen Reisenden aufgrund des neuen Systems ein vertretbares (akzeptables) Risiko nicht übersteigen würde (explizites Risikoakzeptanzkriterium).

C.14.3. Die Abschätzung dieses expliziten Risikoakzeptanzkriteriums erfolgte anhand von Statistiken zu Unfällen in Deutschland, die auf Signalgebungs- und Steuersysteme zurückzuführen waren, und es erfolgte eine Plausibilitätsprüfung gegenüber dem MEM-Kriterium. Diese Sicherheitsnachweisführung entspricht der deutschen EBO-Anforderung, die besagt, dass bei Abweichungen von Regeln der Technik das „gleiche Sicherheitsniveau“ erreicht werden muss. Die Risikoanalyse wurde von der nationalen Sicherheitsbehörde (EBA) auch nachkontrolliert und bewertet.

C.14.4. Dieses Risikobewertungsbeispiel zeigt, wie ein globales explizites Kriterium (für den dritten Risikoakzeptanzgrundsatz in der CSM) für neue Systeme in Fällen hergeleitet werden kann, wo es weder anerkannte Regeln der Technik noch ein Referenzsystem gibt. Die anschließend durchgeführte Risikoanalyse für das neue System gründet sich auf die CENELEC-Normen und steht somit in guter Übereinstimmung mit dem CSM-Prozess. Die Risikobewertung im Beispiel erfüllt die CSM-Anforderungen, aber es wird weder auf die Verwaltung von Gefährdungsprotokollen noch auf den Nachweis der Einhaltung der ermittelten Sicherheitsanforderungen durch das zu bewertende System verwiesen.

C.14.5. Weitere Informationen zu dieser Risikoanalyse finden sich in: Braband, J., Günther, J., Lennartz, K., Reuter, D.: *„Risikoakzeptanzkriterien für den FunkFahrBetrieb (FFB)“*, Signal + Draht, Nr.5, 2001, 10-15

## C.15. Beispiel für einen Anwendbarkeitstest des RAC-TS

C.15.1. Diese Anlage soll anhand eines Funktionsbeispiels des fahrzeugseitigen ETCS-Teilsystems aufzeigen, wie das Kriterium nach Abschnitt 2.5.4 zu verwenden ist and wie bestimmt wird, ob das RAC-TS anwendbar ist.

C.15.2. Das fahrzeugseitige ETCS-Teilsystem (Onboard-System) ist ein technisches System. Betrachtet wird die folgende Funktion: *„Den Triebfahrzeugführer mit Informationen versorgen, die es ihm ermöglichen, den Zug sicher zu führen und im Falle überhöhter Geschwindigkeit eine Bremsung auszulösen“*.

Beschreibung der Funktion: Anhand von streckenseitig gelieferten Informationen (erlaubte Geschwindigkeit) und anhand der vom fahrzeugseitigen ETCS-Teilsystem berechneten Zuggeschwindigkeit:

(a) fährt der Triebfahrzeugführer den Zug und gewährleistet, dass die Zuggeschwindigkeit nicht die erlaubte Geschwindigkeit überschreitet;
(b) überwacht parallel dazu das fahrzeugseitige ETCS-Teilsystem, dass der Zug in keinem Fall die erlaubte Höchstgeschwindigkeit überschreitet. Im Falle einer Geschwindigkeitsüberschreitung werden automatisch die Bremsen angesteuert.


European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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

Triebfahrzeugführer und fahrzeugseitiges ETCS-Teilsystem verwenden beide die Beurteilung der vom fahrzeugseitigen ETCS-Teilsystem berechneten Zuggeschwindigkeit.

C.15.3. Frage: „Ist das RAC-TS auf die Beurteilung der Zuggeschwindigkeit durch das Onboard-Teilsystem anwendbar?“

C.15.4. Anwendung des Ablaufdiagramms in Abbildung 14 und Beantwortung der verschiedenen Fragen:

(a) Betrachtete Gefährdung für das technische System:

*„Überschreitung der an das ETCS mitgeteilten sicheren Geschwindigkeit“* (siehe UNISIG SUBSET 091).

(b) Lässt sich die Gefährdung durch anerkannte Regeln der Technik oder durch ein Referenzsystem kontrollieren?

NEIN. Es gilt als Annahme, dass das ETCS-System ein neues und innovatives Design ist. Deshalb gibt es keine anerkannten Regeln der Technik oder Referenzsysteme, die eine Kontrolle der Gefährdung auf akzeptablem Risikoniveau gestatten.

(c) Ist es wahrscheinlich, dass die Gefährdung zu katastrophalen Folgen führen kann?

JA, denn eine *„Überschreitung der an das ETCS mitgeteilten sicheren Geschwindigkeit“* kann eine Zugentgleisung bewirken, die potenziell zu *„Todesfällen und/oder mehreren Schwerverletzten und/oder wesentlichen Umweltschäden“* führen kann.

(d) Ist die katastrophale Folge ein unmittelbares Ergebnis des Ausfalls des technischen Systems?

JA, wenn es keine zusätzlichen Sicherheitsbarrieren gibt. Die gleiche Beurteilung der vom fahrzeugseitigen ETCS-Teilsystem berechneten Zuggeschwindigkeit wird sowohl an den Triebfahrzeugführer und an die Bremssteuerfunktion des fahrzeugseitigen ETCS-Teilsystems geliefert. Unter der Annahme, dass der Triebfahrzeugführer den Zug (aus Leistungsgründen) mit der streckenseitig erlaubten Höchstgeschwindigkeit fährt, werden somit im Falle einer Unterschätzung der Zuggeschwindigkeit weder der Triebfahrzeugführer noch das fahrzeugseitige ETCS-Teilsystem die überhöhte Geschwindigkeit des Zuges bemerken. Dies kann potenziell zu einer Zugentgleisung mit katastrophalen Folgen führen.

(e) Schlussfolgerungen:

(1) Für die quantitativen Anforderungen: Anwendung einer THR von $10^{-9}$ $h^{-1}$ für die zufälligen Hardwarefehler des fahrzeugseitigen ETCS-Teilsystems, damit gewährleistet ist:

(i) dass in der Beurteilung dieses quantitativen Ziels für redundante Systeme die gemeinsamen Komponenten berücksichtigt werden (z. B. einzelne oder gemeinsame Eingaben in alle Kanäle, gemeinsame Stromversorgung, Vergleichs- und Überwachungsglieder usw.);
(ii) dass die ruhenden bzw. latenten Fehlererkennungszeiten mit erfasst sind;
(iii) dass eine CCF/CMF-Analyse durchgeführt wird;
(iv) dass eine unabhängige Bewertung durchgeführt wird.

(2) Für die Prozessanforderungen: Anwendung eines SIL4-Prozesses zur Verwaltung systematischer Ausfälle/Fehler des fahrzeugseitigen ETCS-Teilsystems. Hierfür sind anzuwenden:

(i) ein Qualitätsmanagementprozess in Übereinstimmung mit SIL 4;
(ii) ein Sicherheitsmanagementprozess in Übereinstimmung mit SIL 4;
(iii) die einschlägigen Normen, z. B.:



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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

- für Software-Entwicklung die Norm EN 50 128;
- für Hardware-Entwicklung die Normen 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 usw.

(3) Eine unabhängige Bewertung des/der Prozesse(s).

# C.16. Beispiele möglicher Strukturen für Gefährdungsprotokolle

## C.16.1. Einleitung

C.16.1.1. Die Mindestanforderungen für Eintragungen in das Gefährdungsprotokoll sind in Abschnitt 4.1.2 der CSM-Verordnung angegeben. In den nachfolgenden Beispielen für Gefährdungsprotokolle sind diese Mindestanforderungen mit Hintergrundschattierung versehen.

C.16.1.2. Es kann verschiedene Wege zur Strukturierung eines Gefährdungsprotokolls sowie zusätzlicher Informationen zur Charakterisierung der Gefährdungen und verbundenen Sicherheitsmaßnahmen geben. Beispielsweise können die Gefährdungen und verbundenen Sicherheitsmaßnahmen mit jeweils einem Feld pro Information eingepasst werden. Unabhängig davon, welche Struktur verwendet wird, ist es jedoch wichtig, dass das Gefährdungsprotokoll eindeutige Verknüpfungen zwischen den Gefährdungen und den verbundenen Sicherheitsmaßnahmen herstellt. Eine mögliche Lösung besteht darin, dass das Gefährdungsprotokoll für jede Gefährdung und jede Sicherheitsmaßnahme mindestens ein Feld mit folgenden Angaben enthält:

(a) eine eindeutige Beschreibung, einschließlich Verweisen, zur Herkunft und zum für die Kontrolle der verbundenen Gefährdung gewählten Risikoakzeptanzgrundsatz. Dieses Feld ermöglicht das Verständnis der Gefährdung und der verbundenen Sicherheitsmaßnahmen und gibt Aufschluss darüber, in welchen Sicherheitsanalysen diese ermittelt wurden.

Da das Gefährdungsprotokoll während des gesamten Lebenszyklus des Systems (d. h. während des Systembetriebs und der Systeminstandhaltung) verwendet und geführt wird, ist eine eindeutige Nachverfolgbarkeit, oder Verknüpfung, zwischen den einzelnen Gefährdungen und:

(1) dem verbundenen Risiko;
(2) den Gefährdungsursachen, soweit bereits ermittelt;
(3) den verbundenen Sicherheitsmaßnahmen sowie den Annahmen, die die Grenzen des zu bewertenden Systems festlegen;
(4) den verbundenen Sicherheitsanalysen, in denen die Gefährdung ermittelt wird;

hilfreich.

Ferner müssen die Sicherheitsmaßnahmen (insbesondere jene, die an andere Akteure wie einen Vorschlagenden zu übermitteln sind) sowie die verbundenen Gefährdungen und Risiken im Wortlaut eindeutig und hinreichend formuliert sein. „Eindeutig und hinreichend“ bedeutet, dass die Sicherheitsmaßnahmen und verbundenen Gefährdungen in Bezug auf die zu kontrollierenden Risiken verstanden werden können, ohne dass auf die entsprechenden Sicherheitsanalysen zurückgegriffen werden muss.

(b) der für die Kontrolle der Gefährdung verwendete Risikoakzeptanzgrundsatz zur Unterstützung der gegenseitigen Anerkennung und zur Unterstützung der Bewertungsstelle bei der Bewertung der ordnungsgemäßen Anwendung der CSM;



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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) eine eindeutige Information über den Status: Dieses Feld zeigt an, ob die entsprechende Gefährdung/Sicherheitsmaßnahme noch offen oder bereits kontrolliert/validiert ist.

(1) Eine offene Gefährdung/Sicherheitsmaßnahme wird bis zu ihrer Kontrolle/Validierung nachverfolgt.

(2) Die kontrollierten/validierten Gefährdungen/Sicherheitsmaßnahmen werden jedoch nur so lange nicht mehr nachverfolgt, bis signifikante Änderungen im Betrieb oder bei der Instandhaltung des Systems eintreten: siehe Punkt [G 6](b) in Abschnitt 2.1.1. Wenn dies geschieht:

(i) wird die CSM auf die erforderlichen Änderungen gemäß Artikel 2 noch einmal angewendet. Siehe auch Punkt [G 6](b)(1) in Abschnitt 2.2.1;

(ii) werden alle kontrollierten Gefährdungen und Sicherheitsmaßnahmen neu betrachtet, um zu prüfen, dass sie von den Änderungen nicht berührt werden. Sollten sie doch berührt werden, werden die diesbezüglichen Gefährdungen und verbundenen Sicherheitsmaßnahmen wieder geöffnet und erneut im Gefährdungsprotokoll geführt.

Es könnte passieren, dass andere Sicherheitsmaßnahmen als die eigentlich im Gefährdungsprotokoll verzeichneten implementiert werden (z. B. aus Kostengründen). Dann folgt die Eintragung der implementierten Sicherheitsmaßnahmen in das Gefährdungsprotokoll gemeinsam mit dem Nachweis / der Begründung ihrer Eignung und mit dem Nachweis, dass das System mit diesen Maßnahmen den Sicherheitsanforderungen genügt.

(d) Verweis auf den verbundenen Nachweis zur Kontrolle einer Gefährdung oder Validierung einer Sicherheitsmaßnahme. Dieses Feld ermöglicht ein späteres Auffinden des Nachweises, der die Kontrolle der Gefährdung und die Validierung der verbundenen Sicherheitsmaßnahme(n) gestattet hat.

Eine Gefährdung kann im Gefährdungsprotokoll nur kontrolliert werden, wenn alle mit der Gefährdung verbundenen und verknüpften Sicherheitsmaßnahmen im Vorfeld validiert werden.

(e) die für die Verwaltung verantwortliche(n) Organisation(en) oder Stelle(n).

C.16.1.3. Ein weiteres Beispiel für den möglichen Inhalt eines Gefährdungsprotokolls findet sich in Anhang A.3. des Leitfadens EN 50126-2 {Ref. 9}.



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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. Beispiel eines Gefährdungsprotokolls für die organisatorische Änderung in Abschnitt C.5 in Anlge C

***Tabelle 6: Beispiel eines Gefährdungsprotokolls für die organisatorische Änderung in Abschnitt C.5 in Anlage C.***

| **Beschreibung der Gefährdung** | **Sicherheitsmaßnahmen** | **Priorität/ Sicherheit Pünktlichkeit** | **Implementierung[16]** | **Anmerkungen** | **Verantwortl.[18]** | **Herkunft** | **Verwendeter Risikoakzeptanzgrundsatz** | **Verantwortl. für Verifizierung** | **Art der Verifizierung** | **Status xx.xx.xx** |
|---|---|---|---|---|---|---|---|---|---|---|
| Verminderte Motivation bei den Beschäftigten des Unternehmens. Dadurch ständig Personalabgänge.<br><br>Demotiviertes/ ausgebranntes Führungspersonal | Durchführung einer neuen Runde von Motivierungsmaßnahmen für das Personal, jeweils in kleineren Gruppen;<br>Ressourcenzuweisung entsprechend bedeutsamer Aufgaben.<br>Häufigere Inspektionen durch Anlagenmanager.<br>Bereitstellung von Mitteln, damit Kernpersonal über den gesamten Prozess im Unternehmen bleibt.<br>Besondere Aufmerksamkeit und Sorgfalt, dass Informationen und Kenntnisse von ausscheidendem Personal an die Mitarbeiter vermittelt werden, die die Aufgaben übernehmen<br>usw. | Hoch/hoch | Koordiniert von XYZ. Regionen müssen Maßnahmen prüfen zur besseren Kontrolle der Gleisanlagen, Aufgabenüberlappung bei Mitarbeitern und Nachprüfungen durch Streckenleiter | Die Verträge müssen mehr Inspektionen einbeziehen.<br>usw. | Unternehmensführung | Brainstorming HAZID Bericht $R_X$ | N/A | | | Änderungen der Bedingungen und Begleitumstände haben dieses Risiko erheblich vermindert. Arbeitsumweltanalyse und Personalschulung wurden durchgeführt. |
| Subunternehmern der Auftragnehmer fehlt es an Fertigkeiten, Kompetenz und Qualitätskontrolle | Erhöhter Bedarf an dokumentierter Kompetenz.<br>Systematische Kontrolle erledigter Aufgaben. | Hoch/mittel | FB muss koordinieren. Regionen müssen Maßnahmen für Kompetenzforderung und Leistungsüberwachung implementieren. | Umgesetzt durch Vertragsüberwachung. Eingabegröße für Änderungsplanung. | Fahrwegbetreiber | Brainstorming HAZID Bericht $R_X$ | N/A | Sicherheitsmanager | | Erhöhte Konzentration auf Kontrollroutinen (2 operative Kontrollen pro Monat je Betriebsbereich) |
| Unsicherheiten bezüglich der | Festlegung der Rollen und Verantwortlichkeiten.<br>Kartierung aller Schnittstellen und Festlegung, | Mittel/mittel | Separat je Region | Implementiert durch Instand- | Regionalleiter | Brainstorming | N/A | Sicherheitsmanager | | Regionen haben ihre |

*(16) Diese beiden Spalten beziehen sich auf die Angaben/Felder zu den Kontrollverantwortlichen für die ermittelten Gefährdungen.*



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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

***Tabelle 6: Beispiel eines Gefährdungsprotokolls für die organisatorische Änderung in Abschnitt C.5 in Anlage C.***

| Beschreibung der Gefährdung | Sicherheitsmaßnahmen | Priorität/ Sicherheit Pünktlichkeit | Implementierung[16] | Anmerkungen | Verantwortl.[18] | Herkunft | Verwendeter Risikoakzeptanzgrundsatz | Verantwortl. für Verifizierung | Art der Verifizierung | Status xx.xx.xx |
|---|---|---|---|---|---|---|---|---|---|---|
| Rollen und Verantwortlichkeiten an der Schnittstelle zwischen dem Unternehmen und dem FB (Fahrwegbetreiber). | wer für welche Schnittstellen verantwortlich ist. | | | haltungsvertrag und Strategieplanung für Neuorganisation | | HAZID Bericht $R_X$ | | | | Strategie vorgestellt. |

## C.16.3. Beispiel eines kompletten Gefährdungsprotokolls für ein fahrzeugseitiges Teilsystem der Zugsteuerung/Zugsicherung

C.16.3.1. Dieser Abschnitt zeigt in einem Beispiel ein Einzelgefährdungsprotokoll (siehe Punkt [G 3] in Abschnitt 4.1.1) für:

(a) Verwaltung aller geltenden internen Sicherheitsanforderungen für das Teilsystem, für das der Akteur verantwortlich ist; und
(b) Verwaltung aller ermittelten Gefährdungen und verbundenen Sicherheitsmaßnahmen, die der Akteur nicht implementieren kann und die an einen anderen Akteur übertragen werden müssen.

***Tabelle 7: Beispiel eines Gefährdungsprotokolls eines Herstellers für ein fahrzeugseitiges Teilsystem der Zugsteuerung/Zugsicherung***

| Gef.-Nr. | Herkunft | Beschreibung der Gefährdung | Zusätzliche Informationen | Verantwortl. Akteur | Sicherheitsmaßnahme | Verwendeter Risikoakzeptanzgrundsatz | Exportiert | Status |
|---|---|---|---|---|---|---|---|---|
| 1 | HAZOP Bericht $R_X$ | Höchstgeschwindigkeit des Zuges zu hoch eingestellt (Vmax) | Falsche spezifische Konfiguration des fahrzeugseitigen Teilsystems (Instandhaltungspersonal). Falsche Dateneingabe im Zug (Triebfahrzeugführer) | Eisenbahnunternehmen | • Festlegung eines Verfahrens zur Genehmigung der Konfigurationsdaten des fahrzeugseitigen Teilsystems;<br>• Festlegung eines Betriebsverfahrens für den Prozess der Dateneingabe durch den Triebfahrzeugführer; | Explizite Risikoabschätzung | Ja | Kontrolliert (exportiert an EBU) Siehe auch Abschnitt Abschnitt C.16.4.2 in Anlage C |
| 2 | HAZOP | Bremskurven (d. h. Fahr- | Das Verfahren zur spezifischen Konfiguration des | Eisenbahn- | • Korrekte Angabe der | Explizite | Ja | Kontrolliert |



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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

***Tabelle 7: Beispiel eines Gefährdungsprotokolls eines Herstellers für ein fahrzeugseitiges Teilsystem der Zugsteuerung/Zugsicherung***

| Gef.-Nr. | Herkunft | Beschreibung der Gefährdung | Zusätzliche Informationen | Verantwortl. Akteur | Sicherheitsmaßnahme | Verwendeter Risikoakzeptanzgrundsatz | Exportiert | Status |
|---|---|---|---|---|---|---|---|---|
| | Bericht $R_X$ | erlaubnis) in Konfigurationsdaten des fahrzeugseitigen Teilsystems zu großzügig | fahrzeugseitigen Teilsystems hängt ab von:<br>• den Sicherheitsgrenzen für das Zugbremssystem;<br>• der Reaktionsverzögerung des Zugbremssystems (hier unmittelbar abhängig von der Zuglänge, besonders bei Güterzügen) | unternehmen | Systemanforderungen in der Systemdefinition;<br>• Ausreichender Toleranzspielraum für Sicherheitsgrenzen des Bremssystems des spezifischen Zuges | Risikoabschätzung | | (exportiert an EBU) Siehe auch Abschnitt C.16.4.2 in Anlage C |
| 3 | HAZOP Bericht $R_X$ | • Höchstgeschwindigkeit des Zuges zu hoch eingestellt (Vmax)<br>• Bremskurven (d. h. Fahrerlaubnis) in Konfigurationsdaten des fahrzeugseitigen Teilsystems zu großzügig | Raddurchmesser des Zuges in der spezifischen Konfiguration des fahrzeugseitigen Teilsystems nicht aktualisiert (Instandhaltungspersonal). | Eisenbahnunternehmen | • Festlegung eines Verfahrens zur Messung des Raddurchmessers des Zuges durch das Instandhaltungspersonal;<br>• Festlegung eines Verfahrens zur regelmäßigen Aktualisierung des Raddurchmessers im fahrzeugseitigen Teilsystem; | Explizite Risikoabschätzung | Ja | Kontrolliert (exportiert an EBU) Siehe auch Abschnitt C.16.4.2 in Anlage C |
| | | | Fehler im Herstellerverfahren zur Vorbereitung und Einlesung der Konfigurationsdaten in das fahrzeugseitige Teilsystem | Hersteller | Festlegung eines Verfahrens zur Aktualisierung des Raddurchmessers in den fahrzeugseitigen Konfigurationsdaten | Explizite Risikoabschätzung | Ja | Kontrolliert durch Verfahren $P_X$ |
| 4 | HAZOP Bericht $R_X$ | Einfahrt des Zuges mit hoher Geschwindigkeit (160 km/h wenn streckenseitiges Signal frei ist) in das Gleis ohne aktives fahrzeugseitiges Teilsystem und ohne Streckensignalgebung | Kann nur durch Wachsamkeit des Triebfahrzeugführers kontrolliert werden.<br>Die Einfahrt in einen mit ATP ausgerüsteten Gleisbereich verlangt eine Quittierung durch den Triebfahrzeugführer vor dem Übergangsort. Falls keine Quittierung erfolgt, werden die Zugbremsen durch das Teilsystem der Zugsteuerung/ Zugsicherung automatisch ausgelöst. | Fahrwegbetreiber | Durch den Fahrwegbetreiber ist sicherzustellen, dass Züge, die nicht mit einem aktiven Teilsystem der Zugsteuerung/ Zugsicherung ausgerüstet sind, das entsprechende Gleis nicht befahren.<br><br>Festlegung eines Verfahrens für die Verkehrsführung. | Explizite Risikoabschätzung | Ja | Kontrolliert (exportiert an FB) Siehe auch Abschnitt C.16.4.2 in Anlage C |
| | | | | Eisenbahnunternehmen | Gewährleistung der Schulung des Triebfahrzeugführers in Bezug auf Einfahrt in einen mit ATP ausgestatteten Gleisbereich | Explizite Risikoabschätzung | Ja | Kontrolliert (exportiert an EBU) Siehe auch Abschnitt C.16.4.2 in Anlage C |
| 5 | HAZOP Bericht $R_X$ | Eingestellte Höchstgeschwindigkeit des Zuges wird dem Triebfahrzeugführer als | Die an der Schnittstelle mit dem Triebfahrzeugführer angezeigten Informationen werden durch das fahrzeugseitige Zugsteuerungs-/Zugsicherungs-Teilsystem der Stufe SIL 4 überwacht, das im Falle | Hersteller | Entwicklung eines fahrzeugseitigen Teilsystems der Zugsteuerung/ Zugsicherung mit SIL 4 | Explizite Risikoabschätzung | Ja | Sicherheitsnachweis über SIL4-Teilsystem bewertet durch einen Unabhängigen |



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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

***Tabelle 7: Beispiel eines Gefährdungsprotokolls eines Herstellers für ein fahrzeugseitiges Teilsystem der Zugsteuerung/Zugsicherung***

| Gef.-Nr. | Her-kunft | Beschreibung der Gefährdung | Zusätzliche Informationen | Verantwortl. Akteur | Sicherheitsmaßnahme | Verwendeter Risikoakzep-tanzgrundsatz | Exportiert | Status |
|---|---|---|---|---|---|---|---|---|
| | | zu hoch angezeigt (Vmax) | auftretender Diskrepanzen zwischen Anzeige und Sollwert die Notbremsung einleitet. Bei Nichtübereinstimmung mit der Fahrerlaubnis (MA) betätigt das fahrzeugseitige Teilsystem der Zugsteuerung/Zugsicherung die Notbremsen. | | | | | Sicherheits-begutachter |
| 6 | HAZOP Bericht $R_X$ | Zug fährt ohne Triebfahrzeugführer-Maschine-Schnittstelle ab | Verlust an redundanter Architektur des fahrzeugseitigen Teilsystems | Hersteller | Entwicklung eines fahrzeugseitigen Teilsystems der Zugsteuerung/ Zugsicherung mit SIL 4 | Explizite Risiko-abschätzung | Ja | Sicherheitsnachweis über SIL4-Teilsystem bewertet durch einen Unabhängigen Sicherheits-begutachter |
| usw. | | | | | | | | |

## C.16.4. Beispiel eines Gefährdungsprotokolls für Informationsübermittlungen an andere Akteure

C.16.4.1 Dieser Abschnitt gibt das Beispiel für ein Gefährdungsprotokoll zur Übertragung der ermittelten Gefährdungen und verbundenen Sicherheitsmaßnahmen, die ein betreffender Akteur nicht implementieren kann, an andere Akteure. Siehe Punkt [G 1] in Abschnitt 4.1.1.
Dieses Beispiel ist identisch mit dem Beispiel aus Abschnitt C.16.3 in Anlage C. Der einzige Unterschied besteht darin, dass alle internen Gefährdungen und Sicherheitsmaßnahmen, die der betrachtete Akteur selbst kontrollieren kann, ausgelassen sind.

C.16.4.2. Die letzte Spalte in Tabelle 8 dient zur Einhaltung der Anforderung aus Abschnitt 4.2 der CSM-Verordnung. Es gibt verschiedene Lösungen, um dies zu erreichen. Eine Möglichkeit wäre ein Verweis auf den Nachweis, den der Akteur verwendet hat, der die exportierten Sicherheitsinformationen erhalten hat. Eine andere Möglichkeit könnte eine Besprechung der beiden Akteure sein, um gemeinsam die geeignetste Lösung für die Kontrolle des/der verbundenen Risikos/Risiken zu finden. Die Ergebnisse einer solchen Besprechung könnten in einem vereinbarten Dokument festgehalten werden (beispielsweise in einem Besprechungsprotokoll), auf das der Akteur, der die sicherheitsbezogenen Informationen exportiert, in seinem Gefährdungsprotokoll verweisen kann, um so die verbundenen Gefährdungen abzuschließen.



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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

***Tabelle 8: Beispiel eines Gefährdungsprotokolls für die Übermittlung sicherheitsbezogener Informationen an andere Akteure.***

| Gef-Nr. | Herkunft der Gef. | | Beschreibung der Gefährdung | Zusätzliche Informationen | Verantwortl. Akteur | Sicherheitsmaßnahme | Anmerkung des Empfängers |
|---|---|---|---|---|---|---|---|
| | Nr. in Tabelle 7 | Sonstig | | | | | |
| 1 | N°1 | HAZOP Bericht $R_X$ | Höchstgeschwindigkeit des Zuges zu hoch eingestellt (Vmax) | Falsche spezifische Konfiguration des fahrzeugseitigen Teilsystems (Instandhaltungspersonal). Falsche Dateneingabe im Zug (Triebfahrzeugführer) | Eisenbahnunternehmen | • Festlegung eines Verfahrens zur Genehmigung der Konfigurationsdaten des fahrzeugseitigen Teilsystems;<br>• Festlegung eines Betriebsverfahrens für den Prozess der Dateneingabe durch den Triebfahrzeugführer; | • Die Konfigurationsdaten des fahrzeugseitigen Teilsystems der Zugsteuerung / Zugsicherung hängen von physischen Eigenschaften der Fahrzeuge ab.<br>• Anhand dieser Daten stimmen Fahrwegbetreiber und Eisenbahnunternehmen dann entsprechende Sicherheitsgrenzbereiche ab.<br>• Diese Daten werden anschließend im Zuge der Montage/Installation, Fahrzeugeinbindung und Abnahme des Teilsystems der Zugsteuerung/ Zugsicherung entsprechend dem zutreffenden Verfahren des Herstellers in das fahrzeugseitige Teilsystem eingelesen.<br>• Die Triebfahrzeugführer werden nach dem Verfahren $D_P$ geschult und beurteilt (evaluiert).<br>• Die Triebfahrzeugführer werden ferner durch den FB nach den für die Infrastruktur des FB geltenden Vorschriften evaluiert. |
| 2 | N°2 | HAZOP Bericht $R_X$ | Bremskurven (d. h. Fahrerlaubnis) in Konfigurationsdaten des fahrzeugseitigen Teilsystems zu großzügig | Das Verfahren zur spezifischen Konfiguration des fahrzeugseitigen Teilsystems hängt ab von:<br>• den Sicherheitsgrenzen für das Zugbremssystem;<br>• der Reaktionsverzögerung des Zugbremssystems (hier unmittelbar abhängig von der Zuglänge, besonders bei Güterzügen) | Eisenbahnunternehmen | • Korrekte Angabe der Systemanforderungen in der Systemdefinition;<br>• Ausreichender Toleranzspielraum für Sicherheitsgrenzen des Bremssystems des spezifischen Zuges | Siehe Anmerkung in Zeile 1 oben. |
| 3 | N°3 | HAZOP Bericht $R_X$ | • Höchstgeschwindigkeit des Zugs zu hoch eingestellt (Vmax)<br>• Bremskurven (d. h. Fahrerlaubnis) in Konfigurationsdaten des fahrzeugseitigen Teilsystems zu großzügig | Raddurchmesser des Zuges in der spezifischen Konfiguration des fahrzeugseitigen Teilsystems nicht aktualisiert (Instandhaltungspersonal). | Eisenbahnunternehmen | • Festlegung eines Verfahrens zur Messung des Raddurchmessers des Zuges durch das Instandhaltungspersonal;<br>• Festlegung eines Verfahrens zur regelmäßigen Aktualisierung des Raddurchmessers im fahrzeugseitigen Teilsystem | • Die Wartung und Instandhaltung des fahrzeugseitigen Teilsystems der Zugsteuerung/Zugsicherung erfolgt nach dem „Instandhaltungsverfahren $MP_Z$“.<br>• Der Raddurchmesser des Zuges wird in festgelegten Zeitabständen nach dem Verfahren $P_W$ aktualisiert.<br>• Für den Dateneingabeprozess werden die Triebfahrzeugführer nach der „Vorschrift $P_{DE}$“ geschult und evaluiert. |
| 4 | N°4 | HAZOP Bericht $R_X$ | Einfahrt des Zuges mit hoher Geschwindigkeit (160 km/h | Kann nur durch Wachsamkeit des Triebfahrzeugführers kontrolliert werden. | Fahrwegbetreiber | Durch den Fahrwegbetreiber ist sicherzustellen, dass Züge, die nicht mit einem aktiven | Die Verkehrsführung auf der Infrastruktur des FB richtet sich nach dem Vorschriftenwerk $R_{TM}$ |



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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

***Tabelle 8: Beispiel eines Gefährdungsprotokolls für die Übermittlung sicherheitsbezogener Informationen an andere Akteure.***

| Gef-Nr. | Herkunft der Gef. | | Beschreibung der Gefährdung | Zusätzliche Informationen | Verantwortl. Akteur | Sicherheitsmaßnahme | Anmerkung des Empfängers |
|---|---|---|---|---|---|---|---|
| | Nr. in Tabelle 7 | Sonstig | | | | | |
| | | | wenn streckenseitiges Signal frei ist) in das Gleis ohne aktives fahrzeugseitiges Teilsystem und ohne Streckensignalgebung | Die Einfahrt in einen mit ATP ausgerüsteten Gleisbereich verlangt eine Quittierung durch den Triebfahrzeugführer vor dem Übergangsort. Falls keine Quittierung erfolgt, werden die Zugbremsen durch das Teilsystem der Zugsteuerung/ Zugsicherung automatisch ausgelöst. | | Teilsystem der Zugsteuerung/ Zugsicherung ausgerüstet sind, das entsprechende Gleis nicht befahren.<br><br>Festlegung eines Verfahrens für die Verkehrsführung. | |
| | | | | | Eisenbahnunternehmen | Gewährleistung der Schulung des Triebfahrzeugführers in Bezug auf Einfahrt in einen mit ATP ausgestatteten Gleisbereich | • Die Triebfahrzeugführer werden in regelmäßigen Abständen nach dem FB-Verfahren $P_{IM\_DP}$ geschult.<br>• Die Triebfahrzeugführer werden durch den FB auch nach den Vorschriften ($S_R$) evaluiert, die auf der Infrastruktur des FB gelten. |
| usw. | | | | | | | |



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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. Beispiel einer generischen Gefährdungsliste für den Bahnbetrieb

C.17.1. Die Sicherheitsanalyse zur Bahnoptimierung ROSA (Rail Optimisation Safety Analysis) ist ein Projekt im Rahmen der DEUFRAKO (deutsch-französische Kooperation) zur Erstellung einer generischen und umfassenden Gefährdungsliste für den Standardbahnbetrieb. Ziel und Herausforderung war es, diese Gefährdungen mit höchstmöglichem Detailgrad zu definieren, ohne dabei jedoch die Spezifika der französischen und deutschen Bahn zu erfassen. Die Liste wurde unter Zuhilfenahme von derzeit bestehenden Gefährdungslisten aus beiden Ländern (SNCF und DB) erstellt und auch gegen Gefährdungslisten anderer Länder geprüft. Trotz des erklärten Zieles einer umfassenden und generischen Aufstellung wird die Liste hier nur zur Information und als Hilfe für Akteure gegeben, die Gefährdungen für ein bestimmtes Projekt ermitteln müssen. Es ist davon auszugehen, dass die in der Liste angegebenen Gefährdungen für spezifische Merkmale eines Projekts verfeinert oder ergänzt werden müssen.

C.17.2. Die Gefährdungen in der untenstehenden Entwurfsliste werden "Starting Point Hazards" (SPH) genannt, also Gefährdungen, die als Ausgangspunkt für eine Folgenanalyse und eine Ursachenanalyse zur Bestimmung von Sicherheitsmaßnahmen/Sicherheitsbarrieren und Sicherheitsanforderungen zur Kontrolle der Gefährdungen dienen können.

C.17.3. ROSA-Projekt: Gefährdungsliste

| | |
|---|---|
| SPH 01 | Falsche Eingangsbestimmung der Höchstgeschwindigkeit (fahrwegbezogen) |
| SPH 02 | Falsche Bestimmung der Höchstgeschwindigkeit (zugbezogen) |
| SPH 03 | Falsche Bremsstrecke bestimmt / falsches Geschwindigkeitsprofil / falsche Bremskurven |
| SPH 04 | Unzureichende Abbremsung (physische Gründe) |
| SPH 05 | Falscher/ungeeigneter Geschwindigkeits-/Bremsbefehl |
| SPH 06 | Falsche Geschwindigkeit registriert (falsche Zuggeschwindigkeit) |
| SPH 07 | Kommunikationsfehler bei Übermittlung der Höchstgeschwindigkeit |
| SPH 08 | Zug entrollt |
| SPH 09 | Falsche Fahrtrichtung / absichtliche Rückwärtsfahrt - (Kombination von SPH 08 und SPH 14) |
| SPH 10 | Falsche absolute/ relative Position registriert |
| SPH 11 | Fehler bei Zugerkennung |
| SPH 12 | Verlust der Zugintegrität |
| SPH 13 | Eventuell falsche Route für Zug |
| SPH 14 | Fehler bei Übermittlung/Kommunikation von Fahrplan/MA (Fahrerlaubnis) |
| SPH 15 | Strukturfehler im Fahrweg |
| SPH 16 | Gebrochene Weichenkomponente |
| SPH 17 | Falscher Weichenstellbefehl |
| SPH 18 | Falsche Weichenstellung |
| SPH 19 | Systemobjekt im Fahrweg/im LRP (Lichtraumprofil) (außer Schotter) |
| SPH 20 | Fremdobjekt im Fahrweg/im LRP |
| SPH 21 | Straßenverkehrsteilnehmer auf BÜ (Bahnübergang) |
| SPH 22 | Sogwirkungen auf Schotterbett |
| SPH 23 | Aerodynamische Krafteinwirkung auf Zug |
| SPH 24 | Zugausrüstung/Zugelement/Zugladung verletzt LRP des Zuges |
| SPH 25 | Unzureichendes LRP für Zug (fahrwegseitig) |
| SPH 26 | Falsche Verteilung der Ladung |
| SPH 27 | Radbruch/Achsbruch |
| SPH 28 | Heißläufer Achse/Rad/Lager |
| SPH 29 | Versagen von Drehgestell / Aufhängung / Stoßdämpfung |
| SPH 30 | Versagen von Fahrzeugrahmen/Wagenkasten |


European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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 31 | Unerlaubtes Betreten (Sicherheitsaspekt) |
| SPH 32 | Befugte Person überquert das Gleis |
| SPH 33 | Personal bei Arbeiten auf dem Gleis |
| SPH 34 | Unbefugte Person auf Gleis (Fahrlässigkeit) |
| SPH 35 | Person stürzt von Bahnsteigkante auf das Gleis |
| SPH 36 | Sogwirkung / Person zu nah an Bahnsteigkante |
| SPH 37 | Personal bei gleisnahen Arbeiten z. B. Nachbargleis |
| SPH 38 | Person verlässt Zug absichtlich (außer Ein-/Ausstieg) |
| SPH 39 | Person stürzt aus (seitlicher) Tür |
| SPH 40 | Person stürzt aus Tür am Wagenende |
| SPH 41 | Zug fährt ab / rollt mit offenen Türen (LRP nicht verletzt) |
| SPH 42 | Person stürzt in den Übergangsbereich zwischen zwei Wagen |
| SPH 43 | Passagier lehnt sich aus Tür |
| SPH 44 | Passagier lehnt sich aus Fenster |
| SPH 45 | Personal/Zugbegleiter lehnt sich aus Tür |
| SPH 46 | Personal/Zugbegleiter lehnt sich aus Fenster |
| SPH 47 | Rangierpersonal auf Fahrzeug lehnt sich vom Trittbrett |
| SPH 48 | Person stürzt/klettert von Bahnsteig zwischen Fahrzeug und Bahnsteigkante |
| SPH 49 | Person stürzt aus dem Zug / verlässt Zug außerhalb des Bahnsteigbereichs |
| SPH 50 | Person stürzt im Türbereich bei Ein-/Ausstieg |
| SPH 51 | Person im Türbereich bei schließenden Zugtüren |
| SPH 52 | Zug bewegt sich während Passagierwechsel |
| SPH 53 | Möglichkeit einer verletzten Person im Zug |
| SPH 54 | Brandgefahr/Explosionsgefahr (im/am Zug) – Unfallkategorie, Folge von SPH 55, SPH 56) |
| SPH 55 | Ungeeignete Temperatur (im Zug) |
| SPH 56 | Vergiftung / Erstickung (im/am Zug) |
| SPH 57 | Tödlicher elektrischer Schlag (im/am Zug) |
| SPH 58 | Person stürzt auf Bahnsteig (außer Passagierwechsel) |
| SPH 59 | Ungeeignete Temperatur (auf Bahnsteig) |
| SPH 60 | Vergiftung / Erstickung (auf Bahnsteig) |
| SPH 61 | Tödlicher elektrischer Schlag (auf Bahnsteig) |



European Railway Agency ● Rue Marc LEFRANCQ, 120 ● 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