Neue Generation Signaltechnik

Sektorweite Initiative zur Sicherung der Zukunftsfähigkeit der Leit- und Sicherungstechnik

Teilbericht

AP 2100 – Erfüllung der CSM VO durch Anwendung der CENELEC-Normen

10.01.2013

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
13.11.2012	Braband, Griebel (Siemens AG)	V01	Erstellung
07.12.2012	Braband (Siemens AG)	V02	Einarbeitung von Beiträgen von Hrn. Heinig und Feucht (Thales) sowie Hrn. Griebel (Siemens AG)
10.01.2013	Braband (Siemens AG)	V03	Abstimmung durch Walkthrough-Review

Inhaltsverzeichnis

1 Einleitung

Der Umgang mit Änderungen, die vollständig auf Grundlage von Regelwerken durchgeführt werden, hat bei der Durchführung der EG Verordnung 352/2009 zu einigen Diskussionen geführt. Dies liegt unter anderem an teilweise den Sinn der Verordnung verändernden Übersetzungen aus dem englischen Original, aber auch an unklaren oder unvollständigen Formulierungen.

Insbesondere im Fall, dass das Regelwerk die CENELEC-Normen EN 50126 ff sind, war es eigentlich Intention der ERA-Arbeitsgruppe, dass bei Einhaltung dieser Normenreihe automatisch auch die Vorgaben der CSM-VO erfüllt sind. Allerdings wurde dies in der CSM VO nicht direkt hinterlegt, sondern nur in den Guidance Dokumenten der ERA diskutiert. Außerdem kann es natürlich sein, dass diese Absicht im komplizierten politischen Komitologie-Prozess der EU, der sich an die Erarbeitung der technischen Empfehlung der ERA anschließt, verwässert oder verändert wurde.

Deswegen soll in diesem Dokument explizit analysiert werden, ob und ggf. unter welchen Randbedingungen die Aussage „Mit der Einhaltung der CENELEC-Normen EN 50126 ff werden auch die Anforderungen der CSM Vo erfüllt" gültig ist. Mit der Bezeichnung EN 50126ff ist der derzeit gültige Stand der CENELEC-Normen EN 50126, 50128 und 50129 gemeint. Der Revisionsentwurf wird zur Unterscheidung als prEN 50126-x bezeichnet.

2 Vorgaben der CSM VO

Der grundsätzliche Prozess aus der CSM VO wird noch einmal dargestellt, um die Lesbarkeit zu erleichtern:

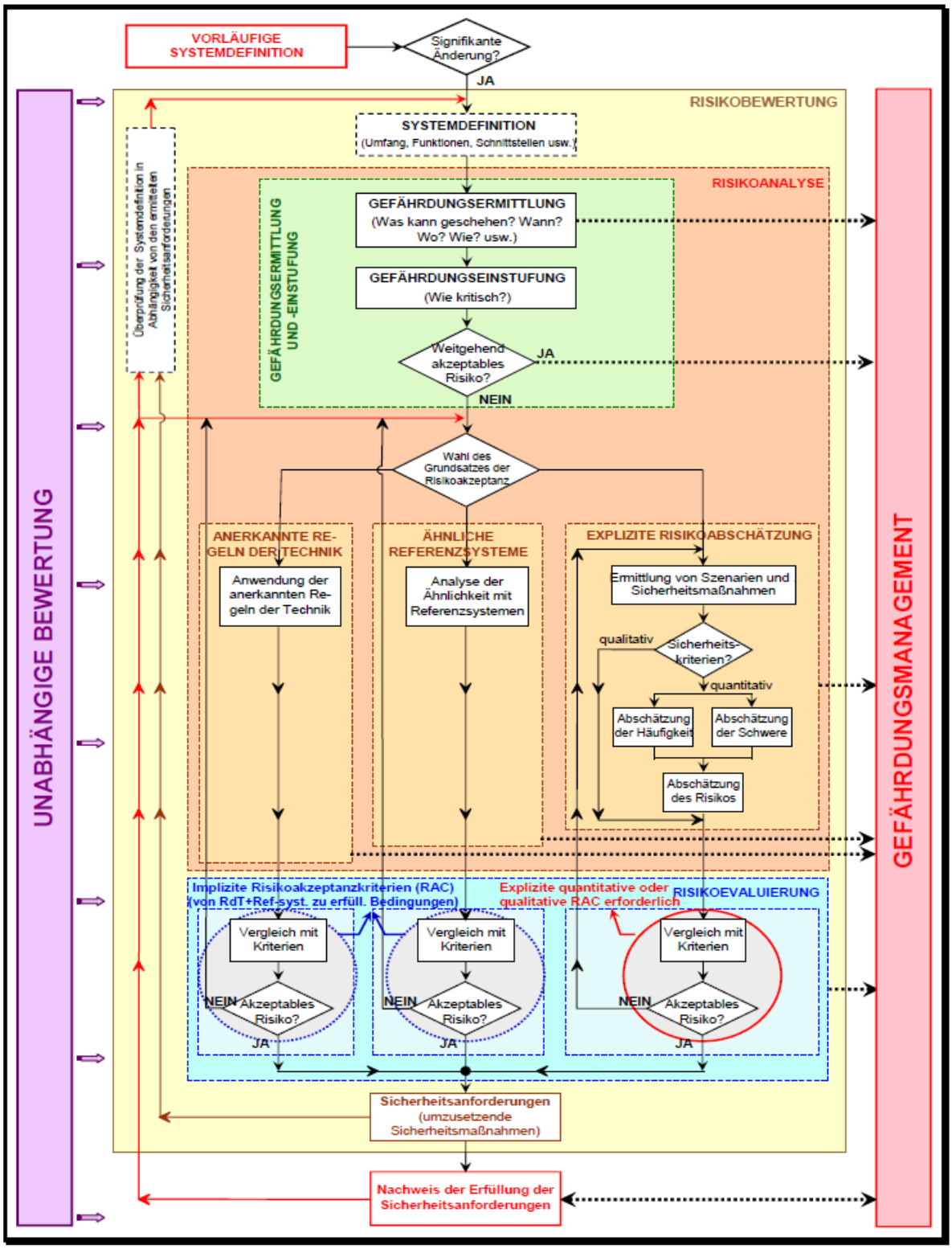

Abbildung 1: CSM Prozess

Aus rechtlichen Gründen verweist die CSM VO nicht direkt auf die CENELEC-Normen, aber in Kapitel 2 der Beispielsammlung zur CSM VO [CSM EX] wird explizit auf den Zusammenhang zur CSM VO eingegangen:

Das Risikomanagementverfahren der CSM lässt sich als V-Darstellung abbilden, beginnend mit der (vorläufigen) Systemdefinition und endend mit der Systemabnahme: Siehe Abbildung 4. Dieses ver-

einfachte 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.

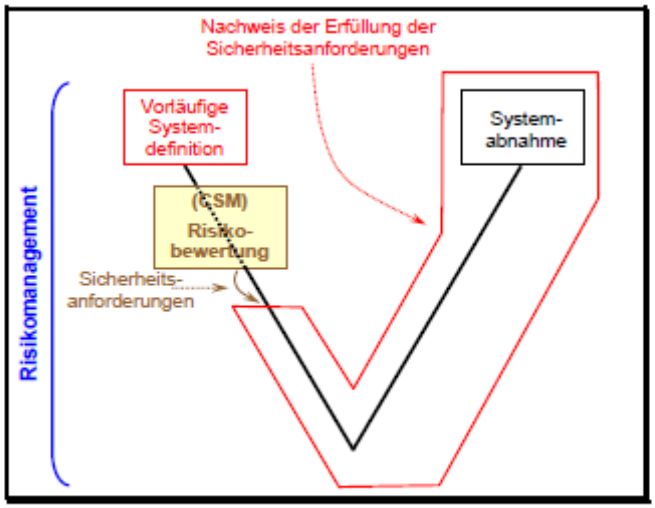

Abbildung 4 : Vereinfachte V-Darstellung nach Bild 10 der Norm EN 50 126.

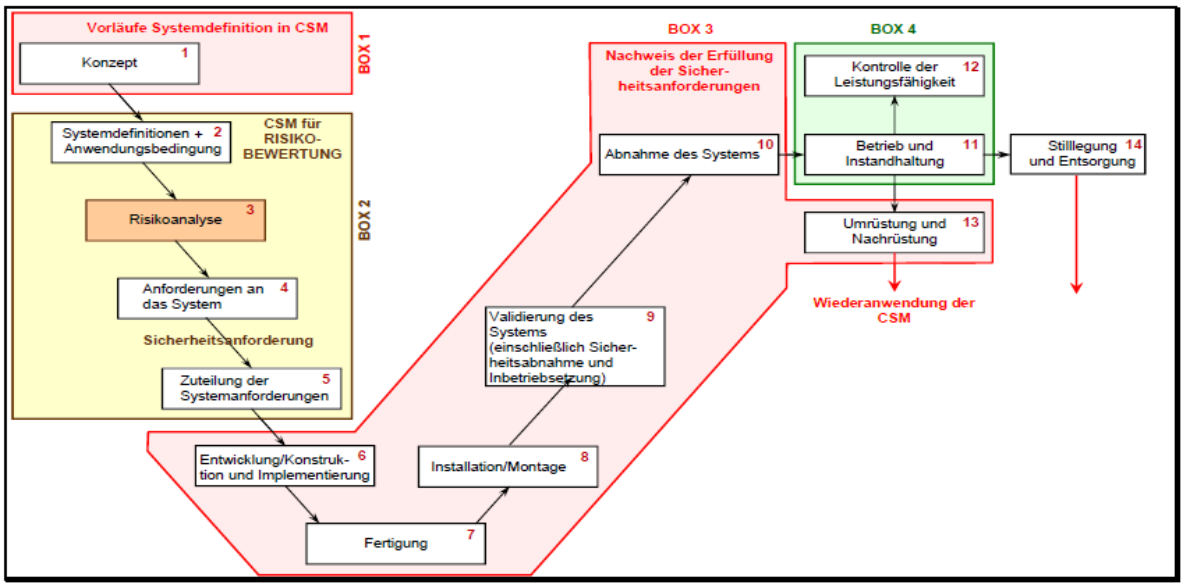

Abbildung 5 : Bild 10 aus der Norm EN 50 126 V-Darstellung (CENELEC Systemlebenszyklus).

Abbildung 2: Vergleiche CSM Prozess und CENELEC V-Modell

Dieser Zusammenhang wird dann in weiteren Ausführungen und Abbildungen noch detailliert. Insbesondere wird explizit festgestellt:

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. …
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.

Zusammengefasst kommt die ERA zu folgendem Ergebnis:

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.

Daraus ist eindeutig die Absicht belegbar, dass CSM VO und CENELEC-Normen vom Entwurf her kompatibel sein sollen. In den folgenden Abschnitten wird geprüft, ob sich im Detail Abweichungen davon erkennen lassen.

3 Analyse

3.1 Voraussetzungen

Die folgenden Annahmen bzw. Voraussetzungen werden der Analyse zugrunde gelegt:

1. Es werden nur Änderungen an technischen Systemen betrachtet
2. Die Änderungen erfolgen vollständig auf Grundlage der CENELEC-Normen EN 50126/28/29
3. Es wird der derzeit gültige Stand der CENELEC-Normen betrachtet. Eine Erweiterung der Analyse auf die neuen prEN 50126-x Entwürfe erfolgt im Anhang
4. Falls der Hersteller Vorschlagender ist, wird ohne Beschränkung der Allgemeingültigkeit der Analyse angenommen, dass die Änderung wie eine signifikante Änderung behandelt wird. Damit kann auf die Betrachtung dieses Schrittes verzichtet werden und die Analyse verkürzt werden.

3.2 Prozess-Analyse

Die Analyse erfolgt aus dem Blickwinkel der CENELEC-Normen, d. h. es wird angenommen, dass diese erfüllt wurden und es wird argumentiert, wie die CSM VO dadurch ebenso erfüllt wird.

3.2.1 Unabhängige Bewertung

Die CENELEC-Normen machen keine Aussagen über Auswahlkriterien für Bewertungsstellen, sondern stellen nur Anforderungen an die Unabhängigkeit und Kompetenz eines Gutachters als Ersteller eines unabhängigen Sicherheitsgutachtens. Insofern gibt es keine Widersprüche, es müssen aber ggf. zusätzliche Anforderungen bez. Anerkennung von Bewertungsstellen nach CSM VO berücksichtigt werden. Liegt eine Akkreditierung nach DIN ISO 17020 vor, so sollten die Anforderungen an die Bewertungsstellen erfüllt sein.

3.2.2 Gefährdungsmanagement

Die Aktivitäten sind inhaltlich in den CENELEC-Normen vorhanden und den entsprechenden Phasen zugeordnet.

3.2.3 Vorläufige Systemdefinition und Signifikanzbewertung

Die vorläufige Systemdefinition entspricht der Konzeptphase (Phase 1 in CENELEC). Wenn jede Änderung als signifikant behandelt wird, ist dieser Schritt nicht relevant und kann entfallen.

3.2.4 Systemdefinition

Dieser Schritt ist identisch mit Phase 2 nach CENELEC. Der Inhalt erscheint zunächst in zwei Punkten detaillierter, und zwar wird in 2.2.6 gefordert

(f) bestehende Sicherheitsmaßnahmen und – nach mehrfacher Anwendung – Definition der im Rahmen des Risikobewertungsverfahrens ermittelten Sicherheitsanforderungen;
(g) Annahmen, die die Grenzen der Risikobewertung bestimmen.

Bei erstmaliger Anwendung gibt es in der Regel keine bestehenden Sicherheitsmaßnahmen, d. h. Forderung (f) ist nicht relevant. Bei einer Änderung (Phase 13 Umrüstung und Nachrüstung in CENELEC) wird in die Phase zurückgesprungen, die relevant ist. Wird die Risikoanalyse nicht verändert, so wird natürlich auf dem vorhandenen Sicherheitsnachweis bzw. den aus der Risikoanalyse abgeleiteten Sicherheitszielen aufgebaut, aber es erscheint inhaltlich nicht sinnvoll, hier formal noch einmal die Systemdefinition der Risikoanalyse anzupassen. Außerdem wird im Rahmen des Sicherheitsmanagements nach EN 50129 für jede Änderung ein Sicherheitsplan erstellt, der wiederum eine Systemdefinition enthält. Dort sollte Punkt (f) berücksichtigt werden und wird es inhaltlich auch.

Der Punkt (g) ist ein Teilaspekt der Annahmen, die der Risikoanalyse zugrunde liegen. Er wird nach EN 50126 Abschnitt 4.6.2.1 im Rahmen der Risikoanalyse dokumentiert. Aus fachlicher Sicht ist das ausreichend. Eine Notwendigkeit, dies bereits im Rahmen der Systemdefinition zu tun, ergibt sich nicht.

3.2.5 Gefährdungsermittlung

Dieser Schritt ist enthalten in Phase 3 nach CENELEC.

3.2.6 Gefährdungseinstufung und Weitgehend Akzeptables Risiko

Die CENELEC Normen benutzen das Konzept des Weitgehend Akzeptablen Risikos nicht. Wenn es nicht benutzt wird, ist auch der Schritt der Gefährdungseinstufung oder Gefährdungsklassifikation nicht zwingend notwendig und diese beiden Schritte können entfallen.

3.2.7 Wahl des Grundsatzes der Risikoakzeptanz

Die aktuell gültigen CENELEC-Normen benennen die verschiedenen Grundsätze nicht, sondern kennen nur die Phase 3 „Risikoanalyse", die dem Grundsatz der expliziten Risikoabschätzung nach

CSM VO entspricht. Insofern stellt die CSM VO formal eine Obermenge bez. der CENELEC-Normen dar, aber die CSM VO wird durch Wahl der Option „ähnliche Referenzsysteme" oder „explizite Risikoabschätzung" erfüllt.

Das Risikoakzeptanzkriterium GAMAB ist grundsätzlich sehr ähnlich zum Risikoakzeptanzkriterium „Vergleich mit Referenzsystem" nach CSM VO, d. h. diese Vorgehensweise wird auch bei Anwendung der CENELEC-Normen praktiziert.

3.2.8 Ähnliche Referenzsysteme

Dieser Ansatz wurde auch schon nach den CENELEC-Normen praktiziert.

3.2.9 Explizite Risikoabschätzung

Dieser Schritt ist enthalten in Phase 3 nach CENELEC.

3.2.10 Risikoevaluierung

Dieser Schritt ist enthalten in Phase 3 nach CENELEC.

3.2.11 Sicherheitsanforderungen

Dieser Schritt entspricht, je nach Detaillierungsgrad, Phase 4 oder 5 nach CENELEC. Die Phase „Zuteilung der Sicherheitsanforderungen" könnte auch teilweise oder ganz im Schritt „Nachweis der Erfüllung der Sicherheitsanforderungen" enthalten sein, wenn es sich z. B. um ein Gesamtsystem handelt.

3.2.12 Nachweis der Erfüllung der Sicherheitsanforderungen

Dieser Schritt umfasst die Phasen 6-11 sowie 13 nach CENELEC. Die CSM VO enthält diese Schritte nur der Vollständigkeit halber, macht aber keine konkreten gesetzlichen Vorgaben, sondern überlässt dieses den einschlägigen Normen.

4 Analyse der Dokumentation

Die CSM VO macht nur wenige Vorgaben bezüglich spezifischer Dokumentation. In den Beispielen der ERA zur CSM VO wird auch bereits festgestellt, dass „Diese Ausgaben der CSM-Risikobewertung … den sicherheitsbezogenen Outputs der Phase 4 in der V-Darstellung der CENELEC, d. h. der Spezifikation der Systemanforderungen, [entsprechen] …", d. h. die ERA hat hier selbst schon Kompatibilität festgestellt.

Dies bedeutet, dass bez. der Dokumentation nur noch wenige, in der CSM VO direkt genannte Dokumente zu betrachten sind.

4.1 Sicherheitsbewertungsbericht

Der Inhalt wird nicht detailliert vorgegeben. Das Gutachten nach CENELEC erfüllt die Vorgaben der CSM VO, soweit dies die technischen Änderungen betrifft. Trotzdem ist es natürlich ratsam , im Gutachten auf die spezifische Struktur des CSM-Prozesses einzugehen.

4.2 Gefährdungsprotokoll

Der Inhalt entspricht dem Gefährdungsprotokoll nach CENELEC, allerdings sind in der CSM VO zum Teil explizitere Vorgaben als in den CENELEC-Normen gemacht, z. B. explizite Ausweisung der Verantwortlichkeit für jede Gefährdung. Inhaltlich wird dies in der EN 50129 über die hierarchische Gliederung der Gefährdungen, siehe zum Beispiel Bild 9 sowie Bild A.4 dort, sowie die Zuordnung in den entsprechenden Sicherheitsplänen erreicht, aber es ist möglich, dass dies in den Gefährdungsprotokollen nicht explizit ausgewiesen wird. Bei technischen Änderungen, die nur einen Hersteller betreffen, ist die Verantwortung klar und muss nicht notwendigerweise explizit aufgeführt werden.

Weitere Abweichungen betreffen den Nachweis und die Herkunft des mit jeder Gefährdung verbundenen Risikos (akzeptabel oder nicht) sowie die Angabe und Herkunft des gewählten Risikoakzeptanzgrundsatzes und deren bestimmte Kriterien. Bei Änderungen an technischen Systemen ist diese Angabe nicht erforderlich, wenn sich an der Risikoanalyse nichts ändert.
Diesee Aspekte sollten gegebenenfalls in den überarbeiten CENELEC-Normen berücksichtigt werden.

4.3 Nachweis der Erfüllung der Sicherheitsanforderungen

Der Inhalt wird nicht detailliert vorgegeben. Der Sicherheitsnachweis nach CENELEC erfüllt für Änderungen an technischen Systemen die Vorgaben der CSM VO, da dieser explizit ein gleichnamiges Kapitel enthält.

5 Zusammenfassung

Die Analyse belegt inhaltlich die Gültigkeit der Aussage „Mit der Einhaltung der CENELEC-Normen EN 50126 ff werden auch die Anforderungen der CSM VO erfüllt". Diese Intention ist auch klar in den Leitlinien und Beispielen der ERA ersichtlich.

Aus formalen Gründen bzw. handwerklichen Unzulänglichkeiten bei der Abstimmung der CSM VO gibt es einzelne Abweichungen zwischen den CENELEC-Normen und der CSM VO. Eine Anpassung der Prozesse würde gegebenenfalls den Klärungsbedarf reduzieren. Es wird vorgeschlagen, die folgende Tabelle als Interpretationshilfe in den eigenen Prozess zu kopieren und diesen Ergebnisbericht als Erläuterung dazu zu referenzieren. Die Einträge in der Tabelle sind dabei als Vorschläge zu verstehen, die je nach firmenspezifischen Gegebenheiten angepasst werden können:

Thema	Abweichungen	Anpassung
Vorschlagender	Die CENELEC-Normen kennen den Begriff nicht.	Diese Rolle wird in der Regel durch den Betreiber wahrgenommen. Falls der Hersteller als Vorschlagender auftritt, dann sollte dies im Prozess berücksichtigt werden.
Signifikanzprüfung	Kategorisierung der geplanten Änderung Prüfung auf Sicherheitsrelevanz Prüfung der Signifikanz	Nur für Vorschlagende relevant. Diese Rolle wird in der Regel durch den Betreiber wahrgenommen. Falls eine Signifikanzbewertung notwendig ist, kann dieses nach [Ergebnisbericht_Signifikanz] durchgeführt werden.
Systemdefinition	Auflistung vorhandener systeminterner Sicherheitsmaßnahmen Umfang des Verfahrens festlegen (Systemannahmen und –grenzen)	Formale Abweichung, inhaltlich erfüllt siehe 3.2.4 Im Prozessschritt Systemdefinition sollte eine Erläuterung nach 3.2.4 aufgenommen werden, bzw. ein Verweis, wo die Inhalte (f) und (g) zu finden sind.
Risikoeinschätzung	Prüfung der Anteilseinhaltung und Zulässigkeit der Gefährdungen nach dessen Risikohöhen (akzeptabel oder nicht)	Nicht relevant, siehe 3.2.6.
Risikobewertung	Festlegung und Anwendung eines Risikoakzeptanzgrundsatzes für jede	Nicht relevant, siehe 3.2.7. Auswahl des Risikoakzep-

	Gefährdung Definition von Risikoakzeptanzkriterien	tanzkriteriums ist nach CE-NELEC nicht vorgegeben.
Gefährdungsmana-gement (Gefähr-dungsprotokoll)	Angabe des beteiligten Akteurs, der für Gefährdung verantwortlich ist Nachweis und Herkunft des mit jeder Gefährdung verbundenen Risikos (akzeptabel oder nicht) Angabe und Herkunft des gewählten Risikoakzeptanzgrundsatzes und deren bestimmten Kriterium	Formale Abweichung, inhalt-lich erfüllt, soweit dies tech-nische Änderungen betrifft, siehe 4.2 Der Aufbau des Gefähr-dungsprotokolls sollte ent-weder ergänzt werden, oder es sollten Erläuterungen im Sinne von 4.2 in die Prozess-beschreibung aufgenommen werden.
Gefährdungsmana-gement (Schnittstel-lenprotokoll)	Erstellung eines Schnittstellenprotokolls (wenn erforderlich) mit folgenden Kriterien: o Definition von Begriffen und Meldungen o Festlegung des Verantwortlichen für Dokumentation o Angaben zu allen Systemannahmen o Angaben zur Gefährdung und deren Risiken o Angaben zu den ermittelten Sicherheitsmaßnahmen durch die verschiedenen Grundsätze o Angaben zu den vorhandenen Verwendungsbeschränkungen o eigenen Erfahrungen beim Versuch der Risikokontrolle	Die CSM VO definiert nur informell eine „Meldung", die im Rahmen des Sicherheits-managements frei definiert werden kann. Ein geeigneter Ort wäre z. B. der Sicher-heitsplan, der auch die Be-ziehungen zu Unterauftrag-nehmern etc. regeln sollte. Die Dokumentation kann im Sicherheitsmanagementbe-richt erfolgen.
Nachweis der Erfül-lung der Sicher-heitsanforderungen	Dieser Nachweis ist Teil des Sicherheits-nachweises von CENELEC, soweit dies tech-nische Änderungen betrifft.	Nur für Vorschlagende rele-vant. Diese Rolle wird in der Regel durch den Betreiber wahrgenommen.
Unabhängige Be-wertung bzw. Si-cherheitsbewer-tungsbericht	Benennung einer Bewertungsstelle Bewertung der Vergleiche und Prüfungen sind in einem Sicherheitsbewertungsbericht zu dokumentieren	Siehe 3.2.1. Das Gutachten nach CENELEC erfüllt diese Anforderungen, soweit dies technische Änderungen be-trifft. Die Kriterien bez. unabhän-giger Bewertung sollte expli-zit aus der CSM VO über-nommen werden, wenn nicht nach DIN ISO 17020 vorge-gangen wird

Tabelle 1:Zusammenfassung der Ergebnisse

.

6 Anhang

6.1 Unabhängiger Vergleich der Ergebnisse

Eine ähnliche Aufgabenstellung wurde parallel und unabhängig davon in einer Diplomarbeit von Hrn. Heinig (TU Dresden) untersucht:

Die vorliegende Arbeit untersucht die qualitativen Risikomanagementprozesse für Bahnanwendungen und deren Anforderungen zum Nachweis einer konformen Anwendung der CSM-Verordnung und der EN 5012x. In diesem Zusammenhang wird die Konformität der Vorgehensweisen und Anforderungen nach der CSM-Verordnung und den EN 5012x analysiert.

Das angestrebte Ergebnis bestand allerdings in einer Synthese der CSM VO und der CENELEC-Normen, d. h. einer Vorgehensweise, die beide Prozesse unter einem Dach vereint. In der vorliegenden Analyse wird nur die Erfüllung der Anforderungen der CSM VO bei Vorgehen nach CENELEC untersucht, d. h. eine wesentlich eingeschränktere Fragestellung. Allerdings eignen sich die Ergebnisse der Diplomarbeit sehr gut als unabhängiger Check.

In Kapitel 6.2.3 werden die in der Diplomarbeit festgestellten Abweichungen zwischen CSM VO und CENELEC rot hervorgehoben. Diese Abweichungen werden jetzt in Bezug auf Relevanz für unsere Analyse untersucht. Es sei bemerkt, dass hier die Terminologie der Diplomarbeit verwendet wird und nur die dort erkannten Abweichungen diskutiert werden. Eine weitere Überprüfung der Argumentation bzw. Ergebnisse ist nicht erfolgt.

Thema	Abweichungen	Diskussion
Signifikanzprüfung	Kategorisierung der geplanten Änderung Prüfung auf Sicherheitsrelevanz Prüfung der Signifikanz	Nicht relevant, siehe 3.2.3
Systemdefinition	Auflistung vorhandener systeminterner Sicherheitsmaßnahmen Umfang des Verfahrens festlegen (Systemannahmen und –grenzen)	Formale Abweichung, inhaltlich erfüllt siehe 3.2.4
Risikoeinschätzung	Prüfung der Anteilseinhaltung und Zulässigkeit der Gefährdungen nach dessen Risikohöhen (akzeptabel oder nicht)	Nicht relevant, siehe 3.2.6.
Risikobewertung	Festlegung und Anwendung eines Risikoakzeptanzgrundsatzes für jede Gefährdung Definition von Risikoakzeptanzkriterien	Nicht relevant, siehe 3.2.7. Auswahl des Risikoakzeptanzkriteriums ist nach CENELEC nicht vorgegeben.
Gefährdungsmanagement (Gefährdungsprotokoll)	Angabe des beteiligten Akteurs, der für Gefährdung verantwortlich ist Nachweis und Herkunft des mit jeder Gefährdung verbundenen Risikos (akzeptabel oder nicht) Angabe und Herkunft des gewählten Risikoakzeptanzgrundsatzes und deren bestimmten Kriterium	Formale Abweichung, inhaltlich erfüllt, siehe 4.2
Gefährdungsmanagement (Schnittstellenprotokoll)	Erstellung eines Schnittstellenprotokolls (wenn erforderlich) mit folgenden Kriterien:	Die CSM VO definiert nur informell eine „Meldung", die im Rahmen des Sicher-

	o Definition von Begriffen und Meldungen o Festlegung des Verantwortlichen für Dokumentation o Angaben zu allen Systemannahmen o Angaben zur Gefährdung und deren Risiken o Angaben zu den ermittelten Sicherheitsmaßnahmen durch die verschiedenen Grundsätze o Angaben zu den vorhandenen Verwendungsbeschränkungen o eigenen Erfahrungen beim Versuch der Risikokontrolle	heitsmanagements frei definiert werden kann. Ein geeigneter Ort wäre z. B. der Sicherheitsplan, der auch die Beziehungen zu Unterauftragnehmern etc. regeln sollte.
Unabhängige Bewertung	Benennung einer Bewertungsstelle Bewertung der Vergleiche und Prüfungen sind in einem Sicherheitsbewertungsbericht zu dokumentieren	Siehe 3.2.1. Das Gutachten nach CENELEC erfüllt diese Anforderungen.

Tabelle 3: Vergleich der Abweichungen

6.2 Vergleich zwischen CENELEC und Revisions-Entwurf CSM VO

Die folgenden Tabellen stellen zunächst die größeren und kleineren Änderungen zwischen der gültigen CSM VO und dem Revisionsentwurf DV 36 vom 6.11.2012 dar. Dies war die Version, die in RISC verteilt wurde.

Größere Änderungen der DV36 gegenüber CSM-VO (352/2009)	**siehe DV36 bei**
Maintenance-Stellen: Auf gleicher Ebene wie Eisenbahnunternehmen (EU´s) und Fahrwegbetreiber (FB´s) tauchen jetzt zusätzlich Maintenance-Stellen auf, die auch ein risk assessment betreiben müssen (mit Verweis auf Artikel 14 von Richtlinie 2004/49/EC bzw. Hinweis auf spezielle Verordnung No 445/2011)	Präambel (4), (12), viele andere Stellen, an denen bisher nur EU´s bzw. FB´s aufgeführt waren
Erweiterter Scope: Im Scope der 352/2009 ist Pkt. 3 (Ausnahmen für Metros, Trams etc.) gestrichen. D.h. die Verordnung ist dann auch für diese Art von Bahnen gültig.	Article 2
Akkreditierung/Recognition: Aufnahme eigener Regelungen für Stellen, die die Eignung von Bewertungsstellen (im Sinne der CSM-VO) feststellen sollen. Alternativ zur Akkreditierung wird auch die Option der Recognition einer Bewertungsstelle behandelt.	- Präambel (13), (14), (15), (17) - Definitions (29), (30) - Article 7 - Article 8 - Article 11 - Article 13 - Article 14 - Annex II
Zusätzlicher Annex III mit Hinweisen zum Inhalt des Safety Assessment Reports	Annex III

Tabelle 4: Größere Änderungen im Revisionsentwurf

Weitere Änderungen der DV36 gegenüber CSM-VO (352/2009)	**siehe DV36 bei**
Neue/geänderte Definitionen	Definitions (11) (25) (27) – (30)
Meinungsbildung des Proposers zum Safety Assessment Report: Der Proposer soll/kann Position beziehen zu den Conclusions im Safety Assessment Report und ggfs. begründen, an welchen Stellen er nicht zustimmt und warum.	Article 15 Pkt. 1
Berücksichtigung des Safety Assessment Report durch die NSA: - 352/2009, Article 7 Pkt. 2: „… the safety assessment report shall be taken into account by the national safety authority in its decision …". - DV36: "… the safety assessment report shall be accepted by the national safety authority in its decision …".	Article 15, Pkt. 2 und 3
Berücksichtigung des Safety Assessment Report durch den NoBo: - 352/2009, Article 7, Pkt. 3: „… the safety assessment report shall be taken into account by the notified body". - DV36: "… the safety assessment report shall be accepted by the notified body … unless…"	Article 15, Pkt. 4
Außerkraftsetzen von 352/2009: 1 Jahr nach Inkraftsetzen von DV31 (bzw. der dann offiziellen Version der CSM-VO)	Article 18
Datum, ab dem die Verordnung anzuwenden ist: 1 Jahr nach Inkraftsetzen.	Article 19
Präzisierung der Bedingungen, dass ein **code of practice als relevant zur Gefährdungsabdeckung** angesehen werden kann: "Successful application of a code of practice for similar cases to manage changes and control effectively the identified hazards of a system in the sense of this Regulation is sufficient for it to be considered as relevant"	Annex I, 2.3.2 (b)
Codes of practice müssen nicht mehr „publicly available" sein: In DV36 heißt es jetzt: "Upon request, they must be available to assessment bodies for them to either assess or, where relevant, mutually recognise…"	Annex I, 2.3.2 (c)
Präzisierung der inhaltlichen Anforderungen an Annex I, 5. „EVIDENCE FROM THE APPLICATION OF THE RISK MANAGEMENT PROCESS" . - Ergänzung "… of the appropriateness of its results are accessible.. **"** - neu - neu	Annex I, 5. 5.1 5.2 (c) und (d) 5.3
Grafik im Appendix, Aussprünge ergänzt: „Justify and document" bei Aussprüngen aus „Significant Change?" und „Broadly Acceptable?"	Appendix

Tabelle 5: Weitere Änderungen im Revisionsentwurf

Zusammenfassend kann man feststellen, dass durch die Änderungen im Revisionsentwurf keine neuen Abweichungen im Vergleich zu Tabelle 1 hinzugekommen sind.

6.3 Vergleich zwischen prEN 50126-x(2012) und Revisions-Entwurf CSM VO

Thema	Abweichungen zu „alter" EN50126	Aussage bzgl. prEN50126-x(2012) [prEN]
Vorschlagender	Die CENELEC-Normen kennen den Begriff nicht.	Diese Rolle wird in der Regel durch den Betreiber wahrgenommen. Falls der Hersteller als Vorschlagender auftriitt, dann sollte dies im Prozess berücksichtigt werden.
Signifikanzprüfung	Kategorisierung der geplanten Änderung Prüfung auf Sicherheitsrelevanz Prüfung der Signifikanz	Nicht relevant, wie in **Fehler! Verweisquelle konnte nicht gefunden werden.** aufgezeigt
Systemdefinition	Auflistung vorhandener systeminterner Sicherheitsmaßnahmen Umfang des Verfahrens festlegen (Systemannahmen und –grenzen)	Systemannahmen und –grenzen sowie deren Schnittstellenbeschreibungen werden in prEN gefordert Die Auflistung systeminterner Sicherheitsmaßnahmen wird im Safety Case verlangt.
Risikoeinschätzung	Prüfung der Anteilseinhaltung und Zulässigkeit der Gefährdungen nach dessen Risikohöhen (akzeptabel oder nicht)	In prEN wird für jeder Gefährdung entweder eine quantitative Vorgabe (THR) oder eine anderweitige Vorgabe, auch qualitativ, ermittelt und deren Zulässigkeit ermittelt.
Risikobewertung	Festlegung und Anwendung eines Risikoakzeptanzgrundsatzes für jede Gefährdung Definition von Risikoakzeptanzkriterien	In prEN werden die drei in der CSM VO stipulierten Risikoakzeptanzkriterien aufgeführt.
Gefährdungsmanagement (Gefährdungsprotokoll)	Angabe des beteiligten Akteurs, der für Gefährdung verantwortlich ist Nachweis und Herkunft des mit jeder Gefährdung verbundenen Risikos (akzeptabel oder nicht) Angabe und Herkunft des gewählten Risikoakzeptanzgrundsatzes und deren bestimmten Kriterium	Die Grundsätze des Safetymanagements, der Risikoanalyse sowie der Hazard Controlphase der prEN
Gefährdungsmanagement (Schnittstellenprotokoll)	Erstellung eines Schnittstellenprotokolls (wenn erforderlich) mit folgenden Kriterien: o Definition von Begriffen und Meldungen o Festlegung des Verantwortlichen für Dokumentation	Die Systemdefinition inkl. der dortigen Schnittstellendefinitionen, der Nachweis des Safetymanagements sowie die Erweiterung um qualitative Ansätze erfüllen die Vorgaben der CSM VO. Zusätzlich werden die Ver-

	o Angaben zu allen Systemannahmen o Angaben zur Gefährdung und deren Risiken o Angaben zu den ermittelten Sicherheitsmaßnahmen durch die verschiedenen Grundsätze o Angaben zu den vorhandenen Verwendungsbeschränkungen o eigenen Erfahrungen beim Versuch der Risikokontrolle	wendungsbeschränkungen sowie Sicherheitserprobungen im SafetyCase geplant und festgeschrieben.
Nachweis der Erfüllung der Sicherheitsanforderungen		
Unabhängige Bewertung	Benennung einer Bewertungsstelle Bewertung der Vergleiche und Prüfungen sind in einem Sicherheitsbewertungsbericht zu dokumentieren	Das Gutachten nach prEN erfüllt diese Anforderungen.

Tabelle 6 - Vergleich prEN50126-x mit CSM VO

Änderung der DV36 gegenüber CSM-VO (352/2009)	Aussage bzgl. prEN50126-x(2012) [prEN]
Erweiterter Scope: Im Scope der 352/2009 ist Pkt. 3 (Ausnahmen für Metros, Trams etc.) gestrichen. D.h. die Verordnung ist dann auch für diese Art von Bahnen gültig.	Diese Arten von Bahnen waren, sind und werden Teil der prEN sein.
Akkreditierung/Recognition: Aufnahme eigener Regelungen für Stellen, die die Eignung von Bewertungsstellen (im Sinne der CSM-VO) feststellen sollen. Alternativ zur Akkreditierung wird auch die Option der Recognition einer Bewertungsstelle behandelt.	Es bleibt zu klären, ob der Safety Case von den Bewertungsstellen angenommen werden.
Präzisierung der Bedingungen, dass ein code of practice als relevant zur Gefährdungsabdeckung angesehen werden kann: "Successful application of a code of practice for similar cases to manage changes and control effectively the identified hazards of a system in the sense of this Regulation is sufficient for it to be considered as relevant"	Es ist zu bewerten, ob die prEN eventuelle Verschärfungen der Anforderungen an einen code of practice übernehmen soll.

Tabelle 7 - Deltaanalyse zu Revisionsentwurf CSM VO

6.4 Referenzen

EN 50 126 DIN EN 50 126: Spezifikation und Nachweis der Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit, Sicherheit (RAMS). 2000 - 03

CSM VO 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, Amtsblatt der Europäischen Union, L 108/4, 29.4.2009

CSM GUI ERA: Leitlinie zur Anwendung der Verordnung der Kommission über die Festle-

	gung einer Gemeinsamen Sicherheitsmethode für die Evaluierung und Bewertung von Risiken gemäß Artikel 6 Absatz 3 Buchstabe a der Eisenbahnsicherheitsrichtlinie, ERA/GUI/01-2008/SAF
CSM EX	ERA: Sammlung von Beispielen für Risikobewertungen und möglicher Werkzeuge zur Unterstützung der CSM-Verordnung, ERA/GUI/02-2008/SAF
DV 36	Revisionsentwurf vom 6.11.2012, Version EN01, RISC65
Heinig	Heinig, Th.: Vorschlag für ein Verfahren zur Umsetzung der CSM-Verordnung in einem Industrieunternehmen, Diplomarbeit, TU Dresden, 2012

6.5 Abkürzungen

Abk.	Langform / Erläuterung
CSM	Common Safety Method
LST	Leit- und Sicherungstechnik