Neue Generation Signaltechnik

Sektorweite Initiative zur Sicherung der Zukunftsfähigkeit der Leit- und Sicherungstechnik

Teilbericht

AP 2100 – Ergebnisbericht zur „Risikoakzeptanz auf Basis von ähnlichen Referenzsystemen" bei Anwendung der CSM-VO

16.07.2013

Gefördert durch:

Bundesministerium
für Wirtschaft
und Technologie

aufgrund eines Beschlusses
des Deutschen Bundestages

Laufzeit: 01.09.2011 – 31.08.2013

Projektträger: TÜV Rheinland Consulting GmbH

Änderungsverfolgung

Datum	Bearbeiter	Version	Inhalt
19.05.2013	Notter (THALES)	V01	Erstellung (auf Thales-Vorlage)
16.07.2013	Notter/Feucht (THALES)	V02	Einarbeitung von Anmerkungen aus AG2
09.08.2013	Notter (THALES)	V03	Einarbeitung von Anmerkungen vom AG2-Abschlusstreffen 5./6.8.2013

Inhaltsverzeichnis

1 Einleitung

Der vorliegende Ergebnisbericht befasst sich mit der Anwendung der Vorgaben zur Risikoakzeptanzermittlung mittels Referenzsystem.

Die CSM-VO beinhaltet als mittlere Säule der Risikoakzeptanzgrundsätze die Ermittlung von Risikoakzeptanzgrundsätzen aus den Sicherheitseigenschaften eines bereits zugelassenen Referenzsystems. Das ermöglicht die Ableitung von Sicherheitsanforderungen für „ähnliche Systeme" aus den Eigenschaften des Referenzsystems durch Sicherheitsanalyse oder aus der vorhandenen Dokumentation.

Als Sicherheitsanforderungen definiert sie die (qualitativen oder quantitativen) Sicherheitsmerkmale eines Systems inklusive des Betriebs und der Instandhaltung.

Begrifflich unterscheidet sie davon die systeminternen Sicherheitsanforderungen, indem sie für diese den Begriff der „umzusetzenden Sicherheitsmaßnahmen" einführt. Mit Sicherheitsanforderungen sind also übergeordnete Sicherheitsziele gemeint, wie sie z.B. die EN 50129 mit dem Konzept der tolerierbaren Gefährdungsraten einführt.

Die Risikoakzeptanzermittlung mittels Referenzsystem ist vergleichbar mit dem Grundsatz GAMAB nach EN 50126 bzw. dem im deutschen Sprachraum geläufigen Grundsatz „mindestens gleiche Sicherheit" (sinngemäß entsprechend EBO, Allgemeine Anforderungen). Die CSM-VO erweitert den Spielraum für die Anwendung von Referenzsystemen und stellt die Grundregeln dafür auf.

Für Referenzsysteme als Grundsatz der Risikoakzeptanz werden hauptsächlich zwei Anwendungsfälle gesehen:

- Ähnliche Referenzsysteme als Basis zur Ermittlung von Sicherheitsanforderungen als Risikoakzeptanzgrundsätze für die Erstellung neuer Systeme
- Cross Acceptance von Systemen auf Basis der Erfahrung mit der Anwendung des selben Systems in einem anderen Kontext

Diese beiden Anwendungsfälle werden im Folgenden näher diskutiert.

Bemerkung: Die Risikoakzeptanzermittlung mittels Referenzsystem ist relevant für signifikante Änderungen, kann aber auch bei nicht-signifikanten Änderungen im Rahmen des eigenen Sicherheitsverfahrens angewendet werden.

2 CSM-VO Inhalte zum Thema „Referenzsysteme"

Die nachfolgenden Punkte stellen die für das Thema „Referenzsystem" relevanten Abschnitte aus der CSM-VO Nr. 402/2013 dar. An Stellen, wo die CSM-VO Nr. 402/2013 von der Vorgängerversion CSM-VO Nr. 352/2009 abweicht, ist der ursprüngliche Text der CSM-VO Nr. 352/2009 mit aufgenommen und durchgestrichen dargestellt während der neue Text der CSM-VO 402/2013 kursiv gekennzeichnet ist.

Begriffsbestimmungen

9. „Sicherheitsanforderungen": die (qualitativen oder quantitativen) Sicherheitsmerkmale eines Systems sowie dessen Betriebs (einschließlich Betriebsvorschriften) *und dessen Instandhaltung*, 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;

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;

25. „System": jeden Teil des Eisenbahnsystems, der Gegenstand einer Änderung ist*, wobei die Änderung technischer, betrieblicher oder organisatorischer Art sein kann*;

Anhang I, 2.1:

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 von Regelwerken (Nummer 2.3);

b) Vergleich mit ähnlichen Systemen (Nummer 2.4);

c) explizite Risikoabschätzung (Nummer 2.5).

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

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.

Anhang I, 2.2.6 : Wird zur Risiko*beherrschung*~~kontrolle~~ auf ein Regelwerk oder auf ein Referenzsystem zurückgegriffen, kann die Gefährdungsermittlung beschränkt werden auf

a) die Überprüfung der Relevanz ~~der anerkannten Regeln der Technik~~ *des Regelwerks* bzw. ~~des~~ Referenzsystems;

b) die Ermittlung der Abweichungen ~~von den anerkannten Regeln der Technik~~ vom Regelwerk bzw. ~~vom~~ Referenzsystem.

Anhang I, 2.4: Heranziehung eines Referenzsystems und Risikoevaluierung

2.4.1. Der Vorschlagende untersucht mit Unterstützung anderer beteiligter Akteure, ob eine ~~oder~~, mehrere *oder alle* Gefährdung(en) durch ein ähnliches System *angemessen* abgedeckt *wird bzw*. werden, das als Referenzsystem herangezogen werden könnte.

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 daher 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.

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.

2.4.4. Weicht das zu bewertende System vom Referenzsystem ab, muss aus der Risikoevaluierung hervorgehen, dass ~~das bewertete~~ *dieses* System mindestens das gleiche Sicherheitsniveau erreicht wie das Referenzsystem, *indem ein anderes Referenzsystem herangezogen oder einer der beiden anderen Risikoakzeptanzgrundsätze angewandt wird*. Die Risiken, die mit den vom Referenzsystem abgedeckten Gefährdungen verbunden sind, werden in diesem Fall als vertretbar angesehen.

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

2.5.1. Wenn die Gefährdungen nicht von einem der beiden Risikoakzeptanzgrundsätze abgedeckt werden, die in den Nummern 2.3 und 2.4 festgelegt 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.

2.5.4. Wenn sich aus Ausfällen technischer Systeme Gefährdungen ergeben, die nicht von den ~~anerkannten Regeln der Technik~~ *Regelwerken* oder der Verwendung eines Referenzsystems abgedeckt werden, gilt für *den Entwurf* ~~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 *reduziert* ~~eingedämmt~~ werden, wenn die Ausfallrate pro Betriebsstunde kleiner oder gleich 10^{-9} ist.

3 Literatur-Überblick

3.1 ERA Leitlinie

Enthält Erläuterungen zu den einzelnen Bestimmungen, aber keine wesentlich weiterführenden Informationen zum Thema „Referenzsysteme".

3.2 ERA Beispiele

Enthält einzelne Erläuterungen zu den einzelnen Bestimmungen, aber keine wesentlich weiterführenden Informationen zum Thema „Referenzsysteme".

Als Beispiel für die Verwendung eines Referenzsystems zur Ableitung von Sicherheitsanforderungen ist die Risikoanalyse für neue elektronische Stellwerksysteme in Deutschland aufgeführt, s. C.13.

- Beschreibung des Verfahrens
- Keine weitergehenden Schlussfolgerungen

3.3 EBA-Hinweise

Enthält keine weiterführenden Informationen zum Thema „Referenzsysteme".

3.4 ORR Guideline

Enthält keine weiterführenden Informationen zum Thema „Referenzsysteme".

4 Beziehung zu den anderen Risikoakzeptanzgrundsätzen

Grundsätzlich stehen sich die Risikoakzeptanzgrundsätze gleichberechtigt gegenüber. Die Auswahl des geeigneten Risikoakzeptanzgrundsatzes wird mit CSM-VO 2.1.4 ausdrücklich dem Vorschlagenden überlassen, der Vorschlagende muss aber nach CSM-VO 2.1.5 die Angemessenheit nachweisen. Die in CSM-VO 2.5.1 angedeutete Nachrangigkeit des Risikoakzeptanzgrundsatzes der expliziten Risikoanalyse wird deshalb als Hinweis verstanden, dass die beiden ersten Risikoakzeptanzgrundsätze meistens leichter anwendbar sind und deshalb im Regelfall nicht auf die explizite Risikoanalyse zurückgegriffen wird, wenn einer der ersten beiden Risikoakzeptanzgrundsätze anwendbar ist.

5 Referenzsysteme zur Ermittlung von Sicherheitsanforderungen für „ähnliche Systeme"

Diese Vorgehensweise zur Ermittlung von Sicherheitszielen ist in der Vergangenheit in verschiedenen Fällen erfolgreich angewendet worden, um Sicherheitsziele für die Neuentwicklung von Systemen abzuleiten (Beispiele I60R, LZB80, Risikoanalyse ESTW Phase 1 der DB AG, …).

Dabei wurden nach EN 50129 auf Basis des Referenzsystems tolerierbare Gefährdungsraten abgeleitet, die neben den aktuellen Normenanforderungen als Sicherheitsziele für die Neuentwicklung dienten. Da in die Gefährdungsraten auch Gefährdungen aus Betrieb und Instandhaltung eingehen, an die entsprechende Anwendungsbedingungen zu stellen sind, erfüllen die tolerierbaren Gefährdungsraten die Definition des Begriffs Sicherheitsanforderung der CSM-VO.

Die oben beschriebene Methodik erfüllt die Anforderungen der CSM-VO auf folgende Weise:

CSM-VO	**Bewertung bzgl. Ermittlung von Sicherheitszielen aus Vergleich mit den Sicherheitseigenschaften ähnlicher Systeme**
2.4.1	Abstimmung der Gefährdungsanalyse mit den Beteiligten, in der Vergangenheit mit dem Eisenbahn-Bundesamt.

CSM-VO	**Bewertung bzgl. Ermittlung von Sicherheitszielen aus Vergleich mit den Sicherheitseigenschaften ähnlicher Systeme**
2.4.2a)	Typischerweise waren die Referenzsysteme zum Zeitpunkt der Verwendung als Referenzsystem im selben Eisenbahnsystem noch im Einsatz und hatten sich bewährt bzw. wurden noch neu installiert. Es konnte deshalb davon ausgegangen werden, dass ihre grundsätzlichen Sicherheitsmerkmale den aktuellen Anforderungen entsprachen, auch wenn sie nicht alle aktuellen Regelwerke bzw. Normen erfüllten. Durch die Abstimmung mit dem Eisenbahn-Bundesamt wurde die Anwendbarkeit durch eine Zulassungsbehörde bestätigt.
2.4.2b)	In den meisten Fällen handelte es sich um Erneuerungen bestehender Systeme. Die grundsätzlichen eisenbahnbetrieblichen Funktionen und Schnittstellen waren deshalb zumindest ähnlich. Dies wurde innerhalb der Sicherheitsanalyse bzw. Gefährdungsanalyse des jeweiligen Systems erläutert.
2.4.2c)	Bei den Anwendungen handelte es sich um Erneuerungen bestehender Systeme bzw. die Anwendung im gleichen betrieblichen Umfeld. Die Anforderung wurde deshalb implizit erfüllt. Bei zukünftigen Anwendungen sollte in der Sicherheits-/Gefährdungsanalyse festgestellt werden, dass es sich um ähnliche betriebliche Bedingungen handelt. Da sich die Anwendung des Referenzsystems auch nur auf einzelne Gefährdungen beziehen darf, ist die Feststellung ähnlicher Betriebsbedingungen für diejenigen Gefährdungen hinreichend, für die das Referenzsystem herangezogen werden soll.
2.4.2d)	Hier gilt das Gleiche wie für 2.4.2c) Betriebsbedingungen. Allerdings lässt sich feststellen, dass beim angewendeten Konzept nach EN 50129 auch unterschiedliche Umweltbedingungen nicht schädlich sind, da die Hazard Rates bzw. die Tolerable Hazard Rates unabhängig von konkreten Umweltbedingungen definiert werden können bzw. gegenüber diesen neutral sind. So kann ein Referenzsystem durchaus auch bei unterschiedlichen Umweltbedingungen herangezogen werden, solange die anderen Anforderungen erfüllt sind, es muss dann nur darauf geachtet werden, dass der Nachweis mindestens gleichen Sicherheitsniveaus unter Berücksichtigung der neuen Umgebungsbedingungen erfolgt (s.2.4.4).
2.4.3a)	Es wurden keine Risikowerte abgeleitet, sondern die Risiken wurden auf Basis der aus den Referenzsystemen abgeleiteten THRs als vertretbar angesehen.
2.4.3b)	Die Referenzsysteme wurden einer tiefgehenden Sicherheitsanalyse zur Ermittlung der erreichten Gefährdungsraten unterzogen (Reverse Engineering der Sicherheitsziele). Dies war erforderlich, da die Referenzsysteme nicht nach EN 50129 entwickelt waren und deshalb keine expliziten Gefährdungsraten vorlagen. Bei Anwendung der Methodik auf nach EN 50129 entwickelte Referenzsysteme kann direkt auf die dort definierten THRs zurückgegriffen werden.
2.4.3c)	Entspricht der Vorgehensweise nach EN 50126/50129, die Basis für die Systemerneuerungen war.
2.4.4	Ermöglicht bei Unterschieden zwischen Referenzsystem und betrachtetem System die gesonderte Betrachtung nicht abgedeckter Gefährdungen nach anderen Verfahren. Die Akzeptanz der vom Referenzsystem abgedeckten Risiken bleibt erhalten. Dieser Passus kommt typischerweise zur Anwendung, wenn in einem neuen System zur vom Referenzsystem abgedeckten Grundfunktionalität weitere Funktionen hinzugefügt

CSM-VO	**Bewertung bzgl. Ermittlung von Sicherheitszielen aus Vergleich mit den Sicherheitseigenschaften ähnlicher Systeme**
	werden.
2.4.5	S. 2.4.4 – die Anwendung von anderen Verfahren auf Abweichungen ist zulässig und verhindert nicht die Anwendung des Risikoakzeptanzgrundsatzes Referenzsystem.
2.5.4	Steht im Zusammenhang mit 2.4.4 und 2.4.5: wenn weder die Anwendung eines Referenzsystems noch Regelwerke einen passenden Risikoakzeptanzgrundsatz ergeben, gibt dieser Abschnitt eine Obergrenze für einen expliziten Risikoakzeptanzgrundsatz an. Ein unmittelbarer Anwendungsfall ist noch nicht bekannt, der Wert von 10^{-9}/h als Grenzwert für Gefährdungen, die direkt zu katastrophalen Folgen führen, ist aber allgemein akzeptierte Praxis.

Bemerkung 1: Erweiterungen und Änderungen können durch neue Gefährdungsursachen zu zusätzlichen Gefährdungsbeiträgen führen, sodass exakt gleiche Sicherheit nicht erreicht werden kann. In diesem Fall kann hinreichende Sicherheit nachgewiesen werden, indem das aus dem Referenzsystem ermittelte Sicherheitsziel geringfügig reduziert wird. Entsprechend dem Konzept des allgemein vertretbaren Risikos kann hierfür ein Maximalwert von 10 % angesetzt werden (s. auch Ergebnisbericht AVR)

Bemerkung 2: In obenstehender Tabelle wurde vorausgesetzt, dass der Vergleich mit dem Referenzsystem auf Basis von Top Level-Sicherheitszielen erfolgt. Bei Vergleich von Systemen auf Basis detaillierter Sicherheitsanforderungen tiefer Designebenen ist damit zu rechnen, dass Sicherheitsanforderungen des Referenzsystems im neuen Kontext nicht mehr relevant oder sinnvoll anwendbar sind.

Für die Ermittlung von Sicherheitszielen für ähnliche Systeme auf Basis von Referenzsystemen lässt sich zusammenfassend feststellen, dass die in der CSM-VO aufgeführten Anforderungen weitgehend der bisher gängigen Praxis entsprechen.

6 Cross acceptance von Systemen auf Basis der Anwendung des identischen Systems in einem anderen Kontext

Eine weitere Anwendung von Referenzsystemen ergibt sich im Bereich der Cross Acceptance.

Nach EN 50129 ist Cross Acceptance (gegenseitige Anerkennung) definiert als:

Zitat:

„gegenseitige Anerkennung

Zustand eines Produktes, den es mit der Anerkennung durch eine Behörde nach den zuständigen Europäischen Normen erreicht und in dem es durch andere Behörden ohne weitere Begutachtungen ebenfalls anerkannt werden kann."

Cross Acceptance wurde in der Vergangenheit in vielen Fällen erfolgreich angewendet. Mit dem TR 50506-1:2007 wurde ein Anwendungsleitfaden zur EN 50129 erstellt, der mögliche Verfahren zur Cross Acceptance beschreibt.

Im Unterschied zum ersten Fall ist das Hauptziel der Cross Acceptance nicht die Ableitung von Sicherheitszielen, sondern die Anerkennung des zu bewertenden Systems in einem neuen Anwendungskontext. Bei grundsätzlich vergleichbarem Sicherheitsniveau in den zu vergleichenden Anwendungsgebieten (verschiedene Betreiber, unterschiedliche Länder,…) kann aber davon ausgegangen werden, dass ähnliche Anwendungsfälle auf vergleichbaren Sicherheitszielen basieren, weshalb eine explizite Ableitung von Sicherheitszielen oder eine Entwicklung nach einem spezifischen Regelwerk nicht erforderlich sind.

Entscheidend ist dabei der Vergleich der Anwendungsbedingungen, da das System höchstens geringfügig angepasst sein darf, wenn Cross Acceptance zur Anwendung kommen soll, die Anwendungsbedingungen aber recht unterschiedlich sein können. In diesem Sinn ist als Referenzsystem nicht nur das technische System zu verstehen, auf das Cross Acceptance angewendet werden soll, sondern der Bereich des Eisenbahnsystems, in dem das technische System bereits zur Anwendung gekommen ist (man könnte auch von Referenzanwendung sprechen). Dieses Verständnis des Begriffs Referenzsystem ist kompatibel mit der CSM-VO, da dort in den Begriffsdefinitionen zwischen „technischen System" und „System" unterschieden wird, wobei als System der Teil eines Eisenbahnsystems verstanden wird, der Gegenstand einer Änderung ist, die auch betrieblicher Art sein kann, also auch der Anwendungskontext eines technischen Systems.

Cross Acceptance ist nur für generische Produkte oder Anwendungen vorgesehen, nicht für spezifische Anwendungen (da diese ja spezifisch erstellt werden und sich immer von den Vorgänger-Anwendungen unterscheiden).

Mit Erscheinen der CSM-VO unterliegen auch Cross Acceptance-Verfahren den Regelungen der CSM-VO. Auch wenn die Regelungen der CSM-VO zunächst eher im Sinne der Ableitung von Sicherheitszielen zu verstehen sind, lässt sich doch zeigen, dass auch die Cross Acceptance unter diesem Risikoakzeptanzgrundsatz durchführbar ist:

CSM-VO	**Bewertung bzgl. Cross Acceptance**
2.4.1	Cross Acceptance-Verfahren wurden und werden immer in Zusammenarbeit mit den zukünftigen Anwendern sowie den Zulassungsverantwortlichen durchgeführt. Dieser Abschnitt beschreibt nur die bisher bereits gängige Praxis.
2.4.2a)	Im Gegensatz zum ersten Anwendungsfall ist das Referenzsystem nicht beim zukünftigen Anwender des zu bewertenden Systems im Einsatz, sondern bei einem anderen

CSM-VO	**Bewertung bzgl. Cross Acceptance**
	Anwender, häufig in einem anderen Eisenbahnsystem in einem anderen Land. Das Referenzsystem nach CSM-VO ist bei Anwendung auf Cross Acceptance eigentlich eine „Referenzanwendung". Im Cross Acceptance-Verfahren ist deshalb zu prüfen, ob der als Referenzsystem gewählte Einsatzfall vergleichbare Sicherheitsanforderungen beinhaltet, wie sie beim zukünftigen Anwender anzulegen sind. Innerhalb der EU kann das derzeit nicht grundsätzlich vorausgesetzt werden (s. Safety Report 2012 der ERA, Figure 17 und 18).
2.4.2b)	Da es sich beim Cross Acceptance-Verfahren um den Einsatz desselben Systems in einem anderen Anwendungsbereich handelt, kann dieser Punkt als erfüllt vorausgesetzt werden. Allenfalls geringfügige Anpassungen sind nach TR 50506-1 innerhalb eines Cross Acceptance-Verfahren erforderlich, müssen dann aber auf neue Risiken analysiert werden (TR 50506-1 Abschnitt 4.4.1 f) und Kerngrundsätze Abschnitt 4.4.2 c) – e).
2.4.2c)	Das Cross Acceptance-Verfahren nach TR 50506-1 sieht eine detaillierte Analyse der neuen Betriebsbedingungen in Bezug auf das zu bewertende System vor. S. TR 50506-1 Tab. 1 Zeile „Auswertung der Unterschiede" und Kern-Grundsätze Abschnitt 4.4.2 c) - e).
2.4.2d)	Hier gilt das Gleiche wie für 2.4.2c) Betriebsbedingungen.
2.4.3a)	Gilt auch für Cross Acceptance, wenn von einem vergleichbaren Sicherheitsniveau in der Referenzanwendung ausgegangen werden kann.
2.4.3b)	Bei Cross Acceptance steht nicht die Ableitung von Sicherheitsanforderungen im Vordergrund, sondern die Bewertung der Sicherheitseigenschaften des existierenden Systems für den neuen Anwendungsfall. Dabei kann bei hinreichender Übereinstimmung der funktionalen und betrieblichen Einsatzbedingungen sowie der Umweltbedingungen davon ausgegangen werden, dass die Sicherheitseigenschaften des zu bewertenden Systems für den neuen Einsatzfall hinreichend sind, solange von grundsätzlich vergleichbarem Sicherheitsniveau von Referenzanwendungsfall und neuem Anwendungsfall ausgegangen werden kann (vergleiche 2.4.2a)).
2.4.3c)	Innerhalb des Cross Acceptance-Verfahrens nach TR 50506-1 ist die Auswertung des Gefährdungslogbuchs des Cross-Acceptance-Systems vorgesehen. Nach TR 50506-1 soll das Gefährdungslogbuch entsprechend der neuen Anwendung aktualisiert werden (s. TR 50506-1 Tab. 1 Zeile „Auswertung der Unterschiede").
2.4.4	Ermöglicht bei Unterschieden zwischen Referenzsystem/-anwendung und neuer Anwendung die gesonderte Betrachtung nicht abgedeckter Gefährdungen nach anderen Verfahren. Die Akzeptanz der vom Referenzsystem bzw. der Referenzanwendung abgedeckten Risiken bleibt erhalten. Dieser Passus kommt typischerweise zur Anwendung, wenn im neuen Anwendungsfall Gefährdungen identifiziert wurden, die im Referenzsystem/anwendungsfall keine Rolle gespielt haben.
2.4.5	S. 2.4.4 – die Anwendung von anderen Verfahren auf Abweichungen ist zulässig und verhindert nicht die Anwendung des Risikoakzeptanzgrundsatzes Referenzsystem. Zur Beherrschung von Risiken aus Abweichungen zum Referenzsystem s. TR 50506-1,

CSM-VO	Bewertung bzgl. Cross Acceptance
	Abschnitt 4.4.2 d) und e).
2.5.4	Steht im Zusammenhang mit 2.4.4 und 2.4.5: wenn weder die Anwendung eines Referenzsystems noch Regelwerke einen passenden Risikoakzeptanzgrundsatz für eine im neuen Anwendungskontext neue Gefährdung ergeben, gibt dieser Abschnitt eine Obergrenze für einen expliziten Risikoakzeptanzgrundsatz an. Ein unmittelbarer Anwendungsfall ist noch nicht bekannt, der Wert von 10^{-9}/h als Zielwert für katastrophale Gefährdungen ist aber allgemein akzeptierte Praxis.

In Fällen, in denen die Vergleichbarkeit der Sicherheitsniveaus von Referenzsystem-Anwendungsbereich und Cross Acceptance-Anwendungsbereich nicht gegeben ist, kann es sinnvoll sein, zusätzlich ein ähnliches Referenzsystem aus dem Cross-Acceptance-Anwendungsbereich zu verwenden, um einen Vergleich mit Sicherheitszielen entsprechend 4.2.1 durchführen zu können.

Zusammenfassend lässt sich feststellen, dass die Anwendbarkeit des Risikoakzeptanzgrundsatzes „Referenzsystem" auf die Cross Acceptance sich zwar nicht unmittelbar aus den Formulierungen der CSM-VO ergibt, sich die Anforderungen der CSM-VO aber alle auf den TR 50506-1 abbilden lassen. Damit kann es als plausibel angesehen werden, dass Cross Acceptance als CSM-VO-kompatibles Verfahren zum Risikomanagement bei der Übertragung eines Systems in einen neuen Anwendungsfall angesehen werden kann.

7 Überlegungen zum Absatz 2.4.5

Der Absatz 2.4.5 wirkt zunächst irritierend, da bei Nichterreichen des Sicherheitsniveaus des Referenzsystems auf eine der beiden anderen Methoden für Risikoakzeptanzgrundsätze verwiesen wird, aus denen dann weiterreichende Sicherheitsmaßnahmen ermittelt werden sollen. Damit müsste es dann aber eigentlich möglich sein, wiederum das Sicherheitsniveau des Referenzsystems zu erreichen.

Sinn macht der Absatz, wenn man annimmt, dass ein Nachweis gleichen Sicherheitsniveaus wie beim Referenzsystem qualitativ statt quantitativ durch Übernahme von technischen Sicherheitsanforderungen erfolgen soll, aber wegen Abweichungen für bestimmte Punkte in dieser Form nicht geführt werden kann (was nicht automatisch bedeutet, dass das Sicherheitsniveau nicht ausreicht, sondern nur, dass ein direkter Vergleich nicht möglich ist). In diesem Fall macht es Sinn, für die betroffenen Punkte / Gefährdungen auf die anderen Risikoakzeptanzgrundsätze zu verweisen, um hinreichende Sicherheit nachzuweisen.

Als ein Sonderfall könnte die gängige Praxis angesehen werden, kleine Verschlechterungen des Sicherheitsniveaus zu akzeptieren, z.B. 5 oder 10 %, wenn durch Einführung neuer Technik zusätzliche Gefährdungen entstehen, ohne dass eine Kompensation an anderer Stelle möglich ist (z.B. wenn einem existierenden System ohne weitere Änderungen eine Schnittstelle hinzugefügt wird). Hierbei entsteht, wenn auch auf Basis eines Referenzsystems, ein neues explizites Risikoakzeptanzkriterium.

8 Zusammenfassung

Mit dem Risikoakzeptanzgrundsatz Referenzsystem steht innerhalb der CSM-VO ein Risikoakzeptanzgrundsatz zur Verfügung, der in der Vergangenheit häufig angewendet wurde und dessen Anforderungen von den gängigen Vorgehensweisen im Rahmen der CENELEC Normen EN 5012X erfüllt werden.

Insbesondere wurde gezeigt, dass bewährte Vorgehensweisen

- zur Ableitung von Sicherheitsanforderungen an ein neues System aus denen eines Referenzsystems und
- zur Cross-Acceptance eines existierenden Systems in einem neuen Kontext

durch diesen Risikoakzeptanzgrundsatz gedeckt sind.

9 Referenzen

CSM-VO	Verordnung der Kommission über die Festlegung einer gemeinsamen Sicherheitsmethode für die Evaluierung und Bewertung von Risiken, Version Nr. 352/2009 vom 24. April 2009,Version Nr. 402/2013 vom 30. April 2013
EBA Leitlinie	Hinweise für die Anwendung der Verordnung (EG) Nr. 352/2009 der Kommission vom 24.04.2009 über die Festlegung einer gemeinsamen Sicherheitsmethode für die Evaluierung und Bewertung von Risiken gemäß Artikel 6 Abs. 3 Buchstabe a der Richtlinie 2004/49/EG des Europäischen Parlaments und des Rates durch das Eisenbahn-Bundesamt
EN 50126	DIN EN 50126: Spezifikation und Nachweis der Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit, Sicherheit (RAMS), 2000
EN 50129	DIN EN 50129, Bahnanwendungen, Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme, Sicherheitsrelevante elektronische Systeme für Signaltechnik, 2003
ERA Beispiele	Sammlung von Beispielen für Risikobewertungen und möglicher Werkzeuge zur Unterstützung der CSM-Verordnung, ERA/GUI/02-2008/SAF
ERA Leitlinie	Leitlinie zur Anwendung der Verordnung der Kommission über die Festlegung einer Gemeinsamen Sicherheitsmethode für die Evaluierung und Bewertung von Risiken, ERA/GUI/01-2008/SAF
ERA Safety Report 2012	"Railway safety performance in the European Union" 2012, www.**era**.europa.eu/Document-Register/Documents/**SafetyReport**2012.pdf
Ergebnisbericht AVR	Projekt NeGSt, Teilbericht „Allgemein vertretbares Risiko", 26.06.2013
ORR Guideline	ORR guidance on the application of the common safety method (CSM) on risk evaluation and assessment, Dec. 2012
TR 50506-1	CLC/TR 50506-1: Railway applications - Communication, signalling and processing systems -Application Guide for EN 50129 - Part 1: Cross-acceptance

10 Abkürzungen

Abk.	Langform / Erläuterung
CENELEC	Europäisches Komitee für Elektrotechnische Normung
DB	Deutsche Bahn
EBO	Eisenbahn-Bau- und Betriebsordnung
EN	Europäische Norm
ERA	European Railway Agency
GAMAB	Globalement Au Moins Aussi Bon
LZB	Linienförmige Zugbeeinflussung
ORR	Office of Rail Regulation
THR	Tolerable Hazard Rate