Neue Generation Signaltechnik

Sektorweite Initiative zur Sicherung der Zukunftsfähigkeit der Leit- und Sicherungstechnik

Ergebnisbericht AP2200
Dokumentationsumfang bei der Zulassung gemäß CENELEC

Unterarbeitspaket 2200.1: Beispielhafte Dokumentenlisten ('Best Practice')

12.08.2013

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
06.06.2013	Mathias Wagner (Bombardier)	0.1	Erster Entwurf
04.07.2013	Mathias Wagner (Bombardier)	0.2	Update nach internem AG3-Review
08.07.2013	Mathias Wagner (Bombardier)	0.3	Update nach internem AG3-Review
16.07.2013	Mathias Wagner (Bombardier)	0.4	Update des Kapitels 4 Skalierbarkeit nach internem AG3-Review
18.07.2013	Mathias Wagner (Bombardier)	0.5	Update nach internem AG3-Review
07.08.2013	Beck (DB AG) Czepa (Thales) Griebel (Siemens) Möller-Neustock (Funkwerk AG, TCC) Pietz (Pintsch Bamag) Dr. Priebe (S&B) Schwencke (DLR) Wagner (Bombardier)	0.6	Erweiterung um SIL 0 und SIL 2
12.08.2013	Beck (DB AG) Czepa (Thales) Griebel (Siemens) Möller-Neustock (Funkwerk AG, TCC) Pietz (Pintsch Bamag) Dr. Priebe (S&B) Schwencke (DLR) Wagner (Bombardier)	1.0	Veröffentlicht nach finalem AG3-Review

Inhaltsverzeichnis

1 Einleitung

Die CENELEC-Normen EN 50126, EN 50128 und EN 50129 beschreiben die Entwicklung von Bahnanwendungen. Sie lassen dem Anwender einen großen Interpretations- und Handlungsspielraum. So kann er auch relativ frei entscheiden, welche Maßnahmen er zur Entwicklung eines sicheren Systems anwenden möchte. Umfassende Tabellen in den Anhängen der Normen EN 50128 und EN 50129 geben eine Auswahl von Maßnahmen, die anzuwenden sind. Oftmals soll der Anwender eine „geeignete" Kombination von Maßnahmen auswählen, wobei nur eingeschränkt spezifiziert ist, unter welchen Umständen eine Auswahl geeignet ist.

Ziel der AG ist eine Abstimmung zwischen allen Projektpartnern über eine einheitliche CENELEC-konforme Dokumentenliste bei der Einreichung zur Zulassung von Projektvorhaben. Auf Basis dieser einheitlichen Liste sollen Best Practice-Beispiele erarbeitet und Interpretationsspielräume der Normen identifiziert und reduziert werden.

Zur Erfüllung dieses Arbeitspaketes 2200 wurde die Aufgabenbeschreibung in die folgenden Unterarbeitspakete strukturiert:

0. Erstellung einer abgestimmten generische CENELEC-Dokumentenliste
1. Erstellung von beispielhaften Dokumentenlisten ('Best Practice') für spezifische Anwendungsfälle
   a) für SIL 4
   b) für SIL 2
   c) für SIL 0/no-SIL
2. ~~Dokumentenliste und der Maßnahmenkatalog ('Best Practice') werden als Anhang zum Sektorhandbuch Infrastruktur aufbereitet.~~
3. Enge Abstimmung mit der AG2 (CSM-VO)
4. ~~Nach der Abstimmung mit dem Betreiber soll die seit 11.2012 vorliegende prEn 50126 in die Dokumentenliste eingearbeitet werden~~

Das Unterarbeitspaket 2200.2 wurde ausgesetzt, da die NeGSt-Arbeitsgruppe 4 die Bearbeitung des „Sektorhandbuches Infrastruktur" im Mai 2013 vorerst ausgesetzt hat.

Das Unterarbeitspaket 2200.3 wurde bereits im Teilbericht „Vorarbeiten und Unterarbeitspaket 2200.3" (NeGSt_Teilbericht_2200.0u3_1.0.pdf) abschließend bearbeitet.

Das Unterarbeitspaket 2200.4 wurde ausgesetzt, da es im Mai 2013 mit dem vorliegenden Zwischenstand der prEN 50126 nicht zielführend scheint, die Dokumentenliste daraufhin anzupassen.

Als Ersatz für die Unterarbeitspakete 2200.2 und 2200.4 wurde das optionale Unterarbeitspaket 2200.1 Teil b „Einarbeitung von SIL 2 in die Best Practices" und 2200.1 Teil c „Einarbeitung von SIL 0 in die Best Practices" in die Liste der Unterarbeitspakete aufgenommen.

Das vorliegende Dokument zeigt die Ergebnisse des Unterarbeitspaketes 2200.1 Teil a bis Teil c „Erstellung von beispielhaften Dokumentenlisten ('Best Practice') für vier spezifische Anwendungsfälle für SIL 4 und SIL 2 und SIL 0".

2 Definitionen

2.1 Spaltentitel

Folgende Spaltentitel werden in Tabelle 4 verwendet.

Spalte im Arbeitsblatt "Dokumente"	**Erläuterung**	**Mögliche Einträge**
CENELEC-Phase Ersterstellung	Phase des CENELEC-Prozesses nach EN 50126, in der das Dokument angelegt wird	Zahl zwischen 1 und 14, ggf. auch mehrere mögliche Phasen
Dokumentenkürzel	Kürzel für den (englischen) Dokumentennamen	<Kürzel>, i.d.R. beginnend mit "Pr...", "Sy...", "Sw..." oder "Hw..." für Projekt-, System-, Software- und Hardware-Dokumente
Dokumentenname	vollständiger Name des Dokuments gemäß aktuellster CENELEC-Norm	<Name>
Kommentar	Gibt es Besonderheiten zum Dokument, die neben den vordefinierten Spalten wichtig zum Verständnis des Dokuments sind?	<freier Text>
Best Practice x: Anwendungsfall	Definition, ob das Dokument für den jeweilige Anwendungsfall • „+" erzeugt/überarbeitet • „-" nicht erzeugt/nicht überarbeitet • „+/-" eventuell, wird standardmäßig erzeugt/überarbeitet • „-/+"eventuell, wird standardmäßig nicht erzeugt/nicht überarbeitet werden soll	„+", „-", „+/-", „-/+"
Erläuterung BP x	Erläuterungen zu dem jeweiligen Dokument für diesen Anwendungsfall	

Tabelle 1: Erklärung der Spaltentitel

2.2 Abkürzungen

Folgende Abkürzungen werden in diesem Dokument verwendet.

Abkürzung	Beschreibung
AG	Arbeitsgruppe
AN	Auftragnehmer
AP	Arbeitspaket
BP	Best Practice
CENELEC	Europäisches Komitee für elektrotechnische Normung
CSM-VO	Verordnung (EG) Nr. 352/2009 über die Festlegung einer gemeinsamen Sicherheits-methode für die Evaluierung und Bewertung von Risiken
DIN	Deutsche Industrienorm
EASA	Europäische Agentur für Flugsicherheit
EBA	Eisenbahn-Bundesamt
EN	Europäische Norm
FMEA	Ausfalleffektanalyse
HW	Hardware
ISO	Internationale Organisation für Normung
NeGSt	Neue Generation Signaltechnik
NTZ	Neue Typzulassung
prEN	Vorläufige europäische Norm
PT1	Planteil 1
PT2	Planteil 2
QS	Qualitätssicherung
RAMS	Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit, Sicherheit" (im englischen: Relia-bility, Availability, Maintainability, Safety)
Sb 3	Sachbereich 3 (des Eisenbahn-Bundesamtes)
SIL	Sicherheitsanforderungsstufe
SW	Software
THR	Tolerierbare Gefährdungsraten

Tabelle 2: Verwendete Abkürzungen

3 Vorgaben

Auf Basis der Dokumentenliste aus dem Teilbericht „Vorarbeiten und Unterarbeitspaket 2200.3" (NeGSt_Teilbericht_2200.0u3_1.0.pdf) wurden Ausprägungen für die folgenden spezifischen Anwendungsfälle erstellt (siehe Kapitel 6):

- Best Practice 1: SW-Fehlerbehebung
- Best Practice 2: Systemerweiterung
- Best Practice 3: Weiterentwicklung einer HW-Steckkarte (als HW-Komponente)
- Best Practice 4: Neue spezifische Applikation

Die spezifischen Anwendungsfälle sind dabei wie folgt definiert:

Best Practice Beispiel	**Definition**
Best Practice 1: SW-Fehlerbehebung	Der Anwendungsfall ‚SW-Fehlerbehebung' setzt voraus, dass ein Release bereits zugelassen ist. Es wird angenommen, dass die SyCIA ergeben hat, dass in Phase 4 bis inkl. 6.1 keine Änderungen vorzunehmen sind. Pläne (Sicherheits-, Qualitäts-, Verifikations-, Validationplan) sollten grundsätzlich so gestaltet sein, dass sie bei einer SW-Fehlerbehebung nicht geändert werden müssen.
Best Practice 2: Systemerweiterung	Der Anwendungsfall ‚Systemerweiterung' setzt voraus, dass ein Release bereits zugelassen ist. Es wird angenommen, dass Änderungen an Hard- und Software nötig sind. Die Frage der Kompatibilität zu bestehenden Systemen ist in der SyCIA zu klären. Ggf. müssen Anforderungen zur Kompatibilität aufgenommen werden. Es wird nicht davon ausgegangen, dass alle im Betrieb befindlichen Systeme rückwirkend aktualisiert werden müssen.
Best Practice 3: Weiterentwicklung einer HW-Steckkarte (als HW-Kompon.)	Der Anwendungsfall ‚HW-Weiterentwicklung' setzt voraus, dass ein Release bereits zugelassen ist. Es wird eine kompatible Änderung einer Komponente durchgeführt. Kompatible Änderung bedeutet, dass die Schnittstellen und RAMS-Anforderungen gleich bleiben und somit keine Softwareänderungen nötig sind. Die Änderung ist nötig aufgrund einer Bauteilabkündigung oder -optimierung, nicht aufgrund von entdeckten Fehlern.
Best Practice 4: Neue spezifische Applikation	Der Anwendungsfall ‚Neue spezifische Applikation' setzt eine gleichbleibende generische Applikation/ein gleichbleibendes generisches Produkt voraus. Best Practice 4 trifft ebenso auf Änderungen an spezifischen Applikationen zu.

Tabelle 3: Definitionen der spezifischen Anwendungsfälle

Die im Kapitel 6 dargestellte Dokumentenliste basiert auf den folgenden Versionen der CENELEC-Normen:

- DIN EN 50126:2000
- DIN EN 50128:2001
- DIN EN 50128:2012
- DIN EN 50129:2003

4 Skalierbarkeit

Das zu betrachtende System kann aus einer mehr oder weniger komplexen Struktur von System/Subsystemen/HW-Komponenten/SW-Komponenten bestehen (HW- und SW-Komponenten als kleinster autarker Bestandteil der Hard- und Software, der in Bezug auf Architektur und Entwurf über klar definierte Schnittstellen verfügt).

Dies trifft in unterschiedlicher Ausprägung und Komplexität für die Kategorien Generisches Produkt, Generische Applikation und Spezifische Applikation zu, welche wiederum aufeinander aufbauen.

Für jede Ebene in einer solchen Struktur kann die generische CENELEC-Dokumentenliste aus dem Teilbericht „Vorarbeiten und Unterarbeitspaket 2200.3" (NeGSt_Teilbericht_2200.0u3_1.0.pdf) grundsätzlich angewendet werden. Pro Ebene ist dabei eine Teilmenge der Dokumente der generischen Dokumentenliste zu erstellen.

Beispielsweise sind am Anfang des Entwicklungsprozesses auf System-Level wahrscheinlich alle Dokumente der Phasen 1-5 zu erstellen. Für die untergeordneten Subsysteme werden dann jeweils die Dokumente der Phasen 4 und 5 erneut und die Dokumente für die folgenden Phasen erstmals erstellt. Ähnlich für die späteren Phasen im V-Modell: Die Dokumente für z.B. Integration, Test, Validation und Assessment werden jeweils für die Subsysteme und erneut für den Systemlevel erstellt. Die Dokumente für die folgenden Phasen wie Abnahme und Betrieb und Instandhaltung werden nur für den Systemlevel erstellt.

Es ist essentiell, dass diese Strukturen pro zu betrachtendem System im Detail analysiert, geplant und dokumentiert werden.

Die im Kapitel 6 dargestellten spezifischen Anwendungsfälle stellen ausgewählte Beispiele für eine solche Analyse dar.

5 Safety Integrity Levels

5.1 SIL 4

Der hier vorliegenden Dokumentenliste (siehe Tabelle 4) wurde der Safety Integrity Level (SIL) 4 zugrunde gelegt.

5.2 SIL 2

Die Betrachtung des Safety Integrity Levels 2 zeigte, dass sich bezüglich der Anzahl und der Titel der Dokumente gegenüber einer SIL 4 Entwicklung keine Änderungen ergeben, siehe DIN EN 50128 Tabelle A.1. Unterschiede zwischen SIL 4 und SIL 2 Entwicklungen ergeben sich durch die verschiedenen Techniken und Maßnahmen, wie z. B. in der DIN EN 50129 Anhang E dargestellt. Daraus ergibt sich ein unterschiedlicher Umfang des Inhalts der Dokumente wie in den CENELEC-Normen ausführlich dargestellt.

5.3 SIL 0

Den CENELEC-Normen konnte kein konkretes Beispiel entnommen werden, was ein repräsentatives SIL 0-Produkt sein könnte.

Keines der beteiligten Unternehmen hat bisher ein Projekt nach SIL 0 aufgesetzt:

1. Offensichtlich nicht sicherheitsrelevante Entwicklungsgegenstände wie z.B. Fahrgastinformationssysteme oder Infotainment-Applikationen werden nicht nach CENELEC entwickelt.

   Dies erfolgt unter Berücksichtigung der Regeln in DIN EN 50129, die zur Thematik die folgenden wesentlichen Aussagen enthält:

   > *» Die Anwendung dieses Sicherheitsmanagementprozesses ist verbindlich für die Sicherheitsanforderungsstufen 1 bis 4 (siehe Anhang A zur Erläuterung der Sicherheitsanforderungsstufen). Jedoch sollten die Tiefe der Darlegungen und der Umfang der begleitenden Dokumentation der Sicherheitsanforderungsstufe des/der betrachteten Systems/Teilsystems/Einrichtung angemessen sein.* ***Die Anforderungen für die Sicherheitsanforderungsstufe 0 (nicht sicherheitsrelevant) liegen außerhalb des Anwendungsbereiches dieser Sicherheitsnorm.***
   >
   > *In allen Fällen sind Gefährdungsanalyse und Risikobewertungsprozesse, wie in EN 50126 definiert, notwendig, um den benötigten Grad an Sicherheitsintegrität jeder einzelnen Situation zu identifizieren. Dies schließt jene Fälle mit ein, wo die Analyse und Bewertung offenbaren, dass die Sicherheitsanforderungsstufe 0 zugeordnet werden darf. Wenn man zu dieser Schlussfolgerung gelangt ist (d. h., die Situation ist nicht sicherheitsrelevant) und feststeht, dass die Stufe 0 bestehen bleibt,* ***dann endet die Anwendbarkeit dieser Sicherheitsnorm.*** *«*

2. Sicherheitsrelevante Systeme, für die quantitative Risikoanalysen (Risikobewertungen) durchgeführt wurden und für die somit THR ermittelt wurden, sind bisher immer in höheren SI-Level angesiedelt.

Die Qualitätssicherung für jeglichen Entwicklungsprozess ist durch die ISO 9000 ff. Normen gegeben, hierfür bedarf es keiner Einhaltung eines besonderen SIL 0-Prozesses. Dies wäre zudem eine unzulässige Vermischung von Qualitätssicherung und Einhaltung eines Safety Integrity Levels.

Darüber hinaus erscheint es weder notwendig noch sinnvoll, für die Entwicklung derartiger Systeme Anforderungen festzulegen, die über gängige Industriestandards und -normen hinausgehen.

Zum Vergleich mit der Praxis in anderen Industriezweigen kann hier auf die Luftfahrt verwiesen werden. In dem von der EASA herausgegebenen Standard CS-25 [1]), der für die Zertifizierung großer

[1] EASA (European Aviation Safety Agency): Certification Specifications for Large Aeroplanes, Amendment 9 vom 05.08.2010

Passagierflugzeuge Regelungen bezüglich Sicherheitsanforderungen und deren Nachweis enthält, findet sich bereits für die niedrigste von 4 Sicherheitsanforderungsstufen folgende Aussage:

> *» A numerical probability range is provided here as a reference. The applicant is not required to perform a quantitative analysis, nor substantiate by such an analysis, that this numerical criteria has been met for Minor Failure Conditions. Current transport category aeroplane products are regarded as* ***meeting this standard simply by using current commonly-accepted industry practice.*** *«*

Aus den genannten Gründen hat die AG beschlossen, dass es (zumindest zurzeit) keinen Sinn ergibt, eine Ergänzung der Dokumentenliste für SIL 0 durchzuführen bzw. Best Practices zu beschreiben.

6 Dokumentenliste

Die folgende Dokumentenliste listet die Dokumente der generischen CENELEC-Dokumentenliste aus dem Teilbericht „Vorarbeiten und Unterarbeitspaket 2200.3" (NeGSt_Teilbericht_2200.0u3_1.0.pdf).

Für die vier Anwendungsfälle wurden die Spalten Best Practice 1 – 4 mit jeweils einer zusätzlichen Erläuterungsspalte eingefügt. In diesen wird angegeben, ob das Dokument für den jeweiligen Anwendungsfall erzeugt/überarbeitet werden soll (siehe auch Tabelle 1: Erklärung der Spaltentitel).

CENELEC-Phase Erststellung	Dokumentenkürzel	Dokumentenname	Kommentar	Best Practice 1: SW-Fehlerbehebung	Erläuterungen BP1	Best Practice 2: Systemerweiterung	Erläuterungen BP2	BP 3: Weiterentwicklung einer HW-Steckkarte	Erläuterungen BP3	Best Practice 4: neue spezifische Applikation	Erläuterungen BP4
1/2 Konzept und Systemdefinition											
	SyCR	Kundenanforderung	optionales Dokument; wird u.U. bis inkl. Phase 4 weiter verfeinert	-		+/-	Falls sich Anforderungen des Kunden ändern.	-		-	
1-2	SyDef	Systemdefinition		-		+/-	Falls sich Anforderungen des Kunden ändern.	-		-	
1-2	SyCIA	Änderungsauswirkungsanalyse	Dokument ist nicht von CENELEC gefordert, wird aber als sinnvoll erachtet. Es ist nur bei Änderungen zu erstellen. Ziel ist zu entscheiden, welche Teile des Prozesses betroffen sind und welche Dokumente und Systembestandteile geändert werden müssen	+	Wenn nicht alle System- und Modultest wiederholt durchgeführt werden sollen, muss dies hier analysiert und begründet werden	+	Die Frage der Kompatibilität zu bestehenden Systemen ist in der SyCIA zu klären. Ggf. müssen Anforderungen zur Kompatibilität aufgenommen werden.	+	Hier ist festzustellen, dass der Umfang der Änderung nur eine Hardwarekomponente (die Steckkarte) betrifft. Die Frage der Kompatibilität zu bestehenden Systemen ist in der SyCIA zu klären.	-	
1	SyDP	Entwicklungsplan	Herstellerspezifisches Projektkonzept; klärt u.a. den Zusammenhang Zulassungsstrategie - Systemarchitektur - Entwicklungsmodelle (V-Modell)	-		-		-		-	
1	PrTL	Projekt-Zeitplan	Der Zeitplan sollte für generische Produkte, generische Applikationen und spezifische Applikationen erstellt werden.	+	Zeit- und Ressourcenplanung für das Fehlerbehebungsprojekt; soll gemäß den Vorgaben des SyMP erstellt werden	+	Zeit- und Ressourcenplanung für das Änderungsprojekt; soll gemäß den Vorgaben des SyMP erstellt werden	+	Zeit- und Ressourcenplanung für das Änderungsprojekt; soll gemäß den Vorgaben des SyMP erstellt werden	+	Zeit- und Ressourcenplanung für das Projekt/Änderungsprojekt; soll gemäß den Vorgaben des SyMP erstellt werden
1	PrDL	Dokument-Übersicht	Die Dokumentenübersicht sollte für generische Produkte, generische Applikationen und spezifische Applikationen erstellt werden.	+		+		+		+	
1	PrG	Glossar		-		-		-		-	
1-2	SySP	Sicherheitsplan	Z SySMR wird als sinnvoll erachtet (da dort die Prüfungsergebnisse zum SySP stehen)	-		-		-		-	

2-10	SySMR	Sicherheitsmanagementbericht	Z SySP wird als sinnvoll erachtet (als zu überprüfendes Dokument), 4-Augen-Prinzip im Falle eines externen Gutachters	+	Ergänzung	+	Ergänzung	+	Ergänzung	-
1-2	SyQMP	Qualitätssicherungsplan	muss nach aktueller Praxis dem Gutachter vorgelegt werden	-		-		-		-
2-10	SyQMR	Qualitätsmanagementbericht	Z SyQP wird als sinnvoll erachtet (als zu überprüfendes Dokument); enthält Ergebnisse zur Anforderungsverfolgbarkeit - kann eigenständiges Dokument (Anf.verfolgbarkeitsmatrix) oder Teil des Berichtes sein, s. diverse Stellen in der DIN EN 50128:2012. 4-Augen-Prinzip im Falle eines externen Gutachters	+	Ergänzung	+	Ergänzung	+	Ergänzung	-
2	SyPVR	Planungsverifikationsbericht	Verifiziert alle Pläne außer dem Validierungsplan. Heißt lt. DIN EN 50128:2012 (Software-) Qualitätssicherungsverifikationsbericht	+	Ergänzung des alten Berichts oder komplett neuer Bericht	+	Ergänzung des alten Berichts oder komplett neuer Bericht	+	Ergänzung des alten Berichts oder komplett neuer Bericht	-
1-2	SyCMP	Konfigurationsmanagementplan		-		-		-		-
1-2	SyVeP	Verifikationsplan	Enthält den Software-Verifikationsplan. Die Aufgaben sind in der 50126 definiert, nicht das Dokument. Im aktuellen Entwurfsstand der neuen 50126-1 werden Verifizierungs- und Validierungsaufgaben für jede Phase gesondert ausgewiesen. Es ist zu prüfen, ob die ISO 900x genauere Angaben zu geforderten Dokumenten macht	-		-		-		-
1-2	SyVaP	Validierungsplan	Die Aufgaben sind in der 50126 definiert, nicht das Dokument. Im aktuellen Entwurfsstand der neuen 50126-1 werden Verifizierungs- und Validierungsaufgaben für jede Phase gesondert ausgewiesen. Es ist zu prüfen, ob die ISO 900x genauere Angaben zu geforderten Dokumenten macht	-		-		-		-
1-2	SyTP	System-Testplan		-		+/-	Hängt von Art und Umfang der Änderung ab.	-		-
1-2	SyAP	Begutachtungsplan	auch als "Prüfhandbuch" bezeichnet; in der Regel fordert das EBA die Vorlage des SyAP; ist bislang nur für SW verpflichtend. Definiert die Kriterien, Arbeitsweise und den Arbeitsumfang der Prüfleitstelle/des Gutachters	-		-		-		-
3 Risikoanalyse										
3	SyHA	Gefährdungs- und Risikoanalyse	In Zukunft gemäß NTZ keine Prüfung durch EBA mehr? Unklar, ob die Revision der 50129 (neue 50126) weiterhin Prüfung durch Aufsichtsbehörde fordert	-		+		-		-

3	SyHL	Gefahrenprotokoll	gängiger Begriff ist "Gefährdungslog-buch". 4A-Prüfung im Falle eines exter-nen Gutachters	+	Fehler muss ergänzt werden, sofern dadurch eine neue Gefährdung verursacht wird	+		-	Da sich aufgrund der Definition des BP keine Änderung aufgrund von Fehlern durchgeführt wird.	-
4 Systemanforderungen										
4	SyRS	System-Anforderungsspezifikation	Bei der Erstellung durch den AN erfolgt auch die Prüfung durch den AN.	-		+		-		-
4	SySRS	System-Sicherheitsanforderungsspezi-fikation	Bei der Erstellung durch den AN erfolgt auch die Prüfung durch den AN. Sicher-heitskonzept gemäß Mü 8004 kann in diesem Dokument aufgehen. Prüfungen finden statt bei Ersteller AN	-		+		-		-
4	SyTS	System-Testspezifikation	enthält neben der Abdeckung der Sys-temanforderungen auch noch zusätzliche Test zur Gesamtsystemfunktionalität	-	Test-Subset wird ggf. in Änderungsauswir-kungsanalyse ausge-wählt	+		-		-
4	SyRVR	System-Anforderungsverifikationsbe-richt	Falls obige Dokumente im Rahmen der Entwicklung (von AN) erstellt werden, müssen sie auch verifiziert werden; wenn SwRS und HwRS mit SyRS zusammen-gelegt, dann auch SwRVR und HwRVR mit SyRVR	-		+		-		-
5 Systementwurf										
5	SyAS	System-Architekturspezifikation	in diesem Dokument können ggf. Sub-systeme definiert werden, die entweder in den SW-/HW-Architekturdokumenten beschrieben werden (6.1.2/6.2.2) oder für die wiederum die System-Dokumente angefertigt werden (neuer Prozess)	-		+/-	Bei Änderungen von Schnittstellen (inner-halb des Systems und nach außen).	-		-
5	SyDS	System-Entwurfsspezifikation		-		+		-		-
5	SyADVR	System-Architektur- und Ent-wurfsverifikationsbericht		-		+		-		-
5-6	SwHwITP	SW/HW-Integrationstestplan		-		+		-		-
6 Entwicklung/Konstruktion und Implementierung										
6.1 Hardware										
6.1.1 HW-Anforderungen										
6	HwRS	HW-Anforderungsspezifikation		-		+		-		-
6.1.2 HW-Entwurf										
6	HwDS	HW-Entwurfsspezifikation	kann entfallen, wenn nur eine Kompo-nente im System vorhanden	-		+		-		-
6	HwAS	HW-Architekturspezifikation	kann entfallen, wenn nur eine Kompo-nente im System vorhanden	-		+		-		-
6	HwIS	HW-Schnittstellenspezifikation	kann entfallen, wenn nur eine Kompo-nente im System vorhanden	-		+		-		-

6.1.3 HW-Komponentenentwurf										
6	HwCDS	HW-Komponentenentwurfsspezifikation		-		+		+		-
6	HwCFMEA	HW-Komponenten-FMEA		-		+		+		-
6	HwCRC	HW-Komponenten-Zuverlässigkeitsberechnungen		-		+		+		-
6.1.4 HW-Fertigungsunterlagen										
6	HwPD	HW-Fertigungsunterlagen	Layout, Stücklisten, Grundschaltungen, etc.	-		+		+		-
6.1.5 HW-Komponententest										
6	HwCTS	HW-Komponententestspezifikation		-		+		+		-
6	HwCTR	HW-Komponententestbericht		-		+		+		-
6.1.6 HW Verifikationsbericht										
6	HwVR	HW-Verifikationsbericht	Verifikationsbericht fasst alle Verifikationsschritte für die HW zusammen.	-		+		+		-
6.2 Software										
6.2.1 SW-Anforderungen										
6	SwRS	SW-Anforderungsspezifikation		+/-	Änderung nur, falls Fehler die SW-Anforderungen betrifft	+		-		-
6	SwOTS	SW-Gesamttestspezifikation	früher (50128:2003): SW-Anforderungstestspezifikation	+/-	Änderung nur, falls Fehler die SW-Anforderungen betrifft	+		-		-
6	SwRVR	SW-Anforderungsverifikationsbericht		+/-	Änderung nur, falls Fehler die SW-Anforderungen betrifft	+		-		-
6.2.2 SW-Entwurf										
6	SwAS	SW-Architekturspezifikation	s. Kommentar SyAS	-		+/-	Bei Änderungen von Schnittstellen (innerhalb des Systems und nach außen).	-		-
6	SwDS	SW-Entwurfsspezifikation	s. Kommentar SyDS	+/-	Änderung nur, falls Fehler den SW-Entwurf betrifft	+		-		-
6	SwIS	SW-Schnittstellenspezifikation	s. Kommentar SyAS/SyDS	+/-	Änderung nur, falls Fehler die SW-Schnittstellen betrifft	+		-		-

6	SwADVR	SW-Architektur- und Entwurfsverifikationsbericht		+/-	s. Kommentare SwDS und SwIS	+	-	-	
6	SwITP	SW-Integrationstestplan		-		+	-	-	
6.2.3 SW-Komponentenentwurf									
6	SwCDS	SW-Komponentenentwurfsspezifikation	Früher (50128:2003) "Modul" statt "Komponente"	+/-	Änderung nur, falls Fehler die SwCDS betrifft	+	-	-	
6	SwCDVR	SW-Komponentenentwurfsverifikationsbericht	Früher (50128:2003) "Modul" statt "Komponente"	+/-	s. Kommentar SwCDS	+	-	-	
6.2.4 SW-Implementierung									
6	SwSC	SW-Quellcode und Hilfsdokumentation	Früher "Zusatzdokumentation" statt "Hilfsdokumentation"; zweite Prüfung gemäß DIN EN 50128:2012 Tabelle C.1 wird nicht immer als sinnvoll erachtet	+		+	-	-	
6	SwSCVR	SW-Quellcodeverifikationsbericht		+		+	-	-	
6.2.5 SW-Komponententest									
6	SwCTS	SW-Komponententestspezifikation	Norm alt: Modul --> Norm neu: Komponente	+		+	-	-	
6	SwCTR	SW-Komponententestbericht	Der zugehörige Verifikationsbericht ist der SwCDVR	+		+	-	-	
6.3 Integration									
6	SwITS	SW-Integrationstestspezifikation		+/-	Änderung nur, falls Fehler die SW-Schnittstellen betrifft	+	Prüfung existierender Komponenten nur falls die SyCIA die Notwendigkeit ergibt.	-	-
6	SwHwITS	SW/HW-Integrationstestspezifikation		+/-	Änderung nur, falls Fehler die SW/HW-Schnittstellen betrifft	+	Prüfung existierender Komponenten nur falls die SyCIA die Notwendigkeit ergibt.	-	-
6	SwITR	SW-Integrationstestbericht		+/-	Je nach Ergebnis der Änderungsauswirkungsanalyse	+	Prüfung existierender Komponenten nur falls die SyCIA die Notwendigkeit ergibt.	+	-
6	SwHwITR	SW/HW-Integrationstestbericht		+/-	Je nach Ergebnis der Änderungsauswirkungsanalyse	+	Prüfung existierender Komponenten nur falls die SyCIA die Notwendigkeit ergibt.	+	-

6	SyAPP	Anwendungs-Generierungsplan	Dieser generische Plan beschreibt die Umsetzung in der spezifischen Anwendung (siehe DIN EN 50128:2012, Pkt. 8.4.1.2). Er entfällt lt. EBA-Tabellen bei generischer Software (nur bei anwend.-spezifisch konfigurierten Systemen); EBA-Vorlage zur Bauaufsichtl. Freigabe/Abnahme Sb 3.	-		-	-	-	
6	SyIVR	Integrationsverifikationsbericht		+/-	Änderung nur, falls Fehler Dokumente in der Integrationsphase betrifft	+	+	-	
7 Fertigung									
7	SyARS	Anwendungs-Anforderungsspezifikation		-		-	-	+	entspricht der geprüften PT1 und PT2
7	SyATS	Anwendungs-Testspezifikation		-		-	-	+	
7	SyAAD	Anwendungsarchitektur und -entwurf	In diesem Dokument geht es um das Kombinieren/Konfigurieren der generischen Anwendung zum Erhalt der spezifischen Anwendung (Modulwahl).	-		-	-	-/+	entspricht im Normalfall der geprüften PT2; nur im Fall besonderer Kombinationen explizit zu erstellen.
7	SySCADA	Quellcode der Anwendungsdaten-/Algorithmen	Z. B. Konfigurationsdateien. Zweite Prüfung wird durch PT2-Prüfung abgedeckt. Mit "Prüfung durch EBA" ist hier das örtliche EBA gemeint.	-		+	-	+	
7	SyAPVR	Anwendungs-Generierungsverifikationsbericht		-		+	-	+	
7	SyATR	Anwendungs-Testbericht	entfällt lt. EBA-Tabellen bei generischer Software (nur bei anwend.-spezifisch konfigurierten Systemen); EBA-Vorlage zur Bauaufsichtl. Freigabe/Abnahme Sb 3	+	Je nach Ergebnis der Auswirkungsanalyse sind für zu aktualisierende Anlagen die relevanten Teile der SyATS Regressionstests durchzuführen. Für neue Anlagen sind alle Teile der SyATS zu testen.	+	-	+	
7	SyRDP	Freigabe- und Bereitstellungsplan	Kein explizites Dokument für den Entwicklungsprozess, wenn z.B. über QS- bzw. ISO 9001 abgedeckt	-		-	-	-	
7	SyADAVR	Anwendungsdaten-/Algorithmen-Verifikationsbericht		-		+	-	+	
7	SyDM	Bereitstellungshandbuch	Kein explizites Dokument für den Entwicklungsprozess, wenn z.B. über QS- bzw. ISO 9001 abgedeckt	-		-	+	-	
7	SyRNs	Freigabemitteilungen	Kein explizites Dokument für den Entwicklungsprozess, wenn z.B. über QS- bzw. ISO 9001 abgedeckt	+		+	+	+	
7	SyRN	Freigabemitteilung	Zusammenfassung der ausführlichen Freigabemitteilungen (Release Notes)	+		+	+	+	

7	SyDR	Bereitstellungsaufzeichnungen	Kein explizites Dokument für den Entwicklungsprozess, wenn z.B. über QS- bzw. ISO 9001 abgedeckt	+		+		+		+
7	SyDVR	Bereitstellungs-Verifikationsbericht	Kein explizites Dokument für den Entwicklungsprozess, wenn z.B. über QS- bzw. ISO 9001 abgedeckt	+		+		+		+
8 Installation/Montage										
8	SyPI	Projektierungsrichtlinie	Inhalte sehr firmenspezifisch: enthält Anleitung zur Projektierung der Anlage, z. B. Anzahl Busteilnehmer, Kabelvorgaben, Fahrstraßentabelle, …	-		+	Ergänzung. Enthält auch die Kompatibilitätsliste (vgl. SyCIA).	+		-
8	SyM	Bedienhandbuch		-		+		-		-
8	SyTI	Prüfanweisungen Hw/Sw		-		+	Ergänzung	+	mindestens Ergänzung eines Verweises auf die neue Steckkarte	-
8	SyII	Installationsanleitung		-		+	Ergänzung	+	mindestens Ergänzung eines Verweises auf die neue Steckkarte	-
9 Validierung										
9	SyTR	System-Testbericht		+	Je nach Ergebnis der Auswirkungsanalyse sind für zu aktualisierende Systembestandteile die relevanten Teile der SyTS Regressionstests durchzuführen.	+	Je nach Ergebnis der Auswirkungsanalyse sind für zu aktualisierende Systembestandteile die relevanten Teile der SyTS Regressionstests durchzuführen.	+	Je nach Ergebnis der Auswirkungsanalyse sind für zu aktualisierende Systembestandteile die relevanten Teile der SyTS Regressionstests durchzuführen.	-
9	SyVaR	System-Validationsbericht	beinhaltet alle Elemente: Software, Hardware, integriertes System und Tools und Betrachtung von Auflagen/Restfehler, In Zukunft gemäß NTZ keine Prüfung durch EBA mehr	+		+		+		-
9	TVaR	Werkzeuge-Validierungsbericht	Kann generisch für die firmenspezifische Toolkette erstellt werden. Enthält die Verweise auf die dortige Nachweisführung.	-		-		-		-
9	SyTSR	Technischer Sicherheitsbericht	In Zukunft gemäß NTZ keine Prüfung durch EBA mehr	+	Nur Anpassung der Referenzen; alternativ können Referenzen in der Freigabemitteilung enthalten sein.	+		+	mindestens Ergänzung eines Verweises auf die neue Steckkarte	-
9	SyRAMSD	RAMS-Nachweis	Manteldokument mit Referenzen auf alle RAMS-Dokumente	+	Nur Anpassung der Referenzen; alternativ können Referenzen in der Freigabemitteilung enthalten sein.	+		+	Nur Anpassung der Referenzen; alternativ können Referenzen in der Freigabemitteilung enthalten sein.	-

9	SySC	Sicherheitsnachweis	In Zukunft gemäß NTZ keine Prüfung durch EBA mehr. Vorbereitung ab Phase 6.	+	Nur Anpassung der Referenzen; alternativ können Referenzen in der Freigabemitteilung enthalten sein.	+		+	Nur Anpassung der Referenzen; alternativ können Referenzen in der Freigabemitteilung enthalten sein.	-	
9	SASC	Anwendungssicherheitsnachweis	SASC=Specific Application Safety Case. In Deutschland ist eine Verwendung nicht bekannt. Kann ggf. im Ausland erforderlich sein. Vorbereitungen laut alter 50126 ab Phase 6. An dieser Stelle wird nur die "Vorbereitung" des Dokumentes erwähnt; weitere Festlegungen fehlen jedoch.	-	Nur Anpassung der Referenzen; alternativ können Referenzen in der Freigabemitteilung enthalten sein.	-		-	Nur Anpassung der Referenzen; alternativ können Referenzen in der Freigabemitteilung enthalten sein.	-/+	
10 Abnahme											
10	SyAR	System-Gutachten	Hierunter sind auch Gutachten zu verstehen, die sich nur auf Software oder Hardware beziehen	+		+		+		+	Für die spezifische Applikation kein Gutachten im CENELEC-Sinne, sondern Abnahmeniederschrift
10	SySAR	Sicherheitsbewertungsbericht	Gutachten zum CSM-VO Nachweisdokument gemäß CSM-VO Abschnitt 5.1. 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.	+		+		+		-	
11 Betrieb / Instandhaltung											
12 Erfassung der Leistungsfähigkeit											
12	SyPR	Leistungsfähigkeitsbericht	Rücklauf aus den Protokollen spezifischer Anlagen für zukünftige Änderungen. Durch ISO 9001 abgedeckte Verfahren	-		+/-	Abhängig von der Art der Erweiterung	-		-/+	je nach Firmenprozess nur Start eines SyPR mit Installation der ersten spezifischen Applikation
13 Änderung / Nachrüstung											
13	SyRP	Releaseplan	Aufstellung der geplanten Erweiterungen und Verbesserungen. Durch die CENELEC nicht offiziell gefordertes Dokument!	-		-		-		-	
13	SyMP	Wartungsplan	Generischer Wartungsprozess (allgemeine Vorgehensweise). Für kleinere Hardwareänderungen gibt es bereits vereinfachtes Verfahren (ohne EBA-Vorlage), Idee: ähnliches für SW? Beinhaltet auch die Release-Planung. In Zukunft gemäß NTZ keine Prüfung durch EBA mehr.	-		-		+	mindestens Ergänzung eines Verweises auf die neue Steckkarte	-	

13	SyMR	Änderungsbericht	Änderungsbericht für jede Wartungsaktivität. Nur für Änderungen, die keine Spezifikationsänderungen beinhalten - sonst nicht zwingend erforderlich. In Zukunft gemäß NTZ keine Prüfung durch EBA mehr.	+	Beinhaltet eine Auflistung aller geänderten Dokumente und Systembestandteile/Artefakte	+	+		-
13	SwMR	SW-Wartungsaufzeichnungen		+		+	-		-
13	SwMVR	SW Wartungsverifikationsbericht		+		+	-		-
14 Stilllegung / Entsorgung									
9-14	SyDDN	Stilllegungs- und Entsorgungshinweise		-		-	+/-	Je nachdem, ob neue Bauteile dies erfordern	-

Tabelle 4: Dokumentenliste für die vier in Tabelle 3 definierten Anwendungsfälle

Hinweis: Verifikationsberichte sind hellgrau markiert.

7 Zusammenfassung und Ausblick

Es wurde von den am Arbeitspaket 2200 beteiligten Projektpartnern Bombardier, DB Netze, DLR, Funkwerk AG TCC, Pintsch Bamag, Scheidt & Bachmann, Siemens und Thales ein gemeinsames Verständnis entwickelt, wie die CENELEC-Normen EN 50126, EN 50128 und EN 50129 Anwendung finden sollen.

Dieses gemeinsame Verständnis ist in die in diesem Ergebnisbericht beschriebenen Arbeitsergebnisse in Form von CENELEC-konformen Dokumentenlisten eingegangen.

Damit wurde aus Sicht der beteiligten Projektpartner eine signifikante Verringerung der Interpretationsspielräume der CENELEC-Normen erreicht.

Auf Basis der generischen Dokumentenliste aus dem Teilbericht „Vorarbeiten und Unterarbeitspaket 2200.3" (NeGSt_Teilbericht_2200.0u3_1.0.pdf) wurden Ausprägungen von Dokumentenlisten für die spezifischen Anwendungsfälle ‚SW-Fehlerbehebung', ‚Systemerweiterung', ‚Weiterentwicklung einer HW-Steckkarte (als HW-Komponente)' und ‚Neue spezifische Applikation' für SIL 4 erstellt.

Mit dem Erstellen der Ausprägungen von Dokumentenlisten für die ‚Best Practices' wurde gleichzeitig die generische Dokumentenliste auf ihre Anwendbarkeit für verschiedene praktische Anwendungsfälle hin positiv verifiziert.

Außerdem wurde gezeigt, dass die Ergebnisse für SIL 4-Entwicklungen auch für SIL 2-Entwicklungen angewendet werden können.

Die hier vorliegenden Ergebnisse stehen als Leitfaden für alle beteiligten Partnerfirmen zur Verfügung und sollten aus Sicht der AG3 breite Anwendung in zukünftigen Projekten finden.