SR40 Safety Plan

Safety Plan - smartrail 4.0

Document Properties

Status: **document signed**

Version: **2**

Owner: Grabowski David (I-SR40-PMO-PLP)

Contributors: Einer Stefan (I-SR40-PMO-FSP), von Buxhoeveden Geltmar (I-SR40-PMO-EXT), Grabowski David (I-SR40-PMO-PLP)

Document history

Version (revision)	Changes	Document Owner	Approved	Signed
1 (317377)	1.1 Grundlegende Überarbeitung unter Berücksichtigung der eingetragenen Kommentare (equals rev. 312334)	Grabowski David (I-SR40-PMO-PLP)		Grabowski David (I-SR40-PMO-PLP) Leu Martin (I-SR40-PMO-EXT)
2 (329726)	1.2 Kommentare eingearbeitet	Grabowski David (I-SR40-PMO-PLP)	Grabowski David (I-SR40-PMO-PLP)	Leu Martin (I-SR40-PMO-EXT)

1 Inhaltsverzeichnis

2 Einleitung

Mit dem Programm smartrail 4.0 soll der Bahnbetrieb grundlegend geändert werden. Durch die Anwendung von neuen Systemen sollen

- die Gesamtkosten reduziert,
- die Trassenkapazität erhöht,
- die Sicherheit beim Rangieren und auf Baustellen erhöht,
- die Verfügbarkeit erhöht und
- die Datenfunk-Kapazität für Kundinnen und Kunden verbessert

werden. Dabei sind sowohl die Anwendungen als auch die Systeme neu zu entwickeln. Ein Teil der Anwendungen und ein Teil der Systeme sind sicherheitsrelevant (im Sinne von Safety). Die Entwicklung der sicherheitsrelevanten Anwendungen und Systeme hat gemäss den aktuell gültigen Vorgaben zur Entwicklung von sicherheitsrelevanten Bahnanwendungen zu erfolgen. Welche Vorgaben in welcher Version anzuwenden sind, ist im Dokument «Safety Policy» festgelegt.

Um die Entwicklungen aufeinander abzustimmen und einheitlich zu gestalten, werden Meta Modelle angewendet, die in den folgenden Kapiteln näher beschrieben werden. Die Anwendung der Meta Modelle erfolgt im Rahmen des Safety Managements der einzelnen Entwicklungsprojekte.

Die Policy für das Safety Management der Entwicklungsprojekte ist im Dokument "*SR40 Safety Policy"* beschrieben. Ergänzende Vorgaben für das Safety Management der Entwicklungsprojekte sind im Kapitel "Sicherheitsstrategie" dieses Dokuments aufgeführt.

Das Programm smartrail 4.0 ist ein Branchenprogramm. Jede Eisenbahnunternehmung des Branchenprogramms verfügt über ein eigenes Sicherheitsmanagementsystem, das seine Verfahren und Instrumente zur Steuerung der Sicherheit aufzeigt. Für die Entwicklung von betreiberspezifischen Anwendungen ist ergänzend zur "*SR40 Safety Policy*" das Sicherheitsmanagementsystem des entsprechenden Bahnbetreibers anzuwenden.

Eine Beschreibung der Organisation des Programms und eine Liste der Projekte finden sich im Kapitel "Organisation des Programms und der Projekte". Die wesentlichen Meilensteine und Lieferungen des übergeordneten Safety Managements sind in Kapitel "Planung der Safety Aktivitäten" aufgeführt. Weitere Kapitel beziehen sich auf die Prozesse, die gemäss Norm im Safety Plan beschrieben werden müssen.

Um die Einhaltung der Prozesse zu überprüfen führt das smartrail 4.0 Safety Management regelmässig (mindestens einmal pro Jahr) Safety Assessments durch.

3 Anwendung der Cenelec Norm

Bei der Entwicklung von sicherheitsrelevanten Bahnanwendungen und deren Systemen ist das in der Cenelec Norm SN EN 50126 aufgeführte Phasenmodell anzuwenden (siehe Dokument «Safety Policy»). Dazu ist das Phasenmodell in den Projekten durch das sogenannte «Tailoring» auf das jeweilige Entwicklungsprojekt anzupassen. Das Tailoring wird massgeblich durch den Typ des Entwicklungsgegenstands (Anwendung, System) bestimmt. In den folgenden Kapiteln wird näher auf die Typen der Entwicklungsgegenstände eingegangen und es wird für jeden Typ ein angepasstes Phasenmodel vorgegeben. Diese Vorgaben sind als Richtlinie zu verstehen, von der in begründeten Fällen abgewichen werden kann. Abweichungen sind zusammen mit einer schriftlichen Begründung im zugehörigen Safety Plan aufzuführen. Die Prozesse zur Umsetzung des RAMS Lebenszyklus beinhalten eine Detaillierung des Tailorings.

3.1 Bahnanwendungen

Mit einer Bahnanwendung wird ein System für den Bahnbetrieb eingesetzt. Dies erfordert neben der Installation und Inbetriebnahme des Systems eine Reihe weiterer Massnahmen, um einen reibungsfreien Bahnbetrieb über den Lebenszyklus der Anwendung aufrecht zu erhalten. Das im folgenden Kapitel aufgeführte Metamodell dient dazu, diese Massnahmen zu strukturieren und Abhängigkeiten aufzuzeigen.

Es ist zwischen der spezifischen Bahnanwendung und der generischen Bahnanwendung zu unterscheiden. Die generische Bahnanwendung ist dabei ein Hilfskonstrukt, das die Entwicklung und Zulassung von spezifischen Bahnanwendungen vereinfacht. Das Kapitel "Generische Bahnanwendungen" beschreibt den Einsatz und die Entwicklung der generischen Bahnanwendungen im Programm smartrail 4.0.

3.1.1 Spezifische Bahnanwendungen

Die Entwicklung von spezifischen Bahnanwendungen erfolgt gemäss den in der Cenelec Norm vorgegebenen Entwicklungsphasen:

1. Konzept
2. Systemdefinition und betrieblicher Kontext
3. Risikoanalyse
4. Systemanforderungen
5. Architektur und Zuteilung der Systemanforderung
6. Design und Implementierung
7. Fertigung
8. Installation und Integration
9. System Validierung
10. Systemabnahme

Nach der Systemabnahme (Phase 10) erfolgt der Betrieb inklusive Instandhaltung und zum Ende

des Lebenszyklus der Bahnanwendung die Ausserbetriebnahme.

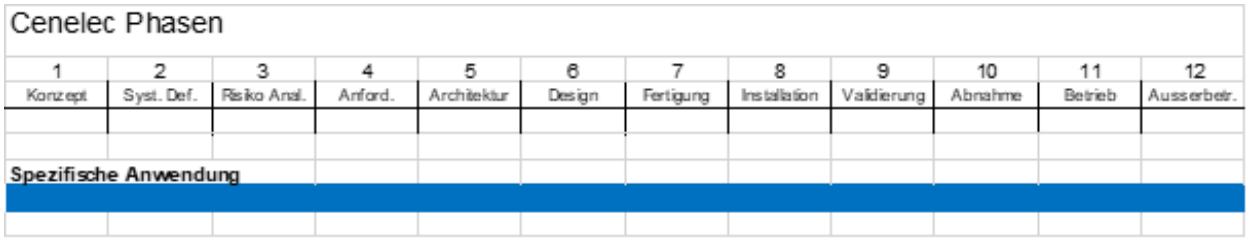


Figure 1: Cenelec Phasen der spezifischen Anwendung

Die Arbeiten an den Entwicklungsphasen 1 bis 5 können (müssen aber nicht) parallel erfolgen, der Abschluss der Entwicklungsphasen muss aber in der vorgegebenen Reihenfolge erfolgen. Jede Phase ist mit einer Verifikation abzuschliessen, zum Ende der Phase 4 ist ergänzend eine Validation durchzuführen (nicht im Ablauf dargestellt).

3.1.2 Generische Bahnanwendungen

Ist es geplant mehrere spezifische Bahnanwendungen zu installieren, die Gemeinsamkeiten aufweisen (z.B. gleiche Systeme, gleiche Betriebsprozesse), kann es sinnvoll sein, eine generische Bahnanwendung zu entwickeln, die bei der Entwicklung der einzelnen spezifischen Bahnanwendungen herangezogen werden kann. Dadurch wird die Entwicklung der spezifischen Bahnanwendungen vereinfacht und vereinheitlicht. Für die generische Bahnanwendung ist das gleiche Meta Modell wie für die spezifische Bahnanwendung anzuwenden. Die Entwicklung durchläuft die gleichen Entwicklungsphasen wie die spezifische Bahnanwendung. Die zu entwickelnden «Gegenstände» beschränken sich dabei auf die Gemeinsamkeiten. Eine Inbetriebnahme einer generischen Bahnanwendung ist nicht möglich. Teile der generischen Bahnanwendung, wie zum Beispiel Dienste, Systeme, Vorschriften, Organisationsstrukturen können in Betrieb oder in Kraft gesetzt werden, ohne dass eine spezifische Bahnanwendung betroffen ist. Die generische Bahnanwendung ist immer nur eine Grundlage für die Entwicklung und Installation von spezifischen Bahnanwendungen.

Generische Anwendungen können aus anderen generischen Anwendungen aufgebaut sein. Dabei ist es möglich, dass zusätzliche Teile hinzugefügt werden, vorhandene Teile ausgeschlossen werden oder mehrere generische Anwendungen zu einer übergeordneten generischen Anwendung zusammengefasst werden.

Bei der Entwicklung der generischen Bahnanwendungen in smartrail 4.0 ist zwischen einem bahnbetreiberunabhängigen Entwicklungsanteil und einem bahnbetreiberabhängigen Entwicklungsanteil zu unterscheiden. Mit der Entwicklung des bahnbetreiberunabhängigen Anteils wird eine generische Anwendungsklasse entwickelt. Die Entwicklung der generischen Anwendungsklasse erfolgt in den Entwicklungsphasen 1 bis 5 und endet im Allgemeinen mit der Phase 5. Die Entwicklung des bahnbetreiberabhängigen Anteils kann begleitend zur Entwicklung des bahnbetreiberunabhängigen Entwicklungsanteil beginnen, baut aber ab Phase 6 auf die entwickelte generische Anwendungsklasse auf. Die Entwicklung des bahnbetreiberabhängigen Anteils durchläuft in jedem Fall die Phasen 6 bis 10.

In den Entwicklungsphase 1 bis 5 werden die Anforderungen an die Systeme und die Umwelt

festgelegt und verfeinert. Mit dem Abschluss der Entwicklung der generischen Anwendungsklasse werden diese Anforderungen abschliessend festgelegt. In der Entwicklungsphase 6 wird der Integrationsprozess bestimmt. Dieser Integrationsprozess, ist der Entwicklungsprozess der spezifischen Anwendung und damit die eigentliche Schnittstelle zwischen generischer und spezifischer Anwendung. Die Ergebnisse der Entwicklung der generischen Anwendung können daher frühestens in der Phase 6 für die Entwicklung von spezifischen Anwendungen verwendet werden.

Die Durchführung des Integrationsprozesses wird durch betreiberspezifische Vorschriften und Werkzeuge unterstützt, die für alle spezifischen Anwendungen der jeweiligen Bahn anzuwenden sind. Deshalb hört die Entwicklung der bahnbetreiberspezifischen generischen Anwendung nicht mit dem Integrationsprozess auf, sondern sieht auch die Entwicklungsphasen 7 bis 10 vor, in denen die generischen Vorschriften und Werkzeuge designed, gefertigt, installiert, validiert und abgenommen werden.

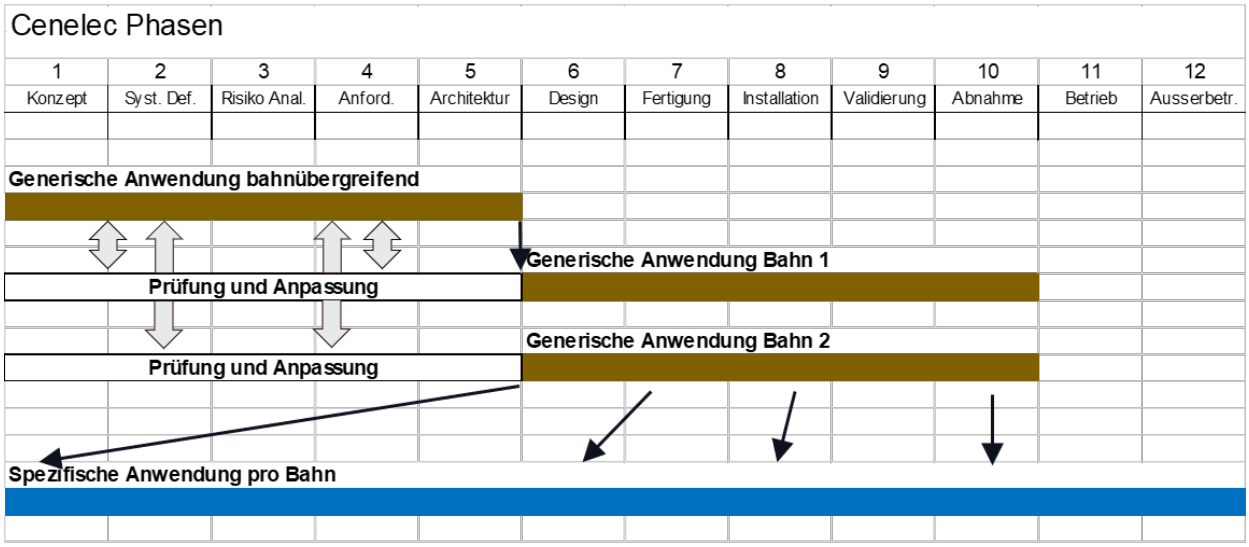


Figure 2: Cenelec Phasen der generischen Anwendung und der Bezug zu den Cenelec Phasen der spezifischen Anwendung. Die schwarzen Pfeile stellen die Übergabe von Ergebnissen dar. Die grauen Pfeile symbolisieren eine inhaltliche Abstimmung zwischen den Aktivitäten.

3.1.3 User Interfaces

Anwendungen mit User Interfaces müssen berücksichtigen, dass das technische System und der Mensch, der das User Interface bedient (User), ein übergeordnetes sozio-technisches System bilden. Die Zuverlässigkeit des technischen Systems ist eine notwendige, aber allein keine hinreichende Bedingung für die Verlässlichkeit des sozio-technischen Systems.

Zusätzliche arbeitspsychologische Aspekte und Human-Factors-Aspekte sind bei der Gestaltung des User Interfaces und der Aufgaben des Users mit zu berücksichtigen. Kriterien sind beispielsweise:

- der Erhalt vollständiger Tätigkeiten, die

  a) das selbstständige Setzen von Zielen ermöglicht,
  b) Handlungsvorbereitungen und Planungsfunktionen erlauben,

c) eine Auswahl der Mittel zur Zielerreichung ermöglicht,
d) Ausführungsfunktionen mit Feedback (ggf. zur Handlungskorrektur) beinhalten,
e) eine Kontrolle mit Resultat-Feedback ermöglicht;

- der Erhalt von Gestaltungs- und Handlungsspielräumen;
- die Nutzung vorhandener Qualifikationen sowie der Aufbau neuen Erfahrungswissens;
- und die Gewährleistung von Prozesstransparenz.

Sind an einem User Interface sicherheitsrelevante Eingaben oder Ausgaben möglich, so muss eine Beschreibung des zugehörigen sozio-technischen System erstellt werden. Das Anwendungsprojekt stimmt mit dem zuständigen Business Architekten ab, wer diese Beschreibung erstellt.

Basierend auf dieser Beschreibung muss eine arbeitspsychologische Analyse durchgeführt werden. In der arbeitspsychologischen Analyse ist festzulegen, wie sich die oben aufgeführte Kriterien und gegebenenfalls weitere Kriterien konkret umsetzen lassen und was sie im Einzelfall bedeuten. Das Anwendungsprojekt muss mit dem zuständigen Business Architekten abstimmen, wer die arbeitspsychologische Analyse durchführt bzw. durchführen lässt. Das Anwendungsprojekt ist in jedem Fall in der Pflicht sicherzustellen, dass die in der arbeitspsychologischen Analyse aufgeführten Kriterien umgesetzt werden. Ist die Umsetzung aus Sicht des Projektes nicht angebracht, muss eine Eskalation erfolgen.

3.2 Systeme

Für eine Anwendung sind ein oder mehrere Systeme notwendig. Ein System kann aus mehreren Sub-Systemen aufgebaut sein. Die Sub-Systeme sind für sich wieder Systeme. Somit ist es immer möglich, die einer Anwendung zugeordneten Systeme zu einem System zusammenzufassen. In diesem Sinne hat jede Anwendung ein System.

Ob ein System sicherheitsrelevant ist oder nicht, hängt vom betrieblichen Kontext des Systems ab. So ist zum Beispiel ein Lokalisierungssystem an einem Güterwagen, dass der Verfolgung (Tracking) der Güter dient, nicht sicherheitsrelevant. Wird das Lokalisierungssystem für eine vom Stellwerk benötigte Ortung eingesetzt, ist es sicherheitsrelevant. Aus diesem Grund ist der betriebliche Kontext für eine Sicherheitsbetrachtung essenziell.

Wird ein System ohne vorgegebenen betrieblichen Kontext entwickelt, so kann die Entwicklung dennoch gemäss den Cenelec Phasen erfolgen. Eine solche Entwicklung zeichnet sich dadurch aus, dass die Bestimmung der Systemumwelt offener erfolgt als bei der Anwendungsentwicklung, in der der betriebliche Kontext vorgegeben ist. Für die Anwendung eines solchen Systems muss geprüft werden, ob Anwendungs- und Systementwicklung zueinander passen.

Bei der Entwicklung sind zwei Arten von Systemen zu unterscheiden:

1. Systeme, die nur für den Einsatz innerhalb von smartrail 4.0 entwickelt werden und nicht weiter vermarktet werden sollen, weder durch den Hersteller noch durch smartrail 4.0.

Diese Systeme werden im folgenden als **programmeigene Systeme** bezeichnet.

2. Systeme, die von Industrie und Gewerbe entwickelt werden und als **Produkte** auch anderen potentiellen Kunden angeboten werden. Damit sollen bei den Lieferanten neben günstigeren Einkaufspreisen auch eine Pflege und Weiterentwicklung der Produkte herbeigeführt werden. Durch den Einsatz der Produkte sollen Integrationsfähigkeiten und Kompetenzen in Industrie und Gewerbe geschaffen werden, auf die die Bahnen bei Bedarf zurückgreifen können

Auch wenn die Produkte von Industrie und Gewerbe entwickelt werden, hat smartrail 4.0 einen Entwicklungsanteil an der Entwicklung der Produkte. Nur wenn smartrail 4.0 Anforderungen an die Produkte vorgibt, ist gewährleistet, dass die für smartrail 4.0 geeigneten Produkte entwickelt werden. Es ist daher ein spezielles Tailoring der Celenec Phasen notwendig, dass in den folgenden Kapiteln beschrieben wird.

3.2.1 Programmeigene Systeme

Sicherheitsrelevante programmeigene Systeme werden gemäss dem Cenelec Phasenmodel entwickelt und durchlaufen die Phasen 1 bis 10:

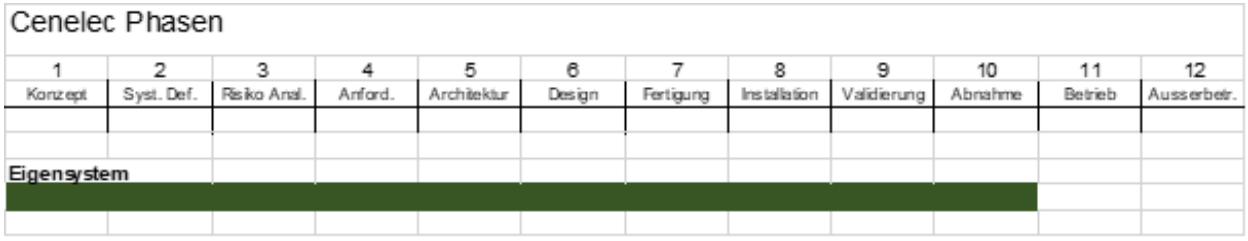


Figure 3: Cenelec Phasen, die bei der Entwicklung eines sicherheitsrelevanten programmeigenen Systems durchlaufen werden.

Die Entwicklung des programmeigenen Systems muss mit der Entwicklung der zugehörigen Anwendung abgestimmt sein. Damit ist sichergestellt, dass Produkt und Anwendung zueinander «passen».

3.2.2 Produkttypen und Produktklassen

Jedes Produkt ist ein System, aber nicht jedes System ist ein Produkt. Die Unterscheidung zwischen Produkt und System ist dabei zum Teil fliessend und branchenabhängig. Innerhalb von smartrail 4.0 erfolgt die Unterscheidung an Hand der Unterscheidbarkeit zwischen Fertigung und Installation: Ein Produkt ist ein System, dessen Fertigung und Installation unterscheidbare Arbeitsschritte sind und von verschiedenen Arbeitsgruppen ausgeführt werden können.

Werden Erwartungen an ein Produkt spezifiziert, können unterschiedliche Hersteller Produkte entwickeln, die diese Erwartungen erfüllen. Mit der Spezifikation von Erwartungen, zum Beispiel durch Anforderungen, wird eine Produktklasse festgelegt. Produktklassen können dabei wieder aus anderen Produktklassen aufgebaut sein.

Bei der Entwicklung von Produkten im Programm smartrail 4.0 muss zwischen der Entwicklung der Produktklassen, der Entwicklung der Produkttypen und der Fertigung der Produktinstanzen

unterschieden werden. Die Entwicklung der Produktklassen erfolgt in der Verantwortung des Programms als Vertreter der Bahnbetreiber (Infrastrukturbetreiber und Eisenbahnverkehrsunternehmen), die Entwicklung der Produkttypen und die Fertigung der Produktinstanzen erfolgt in der Verantwortung der Industrie.

Die Entwicklung der Produkttypen umfasst folgendes:
Design, Fertigungsprozesse, Fertigungseinrichtungen, die Validierung der Fertigung, Prototypen, Validierung und Abnahme der Prototypen, die Abnahme der Fertigungsprozesse, die Abnahme der Fertigungseinrichtungen.
Die nachfolgende Serienfertigung von Produktinstanzen ist nicht Gegenstand der Entwicklung und wird daher hier nicht näher betrachtet.

Die Entwicklung der sicherheitsrelevanten Produkttypen erfolgt gemäss dem Cenelec Phasenmodel und beginnt mit der Entwicklung der zugehörigen Produktklassen:

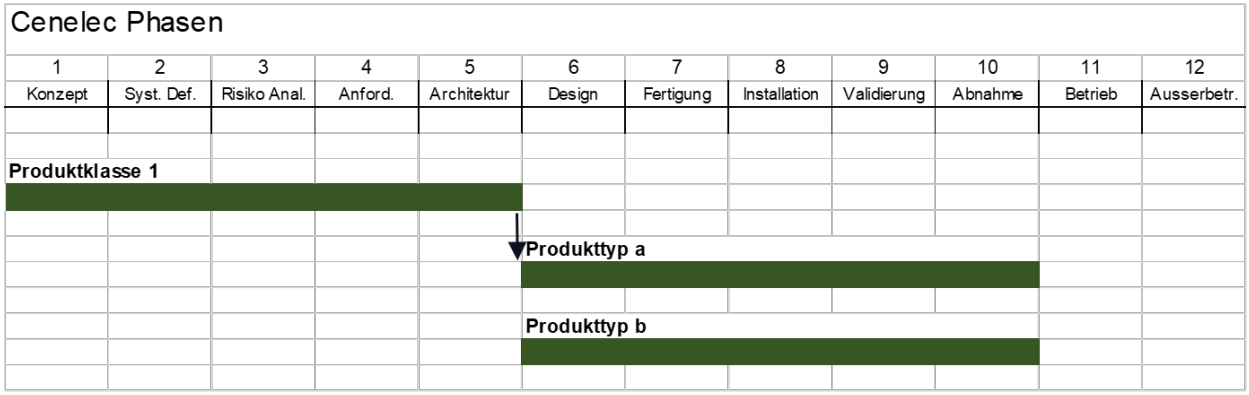


Figure 4: Cenelec Phasen, die bei der Produktentwicklung durchlaufen werden. Die Phasen 1-5 werden in der Verantwortung des Programms als Vertreter der Bahnen durchgeführt, die folgenden Phasen in der Verantwortung von Industrie/Gewerbe.

Die Entwicklung der Produktklasse muss mit der Entwicklung der zugehörigen Anwendung abgestimmt sein.

3.3 Das Meta Model für Bahnanwendungen

Für eine Bahnanwendung wird das in Figure 5 dargestellte Metamodell zugrunde gelegt. Es gibt einen Überblick über die Zusammenhänge der Typen von Entwicklungsgegenständen.

Die Bahnanwendung lassen sich in zwei Kategorien einteilen, die "spezifische Anwendung" und die "generische Anwendung" (siehe Kapitel "Spezifische Bahnanwendungen" und Kapitel "Generische Bahnanwendungen").

Sowohl die spezifische als auch die generische Anwendung beinhalten ein System, das zur Anwendung kommt. Dieses System ist das "System under Consideration" (SuC). In beiden Kategorien gibt es Umsysteme des SuC, die als "Kontext Systeme" bezeichnet werden.

Im Fall der spezifischen Anwendung handelt es sich beim SuC und bei den Kontext Systemen um konkrete Installationen von Systemen. Die generische Anwendung hingegen kann

sich auf Abstraktionen solcher Installationen beziehen. Damit können Eigenschaften gefordert oder vorausgesetzt werden, die von mehreren spezifischen Anwendungen erfüllt werden.

Sowohl die spezifische als auch die generische Anwendung umfassen ergänzend zum SuC und den Umsystemen einen "generischen Kontext". Dieser ist generisch, weil er der Kontext für verschiedene spezifische Anwendungen sein kann. Er umfasst aber in jedem Fall konkrete Personen ("Mitarbeiterpool") und Anleitungen, die den Mitarbeitern zur Verfügung stehen ("Anleitungsbibliothek"). Anleitungen und Personen können sich auf die Rollen in der Betriebsphase der spezifischen Anwendung beziehen oder auch auf die Planung und Realisierung der spezifischen Anwendung, dem "Entwicklungskontext der spezifischen Anwendung". Im Entwicklungskontext der spezifischen Anwendung werden Werkzeuge benötigt. Die Installationen der Werkzeuge ist Teil des generischen Kontextes.

Soll der generische Kontext nur abstrahiert betrachtet werden, also lediglich Merkmale von ihm festgelegt werden, ist die generische Anwendung nicht abschliessend festgelegt, sondern es wird eine "Generische Anwendungsklasse" gebildet. Die generische Anwendungsklasse bildet eine Anforderung für diejenigen generischen Anwendungen, die diese Anforderungen zu erfüllen haben.

Installationen von Systemen bestehen aus programmeigenen Systemen und Produkten. Um deutlich zu machen, dass es sich dabei um bestimmte Exemplare von Produkten handelt, z.B. erkennbar an der Seriennummer, wird von "Produktinstanzen" gesprochen. Ein "Produkttyp" fasst gleiche Produktinstanzen zusammen, hält also das Design der Produktinstanz fest. Eine "Produktklasse" beschränkt sich gegenüber dem Produkttyp auf eine bestimmte Untermenge von Produkteigenschaften und subsummiert so verschiedene Produkttypen.

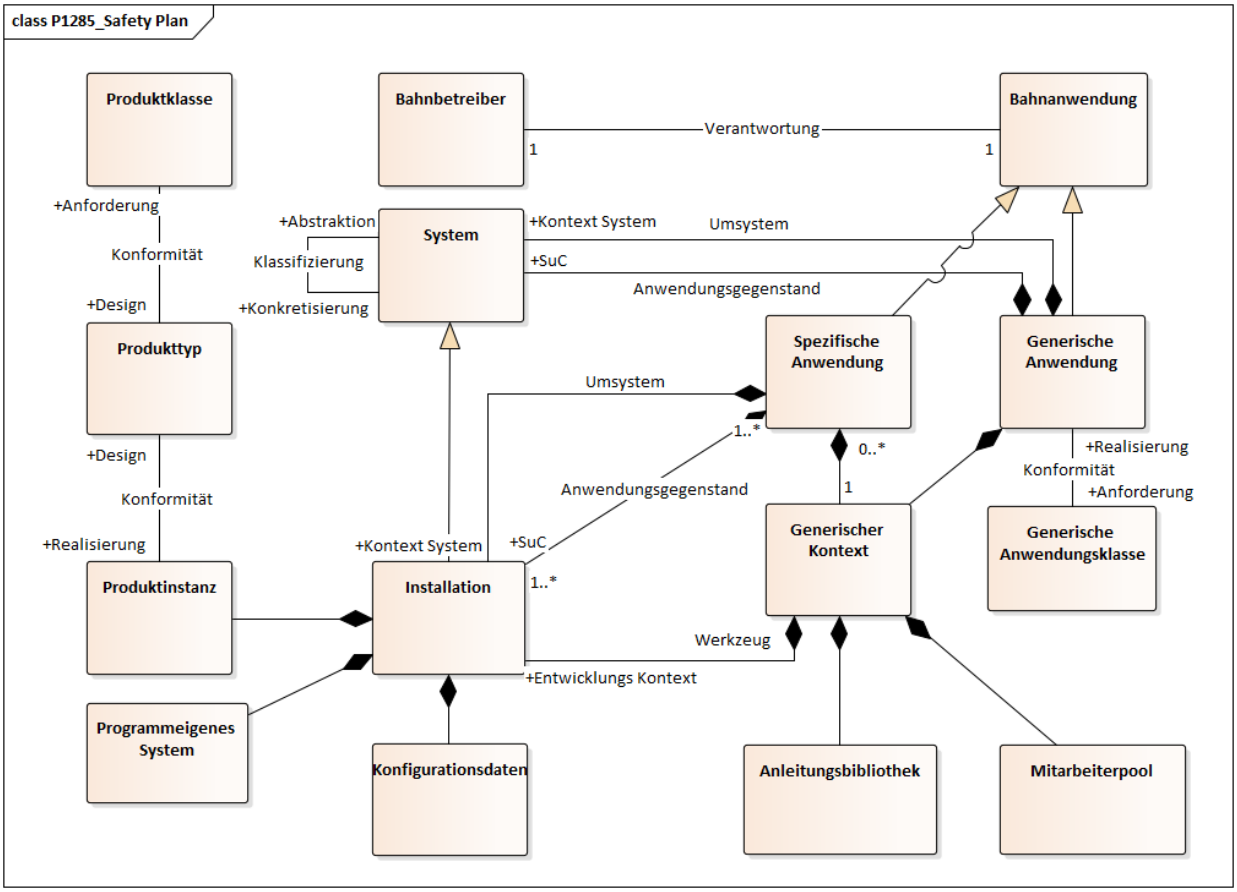


Figure 5: SR40 Metamodell für Bahnanwendungen

3.4 Software

Systeme können aus Hardware oder aus Hardware und Software aufgebaut sein. Software ohne Hardware kann nicht ausgeführt werden und stellt kein System dar. Systeme, die aus Hardware und Software aufgebaut sind, werden hier als **Softwaresysteme** bezeichnet.

Die Entwicklung von Software erfordert immer eine vorrangige Systementwicklung des Softwaresystems. Die Zuweisung von sicherheitsrelevanten Funktionen an die Software sowie die Software-Schnittstellen, erfolgt in der Systemdokumentation des Softwaresystems. Das Softwaresystem muss vollständig definiert sein hinsichtlich:

- Funktionen und Schnittstellen;
- Anwendungsbedingungen;
- Konfiguration oder Architektur des Systems;
- zu kontrollierende Gefährdungen;
- Anforderungen an die Sicherheitsintegrität;
- Aufteilung der Anforderungen und Zuweisung der SIL an die Software und Hardware;
- Zeitvorgaben.

Software, die nachweislich keinen Einfluss auf die Sicherheit hat, d.h. Software, bei der

Fehlfunktionen keine der identifizierten Sicherheitsfunktionen beeinträchtigen können, ist nicht sicherheitsrelevant. Für die Entwicklung von nicht sicherheitsrelevanter Software gibt es keine normativen Vorgaben.

Sicherheitsrelevante Software ist nach den Vorgaben der Cenelec Norm SN EN 50128 zu entwickeln. Die Softwareentwicklung ist Teil der Cenelec Phasen 6 (Design) und 7 (Fertigung) des Softwaresystems. In der Cenelec Phase 8 (Installation) des Softwaresystems wird die Software und Hardware zu einem System integriert.

3.5 Security

Sicherheitsrelevante Meldungen und sicherheitsrelevante Funktionen müssen vor Manipulationen geschützt werden. Damit sind Security und Safety potenziell miteinander verbundene Eigenschaften. Die Vorgaben, wie Security zu realisieren ist, werden im Dokument "Security Planung" (noch in Erstellung) beschrieben.

Um mögliche Konflikte zwischen Security Anforderungen und Safety Anforderungen zu vermeiden, sind im Lebenszyklus der Software folgende Regeln anzuwenden:

- Kompatibilität von Security Massnahmen mit sicherheitsrelevanten Funktionen: Die Anwendung von Security Massnahmen soll die Integrität der sicherheitsrelevanten Funktionen nicht beeinträchtigen

- Kompatibilität der sicherheitsrelevanten Funktionen mit Security Massnahmen: Die sicherheitsrelevanten Funktionen sollen die Wirksamkeit der Security Massnahmen nicht beeinträchtigen.

- Synchronisation der Safety- und Securityaufgaben: Die Kompatibilität zwischen den sicherheitsrelevanten Funktionen und den Security Massnahmen soll über den gesamten Lebenszyklus des Systems etabliert, dokumentiert, validiert und aufrechterhalten werden.

Gegebenenfalls sind vom Entwicklungsprojekt Anwendungsbedingungen zu formulieren, mit denen die geforderte Kompatibilität über den Lebenszyklus aufrechterhalten werden kann.

3.6 Werkzeuge

Es gibt zwei Einsatzbereiche von Werkzeugen (englisch bezeichnet als Tools):

1. Werkzeuge, die für die Entwicklung der Systeme und Bahnanwendungen eingesetzt werden, wie z.B. Simulations- und Analyse Tools, Test Tools, Konfigurationstools, Compiler, Dokumentationswerkzeuge, Projektierungstools, …
2. Werkzeuge für die Bereitstellung von Diensten, die während der Betriebsphase benötigt werden, wie z.B. Monitoring Tools, Diagnose Tools, Reparatur Werkzeuge, ...

In beiden Einsatzbereichen können Werkzeuge die Sicherheit der spezifischen Bahnanwendung beeinflussen. Werkzeuge des ersten Einsatzbereiches fallen unmittelbar unter die Vorgaben der EN 50128 für Werkzeuge der Softwareentwicklung (einschliesslich Daten). Da die Werkzeuge des zweiten Einsatzbereichs ebenfalls Einfluss auf das Laufzeitverhalten eines Systems haben, werden sie in smartrail 4.0 gleich behandelt, wie Werkzeuge der SW-Entwicklung.

Werkzeuge, die die Sicherheit der spezifischen Bahnanwendung beeinträchtigen können, erhalten eine Zulassung bei der Erstanwendung im Rahmen der Zulassung der generischen oder spezifischen Bahnanwendung.

3.6.1 Werkzeuge der Softwareentwicklung

Die Cenelec Norm SN EN 50128 gibt für Werkzeuge der Softwareentwicklung die drei Klassen T1, T2 und T3 vor.

- Werkzeuge der Klasse T1 erzeugen keine Ausgaben, die direkt oder indirekt zum ausführbaren Code (einschließlich Daten) der Software beitragen.
- Werkzeuge der Klasse T2 unterstützen den Test oder die Verifikation des Entwurfs oder ausführbaren Codes, bei dem Fehler im Werkzeug zur Nicht-Erkennung von Fehlern führen können, jedoch in der ausführbaren Software keine Fehler direkt erzeugen können.
- Werkzeuge der Klasse T3 erzeugen Ausgangsdaten, die direkt oder indirekt zum ausführbaren Code (einschließlich Daten) des sicherheitsrelevanten Systems beitragen.

In der Cenelec Norm SN EN 50128 wird für jede der drei Klassen vorgegeben, welche Nachweise für das Werkzeug zu erbringen sind.

Projekte, die sicherheitsrelevante Software entwickeln, müssen alle im Projekt eingesetzten Werkzeuge zur Softwareentwicklung aufführen und in die Klassen T1, T2 und T3 einteilen. Die Einteilung muss gemäss den Vorgaben in der Cenelec Norm SN EN 50128 erfolgen und begründet werden. Die Werkzeuge müssen die Forderungen der Cenelec Norm SN EN 50128 nachweislich erfüllen.

3.6.2 Sonstige Werkzeuge

Die Einteilung und Bewertung von Werkzeugen, die nicht der Softwareentwicklung dienen, erfolgt hier in Analogie zur Einteilung und Bewertung der Werkzeuge zur Softwareentwicklung. Die Einteilung umfasst Werkzeuge, die für die Entwicklung der Systeme und Bahnanwendungen eingesetzt werden als auch Werkzeuge, die für die Bereitstellung von Diensten während der Betriebsphase benötigt werden.

Die Einteilung der Werkzeuge erfolgt in die drei Klassen TS1, TS2 und TS3:

- Werkzeuge der Klasse TS1 erzeugen keine Ergebnisse, die direkt oder indirekt zu einer sicherheitsrelevanten Situation führen können.
- Werkzeuge der Klasse TS2 erzeugen keine Ergebnisse, die direkt zu einer sicherheitsrelevanten Situation führen können. Indirekt können fehlerhafte Ergebnisse zu einer sicherheitsrelevanten Situation führen. Bei der Weiterverarbeitung der Ergebnisse ist aber es wahrscheinlich, dass Fehler in den Ergebnissen gefunden werden.
- Werkzeuge der Klasse TS3 erzeugen Ergebnisse, die direkt oder indirekt zu einer sicherheitsrelevanten Situation führen können. Falls eine Weiterverarbeitung der Ergebnisse vorgesehen ist, ist es unwahrscheinlich, dass Fehler in den Ergebnissen gefunden werden.

Im Zweifelsfall muss an Hand von Analogien zur Einteilung der Werkzeuge der Softwareentwicklung entscheiden werden, welche Klasse zutreffend ist.

Projekte, die sicherheitsrelevante Systeme oder sicherheitsrelevante Anwendungen entwickeln, müssen

- alle im Projekt eingesetzten Werkzeuge aufführen und in die Klassen TS1, TS2 und TS3 einteilen.
- alle für den Betrieb zu entwickelnden Werkzeuge aufführen und in die Klassen TS1, TS2 und TS3 einteilen.

Analog zu den Nachweisen für Werkzeuge der Softwareentwicklung gelten folgende Regeln, die vom Projekt umzusetzen sind:

- Die Auswahl von Werkzeugen in den Klassen TS2 und TS3 ist zu begründen.
  Die Begründung muss die Identifizierung möglicher Fehler enthalten, die in die Ergebnisse der Werkzeuge einfließen können, und die Maßnahmen zur Vermeidung oder Behandlung derartiger Fehler aufzeigen.
- Alle Werkzeuge in den Klassen TS2 und TS3 müssen eine Spezifikation oder ein Handbuch besitzen in der bzw. dem das Verhalten des Werkzeuges klar definiert ist, und alle Anweisungen oder Randbedingungen hinsichtlich seiner Anwendung aufgeführt sind.
- Für jedes Werkzeug in Klasse TS3 muss ein Nachweis verfügbar sein, dass das Ausgangsprodukt des Werkzeugs der Spezifikation des Ausgangsproduktes entspricht oder Fehlfunktionen in den Ausgangsprodukten festgestellt werden. Der Nachweis darf auf

den gleichen Schritten beruhen, die für einen manuellen Prozess als Ersatz für das Werkzeug notwendig sind, und es darf begründet werden, wenn diese Schritte durch Alternativen ersetzt werden (z. B. Validierung des Werkzeugs). Der Nachweis darf auch beruhen auf:

- a) eine geeignete Kombination der Chronik des erfolgreichen Einsatzes in ähnlichen Umgebungen und für ähnliche Anwendungen (innerhalb der Organisation oder anderer Organisationen);
- b) Werkzeug-Validierung
- c) diversitäres redundantes System, dass die Aufdeckung und Kontrolle von Fehlfunktionen erlaubt, die zu Fehlern führen, die vom Werkzeug eingebracht wurden;
- d) Übereinstimmung mit den Sicherheits-Integritätslevel, die aus der Risikoanalyse des Prozesses und der Verfahren, einschließlich der Werkzeuge, abgeleitet werden;
- e) weitere geeignete Methoden zur Vermeidung oder zu Behandlung von Fehlfunktionen, die von Werkzeugen eingebracht werden.

Die Ergebnisse der Werkzeug-Validierung müssen dokumentiert werden und Folgendes umfassen:

- a) eine Aufzeichnung der Validierungsaktivitäten;
- b) die Version des verwendeten Handbuchs des Werkzeugs;
- c) die validierten Werkzeugfunktionen;
- d) verwendete Hilfsmittel und Geräte;
- e) die Ergebnisse der Validierungsaktivitäten; die dokumentierten Ergebnisse der Validierung müssen entweder angeben, dass das Werkzeug die Validierung bestanden hat oder die Gründe für dessen Versagen;
- f) Testfälle und deren Ergebnisse für die anschließende Analyse;
- g) Nichtübereinstimmungen zwischen erwarteten und tatsächlichen Ergebnissen.

Ist kein Nachweis verfügbar, muss das Projekt wirksame Maßnahmen für die Kontrolle der Fehlfunktionen des Systems definieren, deren Fehler dem Werkzeug zuzuschreiben sind.

4 Safety Strategie

Die folgenden Forderungen beziehen sich ausschließlich auf Entwicklungsprojekte, die eine sicherheitsrelevante Anwendung, ein sicherheitsrelevantes System, ein sicherheitsrelevantes Produkt, eine sicherheitsrelevante Produktklasse, ein sicherheitsrelevantes Werkzeug oder eine sicherheitsrelevante Software, gemäss Kapitel 5.1, entwickeln.

Jedes Projekt muss ein projektspezifisches Safety Management etablieren. Wenn Projekte in einer direkten Abhängigkeit zueinander stehen (z.B. die Entwicklung einer Anwendung und die Entwicklung des zugehörigen anzuwendenden Systems), ergibt sich daraus eine Abhängigkeit

der Safety Anforderungen: Es muss ein Austausch von Safety Anforderungen, von Anwendungsbedingungen, Hazards und Nachweisen der Anforderungserfüllung zwischen den Projekten erfolgen. Dieser Austausch erfolgt in Polarion über die dafür vorgesehenen Links und ist über den Lebenszyklus der Entwicklungen zu pflegen. Wie die Weitergabe im Detail umzusetzen ist, wird im Kapitel "Lebenszyklen und deren Prozesse" dieses Dokuments beschrieben.

Jeder sicherheitsrelevante Entwicklungsgegenstand und damit auch jeder Zulassungsgegenstand ist genau einem Projekt zuzuordnen. Gibt es eine projektübergreifende Abhängigkeit von Entwicklungsgegenständen (Artefakten), müssen die betroffenen Projektleiter eine eindeutige Zuordnung der Verantwortung für den Gegenstand zu einem der Projekte festlegen und dokumentieren. Können sich die Projektleiter nicht einigen, müssen die Projektleiter das Problem eskalieren.

Die Entwicklungsarbeiten in den Entwicklungsphasen 1 bis 5 können (müssen aber nicht) parallel erfolgen. Der Abschluss aller Entwicklungsphasen muss aber in der vorgegebenen Reihenfolge erfolgen.

Jedes Projekt muss zu jeder Entwicklungsphase die anzuwendenden Methoden festlegen. Die festgelegten Methoden müssen geeignet sein, um die Ziele der Phase zu erreichen. Methoden und Eignung sind gemäss den vorgegebenen Prozessen zu dokumentieren. Die Entwicklungsprozesse müssen sicherstellen, dass die Wahl einer Methode begründet und die Begründung dokumentiert wird, sofern der Prozess eine Methodenwahl vorsieht.

Basierend auf den anzuwendenden Methoden muss jedes Projekt zu Beginn jeder Entwicklungsphase vorgeben, wie die Verifikation zum Abschluss der Phase zu erfolgen hat. Diese Vorgabe ist ebenfalls prozessgemäss zu dokumentieren.

Jede Entwicklungsphase kann nur mit einer Verifikation abgeschlossen werden. Das Projekt muss einen Verifizierer mit der Durchführung der Verifikation beauftragen. Die Beauftragung hat gemäss den vorgegebenen Prozessen und schriftlich zu erfolgen. Der Verifizierer darf nicht selbst in der Entwicklungsphase des Projekts mitgearbeitet haben, kann aber ein Mitarbeiter eines anderen Projekts von smartrail 4.0 sein. Der Verifizierer muss die Ergebnisse seiner Verifikation schriftlich dokumentieren.

Befunde aus der Verifikation sind vom Projekt auf Relevanz zu prüfen. Relevante Befunde sind zu beheben und vom Verifizierer erneut zu bewerten. Die Verifikation kann nur abgeschlossen werden, wenn keine relevanten Befunde mehr offen sind.

Der Safety Plan jedes Projekts ist dem zuständigen Gutachter mit dem Abschluss der Entwicklungsphase 2 (System Definition) vorzulegen. Für die Projekte bei smartrail 4.0 ist der Gutachter im Allgemeinen die Sicherheitsstelle SR4.0.

Mit dem Abschluss der Phase 4 (Systemanforderungen) ist eine Validierung durch einen unabhängigen Validierer vorzusehen. Für die Projekte bei smartrail 4.0 wurden Herr Montigel und Herr Breuer als unabhängige Validierer bestellt.

Die Validierer begleiten die Projekte mindestens in den Entwicklungsphasen 1 bis 4. Mit dem

Validierungsreport zum Abschluss der Phase 4 endet zunächst der erteilte Validierungsauftrag.

Befunde aus der Validierung sind vom Projekt auf Relevanz zu prüfen. Relevante Befunde sind zu beheben und vom Validierer erneut zu bewerten. Die Validierung kann nur abgeschlossen werden, wenn keine relevanten Befunde mehr offen sind.

Die Rollen der Reviewer, der Verifizierer und der Validierer grenzen sich wie folgt voneinander ab:

Aktivität	Reviewer	Verifizierer	Validierer
Phasenbezug der Prüfung	innerhalb Phase	Abschluss Phase	phasenübergreifend
Prüfung Normvorgaben und Prozesse	×	✓ Einhaltung	✓ adäquate Definition Prozesse sowie Stichproben der Einhaltung
Prüfung Arbeitsmethodik	×	✓ adäquate Auswahl+Einhaltung	✓ adäquate Methodensequenz
Materielle Prüfung der Arbeitsergebnisse	✓	✓ Stichproben (nach Ermessen Verifizierer)	✓ Stichproben (nach Ermessen Validierer)
Prüfung Review	×	✓	✓ Stichproben
Prüfung Gebrauchstauglichkeit in order to allow the system under consideration to serve the intended use or application	×	×	✓
Prüfung Verifizierung	×	×	✓

Tabelle 1: Abgrenzung der Rollen, mit "x" bezeichnete Felder zeigen an, dass die Aktivität von der Rolle nicht durchgeführt wird.

5 The Scope of the Plan

Der vorliegende Safety Plan ist der übergeordnete Safety Plan für alle Entwicklungsprojekte des Gesamtprogramms smartrail 4.0, die eine sicherheitsrelevante Anwendung, ein sicherheitsrelevantes System, ein sicherheitsrelevantes Produkt, eine sicherheitsrelevante Produktklasse, ein sicherheitsrelevantes Werkzeug oder eine sicherheitsrelevante Software entwickeln. Die betroffenen Entwicklungsprojekte werden im folgenden als "sicherheitsrelevante Entwicklungsprojekte" bezeichnet.

Projekte, die Anwendungen, Systeme, Produktklassen, Produkte, Werkzeuge oder Software entwickeln, die nicht sicherheitsrelevant sind, müssen den vorliegenden Safety Plan nicht berücksichtigen. Wie im folgenden Unterkapitel beschrieben, müssen solche Projekte aber nachweisen, dass sie nicht sicherheitsrelevant sind.

Der vorliegende Safety Plan stellt eine Richtlinie dar, von der in begründeten Fällen abgewichen werden kann. Abweichungen sind mit gegebenenfalls betroffenen Projekten abzustimmen und zusammen mit einer schriftlichen Begründung im zugehörigen Safety Plan aufzuführen.

Neben diesem Safety Plan existiert das Dokument "Safety Policy", in dem grundlegende Aspekte und Rahmenbedingungen des Safety Managements für alle sicherheitsrelevanten Projekte des

Gesamtprogramm smartrail 4.0 festgelegt werden. Es macht Vorgaben für das Safety Management und legt unter anderem fest, welche Versionen der Normen anzuwenden sind.

Die Vorgaben im Dokument "Safety Policy" sind von allen sicherheitsrelevanten Projekten umzusetzen.

5.1 Organisation des Programms und der Projekte

Das Gesamtprogramm smartrail 4.0 umfasst fünf Umsetzungsprogramme, die wiederum eine Reihe von Entwicklungsprojekten umfassen. Jedes Projekt ist vom Leitungsteam des Gesamtprogramms, dem sogenannten Kernteam, zu genehmigen (Vorgehen zur Genehmigung siehe Programm Handbuch).

An Hand der bisherigen Konzepte wurde eine vorläufige Einteilung der Projekte in "sicherheitsrelevant" und "nicht sicherheitsrelevant" vorgenommen. Bei allen Projekten, die als "nicht sicherheitsrelevant" eingestuft wurden, hat der Projektleiter eine Analyse nach der SBB Konzernrichtlinie K250.1 durchzuführen und damit zu überprüfen, ob die Einstufung korrekt ist und welche Bedingungen mit der Einstufung verbunden sind. Die Analyse inklusive Ergebnis ist zu dokumentieren und vom Projektleiter freizugeben.

Die folgende Liste gibt einen Überblick über die Umsetzungsprogramme, die den Umsetzungsprogrammen zugeordneten Projekten und deren Einstufung bezüglich der Sicherheitskritikalität. Solange keine freigegebene Analyse zur Sicherheitsrelevanz vorliegt, ist die Einstufung als vorläufig anzusehen.

Das Programm Trafic Management (TMS) beinhaltet die folgenden Projekte:

- TMS Planung und Steuerung (Sicherheitsrelevanz noch offen, Softwareentwicklung nach SIL0)
- TMS Lenkung (nicht sicherheitsrelevant, Draft Version der Analyse liegt vor)
- TMS-Topologie (TMS-TOPO) (nicht sicherheitsrelevant, Draft Version der Analyse liegt vor)
- TMS Automatic Train Operation (ATO) auf Seite Infra (nicht sicherheitsrelevant, Analyse noch ausstehend)

Das Programm ETCS Stellwerk beinhaltet folgende Projekte:

- Anwendung APS (sicherheitsrelevant)
- APS Core (sicherheitsrelevant)
- Object Controller (OC) (sicherheitsrelevant)

- sichere Topologie (Topo4) (sicherheitsrelevant)
- Engineering Data Preparation (EDP, ehemalig AMP) (nicht sicherheitsrelevant, Analyse liegt vor)
- Diagnose, Monitoring und Device Configuration (DMDC, ehemalig DMMC) (Diagnose, Monitoring nicht sicherheitsrelevant, Analyse noch ausstehend, Device Configuration sicherheitsrelevant)
- Manoeuvre Train Control (MTC) (sicherheitsrelevant)
- Safe Data Center (SDC, ehemalig "sicheres Rechenzentrum") (sicherheitsrelevant)

Das Programm Localisation, Connectivity und Security (LCS) beinhaltet folgende Projekte:

- Connectivity (Funknetz) (nicht sicherheitsrelevant, gemäss EN 50129 (2010))
- Connectivity (Festnetz) (nicht sicherheitsrelevant, gemäss EN 50129 (2010))
- Applikation FRMCS auf dem Fahrzeug (COAT), Bedienung Sprach- und Datenfunk (nicht sicherheitsrelevant, Analyse noch ausstehend)
- Plattform Security (nicht sicherheitsrelevant, Analyse noch ausstehend)
- Genaue lokalisierbare allgemeinverwendbare Endgerätetechnik (GLAT) (sicherheitsrelevant)
- Automatische Warn Anlagen Produkte (AWAP) (sicherheitsrelevant)
- Applikation TIMS auf der Plattform COAT zur Detektion der Zug Integrität (sicherheitsrelevant)

Das Programm Automatic Train Operation (ATO) beinhaltet gemäss den betrieblichen Anforderungen der ERMTS User Group ATO OVER ETCS OPERATIONAL REQUIREMENTS, V1.7, keinerlei sicherheitsrelevante technische Systeme. Das zu entwickelnde User Interface erlaubt aber sicherheitsrelevante Eingaben.

Das Programm Fahrzeugausrüstung (COAT) beinhaltet nachfolgende Projekte:

- Applikation VMS, On-board Applikation zu Diagnose, Maintenance, Monitoring, Konfiguration (nicht sicherheitsrelevant, Analyse noch ausstehend)
- Middleware, beinhaltet SRACS und Engineering Rules für Applikationen, SDK, OS, Virtualisierung und Schnittstellenabstraktion (sicherheitsrelevant)
- Hardware, vorzertifizierte Rechnerhardware die Funktionen bis SIL-4 ermöglichen (sicherheitsrelevant)
- DMI, vorzertifizierte Bedienhardware (nicht sicherheitsrelevant, Analyse noch ausstehend)
- Peripherie, vorzertifizierte Sensoren- und Aktoren die Funktionen bis SIL-4 ermöglichen (sicherheitsrelevant)
- Baureihenintegration, Integration aller generischen Lösungsteile in eine Fahrzeugbaureihe / Flotte (kein Entwicklungsprojekt).

Neben den Umsetzungsprogrammen und den darin enthaltenen Projekten gibt es querschnittliche Programme, deren Aktivitäten und Projekte auf die Projekte in den Umsetzungsprogrammen wirken. Beispiele dafür sind Safety und Security aber auch die Gesamtarchitektur und das Querschnittsprogramm Prozesse & Anforderungen (P&A).

5.2 Safety Organisation

Querschnittliche Themen wie z.B. Safety, Security und RAM sind dem Programm Fachliche Querschnittsthemen (FQT) zugeordnet. Das Programm FQT hat die Aufgabe, projektübergreifende Vorgaben zu entwickeln und die Projekte bei der Umsetzung der querschnittlichen Themen zu unterstützen. Jedes sicherheitsrelevante Projekt hat einen projektspezifischen Safety Manager, der vom Safety Team des FQTs fachlich geführt wird. Die Safety Organisation ist wie folgt aufgebaut:

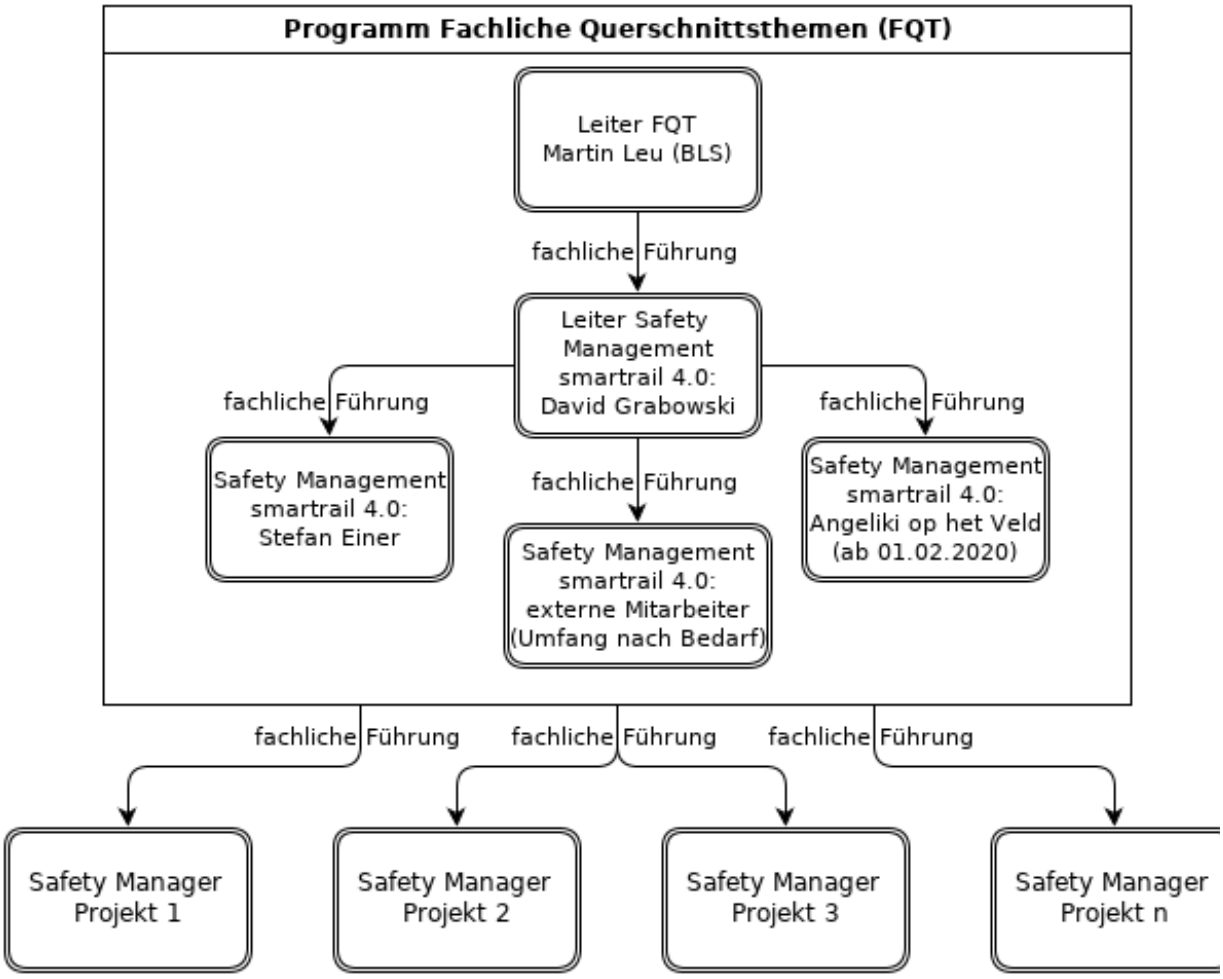


Figure 6 : Safety Organisation smartrail 4.0

5.3 Safety Planung der Projekte

Jedes Projekt muss einen projektspezifischen Safety Plan erstellen, der die in der Cenelec Norm SN EN 50126-1, Kapitel 7.3.2.3 (Safety Plan) aufgeführten Aktivitäten abdeckt. Dabei kann auf die Angaben in diesem Safety Plan verwiesen werden, sofern die Angaben in diesem Dokument die Aktivität ausreichend beschreiben. Wenn vorgegebene Aktivitäten nicht angewendet werden sollen, ist das im Safety Plan zu begründen.

Der Safety Plan muss die projektspezifische Anwendung des Meta Modells (siehe Kapitel "Meta Modell") und das Tailoring der Entwicklungsphasen beschreiben.

Der Safety Plan muss eine Liste der zu erstellenden Dokumente enthalten. Alle diese Dokumente sind in Polarion zu erstellen. Jedes dieser Dokumente muss einem Review unterzogen werden. Siehe dazu auch *Safety/70_safety/Safety Policy*, Kapitel 8, "Geforderte Safety Dokumente".

6 Planung der Safety Aktivitäten

Es ist zwischen den Planungsaktivitäten auf Programmebene und den Planungsaktivitäten auf Projektebene zu unterscheiden. Auf der Programmebene werden Meilensteine, die für das Programm gelten, geplant. Auf Projektebene werden die Durchläufe der S-Lebenszyklen geplant.

Meilensteine für Lieferungen durch das Programm smartrail 4.0:

Datum	Meilenstein	Status
01.03.2020	Abgabe der Dokumente zur vierten Kommentierung an die SiSt SR40	offen
01.06.2020	Abgabe Draft Risikoanalysen Phase 4 an die RBS (SiSt SR40)	offen
01.04.2021	Abgabe Risikoanalyse Phase 4 an die RBS (SiSt SR40)	offen
01.06.2021	Abgabe Sicherheitsnachweis Phase 4 an die SiSt SR40	offen
01.06.2021	Abgabe der Systemanforderungen und Zuteilungen für die Komponenten an die SiSt SR40	offen
01.03.2022	Abgabe Sicherheitsbericht Phase Planung für die Erprobungsstrecke an die SiSt SR40	offen
01.05.2024	Abgabe der Risikoanalysen generische Anwendungen an die RBS (SiSt SR40)	offen
01.06.2024	Abgabe Sicherheitsnachweis generische Anwendungen an die SiSt SR40	offen
01.08.2024	Abgabe Risikoanalyse Erprobungsstrecke an die RBS (SiSt	offen

	SR40)	
01.08.2024	Abgabe Sicherheitsnachweis Erprobungsstrecke an die SiSt SR40	offen

Meilensteine für Lieferungen an das Programm smartrail 4.0:

Datum	Meilenstein	Status
05.10.2018	Zweite Kommentierung zur Zulassungsfähigkeit durch die SiSt SR40	erledigt
01.06.2019	Dritte Kommentierung zur Zulassungsfähigkeit durch die SiSt SR40	erledigt
15.04.2020	Vierte Kommentierung zur Zulassungsfähigkeit durch die SiSt SR40	offen
01.08.2020	Bewertung Draft Risikoanalysen durch die RBS (SiSt SR40)	offen
01.05.2021	Validerungsbericht Phase 4 generische Anwendungen durch den Validierer	offen
01.05.2021	Bewertung Risikoanalyse Phase 4 durch die RBS (SiSt SR40)	offen
01.08.2021	Gutachten Phase 5 generische Anwendungen durch die SiSt SR40	offen
01.02.2022	Validierungsbericht Phase 4 Erprobungsstrecke durch den Validiereroffen	offen
01.04.2022	Gutachten Phase Planung Erprobungsstrecke durch die SiSt SR40	offen
01.05.2024	Validierungsbericht Phase 9 generische Anwendungen durch den Validierer	offen
01.07.2024	Validierungsbericht Phase 9 Erprobungsstrecke durch den Validierer	offen
01.07.2024	Bewertung Risikoanalyse generische Anwendungen durch die RBS (SiSt SR40)	offen
01.08.2024	Gutachten generische Anwendung durch die SiSt SR40	offen
01.09.2024	Bewertung Risikoanalyse Erporbungsstrecke durch die RBS (SiSt SR40)	offen
01.10.2024	Gutachten Erprobungsstrecke durch die SiSt SR40	offen
01.01.2025	Betriebsbewilligung Erprobungsstrecke durch das BAV	offen

7 Lebenszyklen und deren Prozesse

Wie in Kapitel 3 bereits beschrieben, ist in smartrail 4.0 der RAMS-Lebenszyklus nach EN 50126 anzuwenden. Je nach Typ der Entwicklung ergibt sich ein bestimmter Bezug des Entwicklungsprojektes zu diesem RAMS-Lebenszyklus.

Durch den RAMS-Lebenszyklus werden Entwicklungsergebnisse (Artefakte) im Laufe der Entwicklungen zueinander in Beziehung gesetzt, also beispielsweise wird eine Subsystemanforderung derjenigen Systemanforderung zugeordnet, der sie entspringt. Der Nachweis der Einhaltung des RAMS-Lebenszyklus erfordert, dass diese Beziehungen aufgezeigt werden können. Dies wiederum erfordert, dass mit der Aktualisierung der Entwicklungsergebnisse, die Aktualisierung der Beziehungen und der verknüpften Entwicklungsergebnisse durchgeführt wird und nachvollziehbar ist.

Die geforderte Aktualisierung ist nur über definierte Prozesse zu erreichen, die sicherstellen, dass ein Entwicklungsergebnis nur den Zielstatus erlangt, wenn die Abstimmung mit den verknüpften Entwicklungsergebnissen erfolgt ist. Die Sicherstellung soll werkzeuggestützt mit dem Application Lifecycle Management"-Werkzeug "Polarion" erfolgen. Der Nachvollzug des RAMS-Lebenszyklus kann damit grundsätzlich automatisiert erfolgen.

Die Prozesse sind ein Schlüsselfaktor der sicheren Entwicklung und müssen ihrerseits den zuvor beschriebenen Ansprüchen genügen. Die Entwicklung der Prozesse ist deshalb in smartrail 4.0 ein eigenes Projekt, das Projekt "SPM".

7.1 SPM - smartrail 4.0 Process Model

Das Projekt "Smartrail 4.0 Process Model" (SPM) definiert die Prozesse innerhalb der Entwicklungsprojekte, zwischen den Entwicklungsprojekten und auf Programmebene. Es legt damit fest, welche Arbeitsergebnisse wie und durch wen zu erbringen sind.

SPM zentralisiert die Informationen rund um Prozesse und Methoden konsistent und gegenseitig abgestimmt. Die SPM-relevanten Informationen werden dabei einheitlich anhand einer definierten Methode modellbasiert in einem zentralen Repository zuhanden aller Projekte in smartrail 4.0 festgehalten.

Das bereitgestellte, generisch zu nutzende Prozessmodell, wird schrittweise entwickelt.
Für detailliertere Informationen zu SPM resp. den in SPM definierten Prozessen wird an dieser Stelle auf SPM Management & Organisation verwiesen.

7.1.1 Safety Mangement in der Anwendung des SPM

Die SPM-Prozesse gelten für alle Projekte, die als sicherheitsrelevant eingestuft werden (siehe Kapitel 5.1). Diese Projekte haben alle einen Bezug zum RAMS-Lebenszyklus nach EN 50126. Allerdings ist dieser Bezug nicht für alle Typen von Projekten gleich, so dass die Prozesse folgende Eigenheiten aufweisen:

- Die Auswahl des "Entwicklungsweges" in einem Prozess kann durch den Typ des Projekts vorgegeben sein.
- Ein Entwicklungsweg kann eine Verzichtserklärung bzgl. bestimmter Prozesse oder Prozessschritte beinhalten.
- Es kann Aktivitäten geben, die die Methodenbestimmung den Anwendern, also den Projekten überlässt.

Durch Kontrollen, die selbst Gegenstand der Prozesse sind, ist abgesichert, dass das Projekt einen geeigneten und zulässigen Entwicklungsweg wählt. Ferner sind safety-eigene Aufgaben ebenfalls in den Prozessen abgebildet. Das Safety Management in der Anwendung des SPM, d.h. in den Projekten, findet also durch die Anwendung des SPM statt.

7.1.2 Prüfung der Einhaltung des RAMS-Lebenszyklus

Ein spezielle Form der Kontrolle in der Anwendung des SPM ist die Kontrolle über die Einhaltung des RAMS-Lebenszyklus. Diese Kontrolle ist im SPM ein eigener Prozess. Der RAMS-Lebenszyklus selbst ist aber kein eigener Prozess im SPM. Dies ist dadurch begründet, dass der RAMS-Lebenszyklus in der einzelnen Phase viele parallele Aufgaben vorsieht, von denen sich einige in weiteren Phasen wiederholen. Die "Deliverables" einer Phase werden also nicht in einem gemeinsamen Prozess entwickelt, sondern können verschiedenen Prozessen entspringen. Entscheidend für den Stand des Phasenabschlusses ist, ob die Deliverables in der Tiefe, die die Phase verlangt, existieren.

7.1.3 Grenzen der SPM-Prozesse hinsichtlich des RAMS-Lebenszyklus

Das SPM alleine ist nicht hinreichend, um den RAMS-Lebenszyklus vollständig zu kontrollieren. Beispielsweise stösst SPM an folgende Grenzen:

- Die Entwicklung von Produkttypen aus den Anforderungen einer Produktklasse heraus, bedingt eine Übergabe der Entwicklungsverantwortung vom Programm smartrail 4.0 an Lieferanten. Diese haben eigene Prozesse und werden folglich nicht den SPM-Prozessen

folgen.

- Die generischen Anwendungen sind bahnspezifisch zu bestimmen und zu integrieren. Die einzelnen Bahnen haben eigene Prozesse und werden folglich nicht den SPM-Prozessen folgen.
- Die spezifischen Anwendungen sind aus Sicht des Programms smartrail 4.0 Projektierungen und nicht Entwicklungen im engeren Sinne. Sie müssen sich also in erster Linie nicht an den SPM-Prozessen, sondern am "Integrationsprozess" messen, der erst aus der Entwicklung der generischen Anwendung heraus entsteht.

In einem ersten Schritt müssen die SPM-Prozesse mindestens geeignet sein, die Entwicklung von generischen Anwendungen und Produkten bis zur Phase 5 des RAMS-Lebenszyklus zu unterstützen.

7.1.4 Safety Management in der Entwicklung des SPM

Das programmeigene Safety Management kontrolliert, dass die Anforderungen, die die Normen in Bezug auf den RAMS-Lebenszyklus haben, durch die Prozesse erfüllt werden. Dazu stellt das programmeigene Safety Management Anforderungen an das SPM und kontrolliert deren Erfüllung. Diese Anforderungen berücksichtigen bereits konzeptionelle Grundsätze in der Auslegung der Norm, die dem Programm smartrail 4.0 gerecht werden.

Derzeit befinden sich die Anforderungen und die Prozesse noch in der Entwicklung. Sie werden nach der Entwicklung in den nachfolgenden Kapiteln als Referenzen aufgeführt. Konzeptionelle Grundsätze zu den Prozessen sind bereits in den folgenden Kapiteln dargelegt.

7.2 Prozess zur Sicherstellung der personellen Unabhängigkeit

7.2.1 Konzeptionelle Grundsätze

Die personelle Unabhängigkeit muss für Verifizierer, Validierer und Gutachter, die hier summarisch als "Prüfer" bezeichnet werden, sichergestellt werden.

Jede Verifikation, jede Validierung und jedes Gutachten, summarisch als "Prüfung" bezeichnet, braucht eine Beauftragung. Die Unabhängigkeit des Prüfers bezüglich einer Beauftragung muss im Kontext des Durchlaufs des Sicherheitslebenszyklus beurteilt werden.

An die Beauftragung der Prüfung werden Anforderungen an die Unabhängigkeit des Prüfers geknüpft.

Der Prüfer erklärt, die Anforderungen an die Unabhängigkeit zu erfüllen.

Der Safetymanager überprüft die Erklärung der Unabhängigkeit in Bezug auf die einzelne Verifikation oder Validierung im Sinne eines Nachvollzugs der Anforderungserfüllung.

Der Safetymanager legt im Rahmen der Sicherheitsnachweisführung dar,
- dass die Anforderungen an die einzelne Verifikation und Validierung bzgl. Unabhängigkeit angemessen sind, d.h. dass sie insbesondere die Massgabe der EN 50126-2 (2017) erfüllen.
- dass er alle in Bezug auf den Durchlauf des Sicherheitslebenszyklus relevanten Verifikationen und Validierungen in Bezug auf Erfüllung der Unabhängigkeit geprüft hat.

Der Gutachter des Durchlaufs des Sicherheitslebenszyklus überprüft den genannten Aspekt der Unabhängigkeit im Sicherheitsnachweis.

Die Aufsichtsbehörde hat die Aufgabe zu überprüfen, dass der Gutachter unabhängig ist, d.h. dass er insbesondere die Massgabe der EN 50126-2 (2017) bzw. die Unabhängigkeitsanforderungen eines Sachverständigen gemäss der Richtlinie Unabhängige Prüfstellen Eisenbahnen (RL UP-EB) erfüllt.

7.2.2 Anforderungen an den Prozess

tbd

7.2.3 Abdeckung durch SPM

tbd

7.3 Prozess zur Hazard Identifikation und Analysis

7.3.1 Konzeptionelle Grundsätze

Gemäss EN 50126-2, Kap. 5 muss grundsätzlich zwischen der "Gefährdungsermittlung" im Rahmen des Risk Assessments (oberer Teil der Sanduhr in Figure 1) und zwischen der "Gefährdungsermittlung" im Rahmen der Gefährdungsanalyse (unterer Teil der Sanduhr in Figure 1) unterschieden werden.

In Bezug auf den SRP-9768 - Prozess zur Hazard Identifikation und Analysis wird nur die Gefährdungsermittlung im Rahmen der Gefährdungsanalyse betrachtet. Die Gefährdungsanalyse im Rahmen des Risk Assessment wird im Prozess SRP-9769 - Prozess zum Risk Assessment und Risk Management behandelt.

7.3.2 Anforderungen an den Prozess

tbd

7.3.3 Abdeckung durch SPM

tbd

7.4 Prozess zum Risk Assessment und Risk Management

7.4.1 Konzeptionelle Grundsätze

Die Begriffe im "Risk Assessment", wie "Risk Analysis" und "Risk Evaluation" sind für eine offensichtliche gegenseitige Abgrenzung nicht ausreichend selbsterklärend. Zudem werden die Begriffe an verschiedenen Stellen der EN 50126-1 und EN 50126-2 zueinander in Bezug gesetzt. Bei der Definition der Begriffe gilt es der EN 50126-1, Kap. 6.3 und Kap. 7.4.2.1 sowie der EN 50126-2, Kap. 5.2 gerecht zu werden.

Da die Bezeichnungen der Begriffe "Risikobeurteilung" und "Risikobewertung", wie sie in der deutschen EN 50126-1 verwendet werden, in Kapitel 5 der EN50126-2 umgekehrt genutzt werden, sind in smartrail 4.0 stets die englischen Bezeichnungen "Risk Assessment" und "Risk Evaluation" zu verwenden. Um die Abgrenzung zwischen Gefährdungen im Sinne der Sicherheit für Leib und Leben von anderen Gefährdungsbegriffen abzugrenzen, wird im Programm in diesem Kontext von "Hazards" gesprochen.

Ferner ist die Hazardunterscheidung bzgl. der Systemgrenzen nach EN 50126-2, Kap. 5.3 zu berücksichtigen. Hinsichtlich der Projekttypen von smartrail 4.0 bedeutet das, dass im Rahmen des Risk Assessments sowohl Hazards auf Ebene "Bahnsystem" als auch Hazards an der Systemgrenze ermittelt werden.

In der Produktentwicklung liegt der Schwerpunkt der weiteren Analysen im Risk Assessment auf den "Hazards der Systemgrenze", in der Anwendungsentwicklung liegt der Schwerpunkt dieser Analysen dagegen auf der Ebene "Hazards des Bahnsystems".

Die Methode der Gefährdungsermittlung im Rahmen des Risk Assessments ist nicht für alle Projekte gleich, sondern es wird im Prozessablauf über sie entschieden. Folglich sind Auswahl und Anwendung der Methode zwei verschiedene Schritte, die je einem Review unterliegen sollen.

Obwohl viele Tätigkeiten des Risk Assessments sich auf die Hazards im Einzelnen beziehen, muss die Risikobewertung gesamthaft reviewed werden, d.h. einer Expertenmeinung unterliegen. Es muss auch gesamthaft über sie berichtet werden.

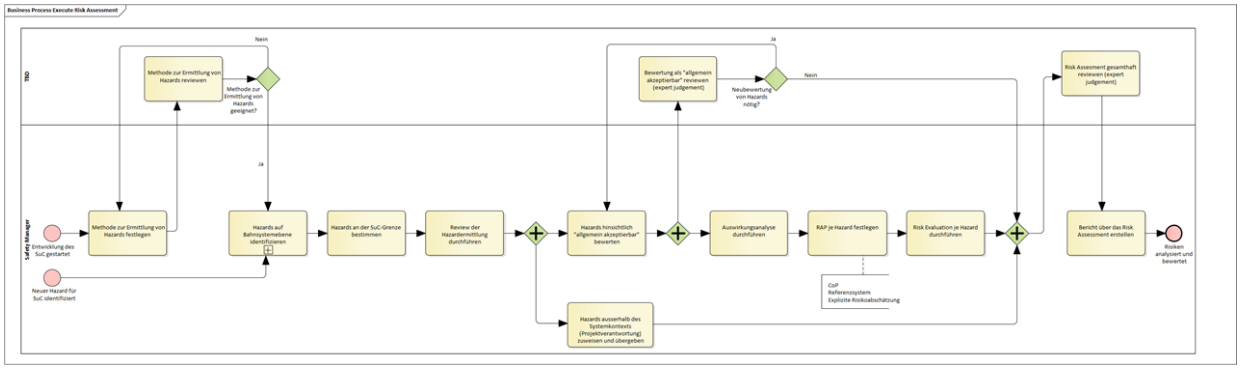
Der Abschluss des Prozesses ist nicht daran gebunden, dass alle Hazards bereits abschliessend beurteilt wurden. Vielmehr wird unter "on-going risk management" verstanden, dass der Prozess des Risk Assessment zu geeigneten Zeitpunkten wiederholt wird. Diese Wiederholungen sollen durch den Prozess zur Kontrolle der Einhaltung des RAMS-Lebenszyklus sichergestellt werden.

7.4.2 Anforderungen an den Prozess

tbd

7.4.3 Abdeckung durch SPM

Der Prozess liegt im Entwurf vor, die konforme Festlegung zu den Anforderungen des Prozesshandbuchs steht noch in weiten Teilen aus. Um einen Einblick in die Art der Prozessdarstellung zu geben, wird der Entwurf hier abgebildet, ohne den Anspruch, das jede Aktivität lesbar ist. Massgebend ist das Process Handbook , ein Report in Polarion.



7.5 Prozess zur Risikoakzeptanz und Überprüfung der Risikoakzeptanz

7.5.1 Konzeptionelle Grundsätze

Das Risikoakzeptanzkriterium ist dem Risikoakzeptanzprinzip "Explizite Risikoabschätzung" untergeordnet.

Eine explizite Risikoabschätzung für Produkte ist im Allgemeinen nicht sinnvoll.

Die explizite Risikoabschätzung wird bei Bahnanwendungen vorgenommen.

Das Risikoakzeptanzkriterium einer Anwendung in smartrail 4.0 besteht aus zwei Teilen:
a) die Unterschreitung eines Grenzwertes eines individuellen Risikos
b) die Minimierung des Verhältnisses aus monetarisiertem kollektivem Risiko und Kosten zur Risikovermeidung

Das Bundesamt für Verkehr (BAV) hat in Zusammenarbeit mit der BLS und SBB ein Handbuch "Akzeptanz individueller Risiken" sowie eine Beschreibung des Vorgehens zur Beurteilung der

Akzeptanz der Risiken der Reisenden und eine Beschreibung des Vorgehens zur Beurteilung der Akzeptanz der Risiken des Personals erarbeitet und veröffentlicht. Diese Dokumente bilden die methodische Grundlage für die quantitative Bestimmung der Risiken. Die für die Anwendung der Methoden notwendigen Grenzwerte ("Safety Targets") sind an Hand der gesetzlichen Vorgaben, der BAV Richtlinien und der BAV Sicherheitspolitik abgeleitet und im Dokument "Safety Targets" *Safety/70_safety/SmartRail 40 Safety Targets* aufgeführt und begründet worden. Die "Safety Targets" wurden mit der Sicherheitsstelle und dem BAV abgestimmt und wurden am 18.07.2018 vom smartrail 4.0 Kernteam als Vorgabe für das Branchenprogramm smartrail 4.0 verabschiedet.

Die explizite Risikoabschätzung erfolgt derart, dass:

- das individuelle Risiko anhand von extremen Konfigurationsdatenwerten der spezifischen Anwendung, aber anhand von durchschnittlichen Wahrscheinlichkeiten für die Folgen der Hazards erfolgt.
- das kollektive Risiko anhand von durchschnittlichen Konfigurationsdatenwerten der spezifischen Anwendung erfolgt
- die Risikoabschätzung herangezogen wird, um generische Konfigurationsdatenwerte ("Systemdaten" genannt) zu optimieren.

Eine solche Risikoabschätzung ist grundsätzlich für die generische Anwendung vorzunehmen, so dass in der spezifischen Anwendung die explizite Abschätzung verzichtbar ist.

Die spezifische Anwendung unterliegt dann keiner expliziten Risikobestimmung, sondern stattdessen einer Konformitätserklärung, dass die Konfigurationsdatenwerte der spezifischen Anwendung den Regeln der generischen Anwendung entsprechen. Diese Regeln spiegeln die Konfigurationsdatenwerte, die bei der Risikobestimmung der generischen Anwendung herangezogen wurden, wieder.

Das Safety Target gilt für die Anwendung von smartrail 4.0 in der Schweiz. Der Prozess muss also vor allem die Aufgabe behandeln, das Safety Target auf untergeordnete generische Anwendungen herunterzubrechen oder aber die Risiken, die auf untergeordneter Ebene ermittelt werden, zu sammeln.

Projektierungsvorgaben optimieren:

- Es muss für jedes Element derjenigen Konfigurationsdaten, die dem Projektierenden Entscheidungsspielraum überlassen, überprüft werden, ob sich mit einer Veränderung des Wertes dieses Konfigurationsdatums vom Grenzwert zu einem höheren Nutzwert des Konfigurationsdatums eine Verbesserung des Verhältnisses aus monetarisiertem kollektivem Risiko und Kosten zur Risikovermeidung erzielen lässt.
- Ist dies der Fall, ist der diesbezüglich optimale Nutzwert des Konfigurationsdatums als ansatzweises Projektierungsoptimum festzuhalten.
- Es ist dann zu überprüfen, ob die angesetzten Projektierungsoptima gegenseitige

Zielwidersprüche enthalten. Ggf. sind sie optimal aufeinander abzustimmen.

- Mit den angesetzten Projektierungsoptima wird erneut mittels der Risikobewertung bestimmt, ob mit ihnen das zulässige individuelle Risiko nicht überschritten wird.
- Wird das zulässige individuelle Risiko überschritten, sind Korrekturen vorzunehmen.
- Wird das zulässige individuelle Risiko nicht überschritten, sind die Grenzwerte der betreffenden Konfigurationsdaten und die Projektierungsoptima als Anforderungen für entsprechende Projektierungsvorschriften festzuhalten.

7.5.2 Anforderungen an den Prozess

tbd

7.5.3 Abdeckung durch SPM

tbd

7.6 Prozess zur Überprüfung der Wirksamkeit von Maßnahmen zur Risikominderung

7.6.1 Konzeptionelle Grundsätze

In der Entwicklung bedeutet das Ergreifen einer risikomindernden Massnahme eine Veränderung der Spezifikationen und folglich eine Anpassung der Gefährdungsidentifikation und Risikoanalyse. Der Prozess umfasst:

1. Bestimmen der Auswirkungen der risikomindernden Massnahme auf Spezifikationen
2. Vornehmen der Spezifikationsänderungen
3. Neuer Durchlauf des Risk Assessments

Der vorliegende Prozess verdeutlicht die Anforderung, Gefährdungsidentifikation und Risikomodellierung in ihren einzelnen Punkten mit den Spezifikationen zu verknüpfen.

Der Prozess zur Überprüfung der Effektivität von risikomindernden Massnahmen im Rahmen in Betrieb befindlicher spezifischer Anwendungen ist Aufgabe des Managements der spezifischen Anwendung, das mit der generischen Anwendung entwickelt wird. Er ist folglich nur insofern im Umfang des vorliegenden Safety Plans, dass der S-Lebenszyklus der generischen Anwendung vorsehen muss, dass der besagte Prozess als Teil der generischen Anwendung erzeugt wird.

7.6.2 Anforderungen an den Prozess

tbd

7.6.3 Abdeckung durch SPM

tbd

7.7 Prozess zur Festschreibung und laufenden Überprüfung der Angemessenheit der Sicherheitsanforderungen

7.7.1 Konzeptionelle Grundsätze

tbd

7.7.2 Anforderungen an den Prozess

tbd

7.7.3 Abdeckung durch SPM

tbd

7.8 Prozess für den Systementwurf

7.8.1 Konzeptionelle Grundsätze

tbd

7.8.2 Anforderungen an den Prozess

tbd

7.8.3 Abdeckung durch SPM

tbd

7.9 Prozess zur Verifikation

7.9.1 Konzeptionelle Grundsätze

Die Verifikation erfolgt stets nach dem gleichen Muster, aber je nach Entwicklungsphase, die es zu verifizieren gilt, werden unterschiedliche Typen von Artefakten geprüft. Es ist daher zu überlegen, die Verifikation als "Process Pattern" festzuhalten.

Das Muster der Verifikation beinhaltet die Schritte:

1. Beauftragung der Verifikation
2. Durchführung der Verifikation
3. Verifikationsbericht erstellen

In der Beauftragung der Verifikation muss deutlich werden, auf welche Entwicklungsphase sich die Verifikation bezieht. Mit dieser Information muss in der Anwendung des Prozessmusters klar sein, welche Artefakte worauf zu überprüfen sind.

Es sind Teilverifikationen möglich, wenn eine Phase als von vornherein nicht abgeschlossen gilt, aber bzgl. des aktuellen Stands überprüft werden soll. Die Beauftragung der Verifikation muss deutlich erkennen lassen, dass eine Teilverifikation beauftragt wird.

Die Beauftragung muss die Unabhängigkeit und die Sachverständigkeit des Verifizierers erklären.

Der Auftrag muss vom Verifizierer und vom Safetymanager bestätigt werden. Dabei darf der Safetymanager die Rolle des Auftraggebers haben. Mit der Bestätigung des Auftrags bestätigen der Safetymanager und der Verifizierer, dass die Begründung der Unabhängigkeit und Sachverständigkeit des Verifizierers stimmt.

Der Verifizierer muss über die Verifikation berichten. Im Bericht muss die Prüfmethode erkennbar sein. Es muss im Fazit deutlich werden, ob eine Verifikation oder eine Teilverifikation erfolgte und ob diese Verifikation erfolgreich war bzw. welche Feststellungen den Erfolg der Verifikation einschränken.

7.9.2 Anforderungen an den Prozess

tbd

7.9.3 Abdeckung durch SPM

tbd

7.10 Prozess für die Validierung, um Übereinstimmung zwischen Systemanforderungen und der entsprechenden Umsetzung zu erreichen

7.10.1 Konzeptionelle Grundsätze

Für die Validierungen gelten grundsätzlich die gleichen konzeptionellen Überlegungen, die zur Verifikation angestellt wurden.

Im Unterschied zur Verifikation findet die Validierung nicht in Bezug auf die Arbeit in einer Phase statt, sondern bezieht sich entweder auf die Prüfung der Zweckmässigkeit der Requirements gegen einen "Intended Use" oder aber auf die Prüfung, dass die Requirements erfüllt sind.

Zudem ist zwischen der Beauftragung und der Durchführung der Validierung ein Validierungsplan zu erstellen.

Der Validierer erstellt seinen Validierungsplan und stimmt ihn mit dem Safetymanager ab, ohne dass der Safetymanager den Plan bestätigen müsste. Verantwortet wird der Validierungsplan vom Validierer allein.

Es ist ein Validierungsbericht zu erstellen, der grundsätzlich die Anforderungen erfüllen muss, die die EN 50126-1:2017 für diesen vorsieht. Bezieht er sich auf andere Phasen muss er die Normanforderungen so weit wie möglich und sinngemäss erfüllen.

Den Validierungsbericht verantwortet der Validierer allein, stellt seine Erkenntnisse aber selbstverständlich dem Projekt zur Verfügung.

7.10.2 Anforderungen an den Prozess

tbd

7.10.3 Abdeckung durch SPM

tbd

7.11 Prozess zur Erreichung der Übereinstimmung des Managementprozesses mit dem Sicherheitsplan

7.11.1 Konzeptionelle Grundsätze

tbd

7.11.2 Anforderungen an den Prozess

tbd

7.11.3 Abdeckung durch SPM

tbd

7.12 Prozess zur Sicherstellung der Sicherheit bei der Parametrierung des Systems

7.12.1 Konzeptionelle Grundsätze

Konfigurationsdatenwerte sind grundsätzlich eine Eigenschaft des SuC (System under Consideration), die im Rahmen der Anwendungsentwicklung festzulegen sind.

Die Prüfung der Einhaltung der entwickelten Konfigurationsdatenwerte ist Gegenstand des Integrationsprozesses, der in Phase 6 des RAMS-Lebenszyklus zu bestimmen ist.

Grundsätzlich muss zwischen generischen Konfigurationsdaten (Systemdaten) und spezifischen Konfigurationsdaten (Engineering Daten) unterschieden werden.

Systemdatenwerte sind solche, die bereits in der Entwicklung der generischen Anwendung, d.h. auf Basis eines abstrakten Systems bestimmt werden können.

Werte der Engineering Daten können dagegen erst durch das System der spezifischen Anwendung bestimmt werden bzw. sind Teil der Bestimmung des spezifisch angewendeten Systems.

Im Allgemeinen ist eine spezifische Anwendung konform zu einer generischen Anwendung und man kann die Entwicklung der spezifischen Anwendung als Integration des SuC der generischen Anwendung betrachten.

Folglich wird die Entwicklung der spezifischen Anwendung mittels des Integrationsprozesses, der in der generischen Anwendung entwickelt wird, standardisiert. Der Integrationsprozess der generischen Anwendung ist also der Entwicklungsprozess der spezifischen Anwendung.

Der Entwicklungsprozess der spezifischen Anwendung muss sicherstellen, dass Werte der Systemdaten realisiert und kontrolliert werden und dass Werte der Engineering Daten bestimmt,

realisiert und kontrolliert werden.

Eine spezifische Anwendung ist grundsätzlich erst dann vollständig bestimmt, wenn alle Werte der Engineering Daten festgelegt sind.

Es gibt Konfigurationsdaten, die beschreiben, wo welche Produkte installiert sind und solche, die beschreiben, wie die installierten Produkte konfiguriert sind. Im Allgemeinen Fall sind beide Formen der Konfigurationsdaten in der spezifischen Anwendung zu bestimmen. Könnte aber die Systeminformationen in der Entwicklung der generischen Anwendung bereits vollständig bestimmt werden, wird eine spezielle generische Anwendung entwickelt, die auch als spezifische Anwendung bezeichnet werden könnte. Unabhängig davon, ob diese Anwendung als generisch oder spezifisch bezeichnet wird, muss ihr Integrationsprozess vorsehen, dass spezifische Parameterwerte bestimmt, realisiert und kontrolliert werden.

7.12.2 Anforderungen an den Prozess

tbd

7.12.3 Abdeckung durch SPM

tbd

8 Einzelheiten zu allen sicherheitsbezogenen Ergebnissen bzw. Liefergegenständen der Lebenszyklusphasen

Die «Deliverables» jeder Phase des RAMS-Lebenszyklus sind in der EN 50126 eigens beschrieben.

Sie sind aus Artefakten, die in der Anwendung des SPM entstehen zu bilden.

Mit der Entwicklung des SPM ist zu entwickeln, welche Artefakte, welche Deliverables bilden.

Es gilt das Zusammenwirken zwischen Safetymanagement und SPM wie es bereits im Zusammenhang mit den Lebenszyklen und Prozessen beschrieben wurde.

9 Prozess zur Erstellung des Sicherheitsnachweises

Der Prozess zur Sicherheitsnachweisführung ist noch nicht festgelegt worden. Folgende Vorgaben wurden bereits erarbeitet:

Die Sicherheitsnachweisführung muss den Ansprüchen der EN 50129 genügen.

Die EN 50129 sieht Sicherheitsnachweise für Produkte, für generische Anwendungen und für spezifische Anwendungen vor.

Für die Sicherheitsnachweisführung der spezifischen Anwendungen gilt die BAV Richtlinie Nachweisführung Sicherungsanlagen (RL SA).

Der Sicherheitsnachweis der spezifischen Anwendung muss vorbehaltlos die Sicherheit der spezifischen Anwendung aufzeigen, bevor diese in Betrieb gesetzt werden darf. Der Sicherheitsnachweis darf sich dabei auf die Sicherheitsbegründung von generischen Anwendungen stützen.

Der Sicherheitsnachweis der generischen Anwendung stellt der spezifischen Anwendung eine Sicherheitsbegründung zur Verfügung, sofern diese konform zur generischen Anwendung ist. Er weist nach, dass diese Sicherheitsbegründung verlässlich ist.

Die Sicherheitsbegründung, die die generische Anwendung bietet, ist grundsätzlich für die spezifische Anwendung als alleinige Sicherheitsbegründung nicht ausreichend. Im Sicherheitsnachweis der spezifischen Anwendung ist mindestens zusätzlich die Konformität zur generischen Anwendung nachzuweisen. Der Sicherheitsnachweis der generischen Anwendung setzt dazu die Einhaltung bestimmter Anwendungsbedingungen voraus, die im Sicherheitsnachweis der spezifischen Anwendung nachgewiesen wird. Die Anwendungsbedingungen können so formuliert sein, dass sie zusätzliche Sicherheitsbegründungen erfordern.

Der Integrationsprozess der generischen Anwendung und damit der Entwicklungsprozess der spezifischen Anwendung soll ausweisen, wie der Sicherheitsnachweis der spezifischen Anwendung zu erbringen ist.

Der Sicherheitsnachweis eines Produkts besteht im wesentlichen aus dem Sicherheitsnachweis eines Produkttyps. Dieser weist nach, dass ein Produkt des Typs die Eigenschaften erfüllt, die der Typ dem Produkt zuschreibt. Er muss sich auf einen bestimmten Fertigungs- und Prüfprozess stützen, der gewährleistet, dass eine Produktinstanz verlässlich als konform zum Produkttyp erklärt werden kann. Die Konformitätserklärung der einzelnen Produktinstanz dient dann als eine der Sicherheitsbegründungen der spezifischen Anwendung.

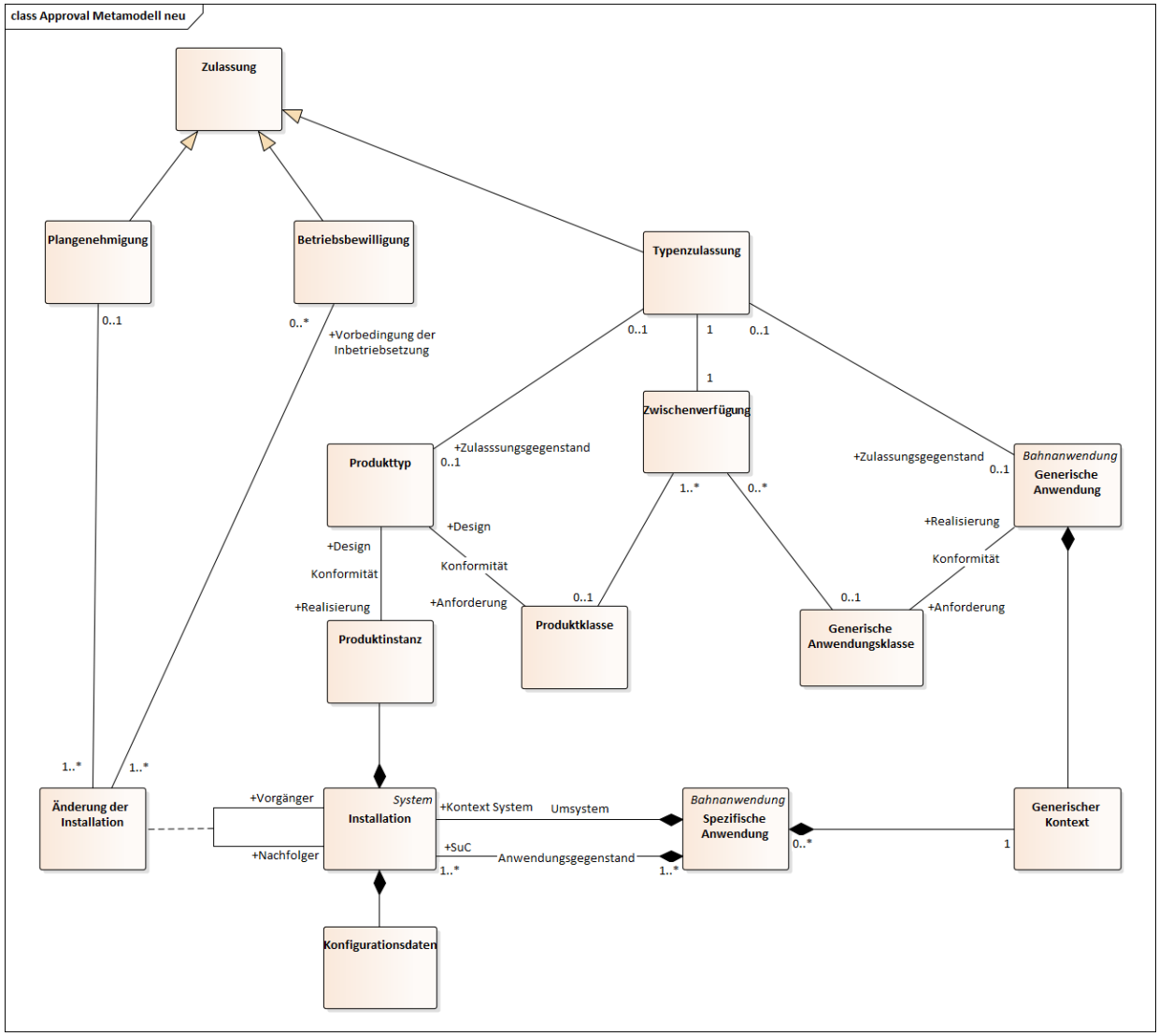
Werkzeuge, SW und Produktklassen benötigen keinen Sicherheitsnachweis nach EN 50129. Da sie aber zur Sicherheitsbegründung der genannten Sicherheitsnachweise herangezogen werden, benötigen sie die Dokumentation ihres Beitrags zur Sicherheitsbegründung und den Nachweis darüber, dass dieser Beitrag verlässlich geboten wird. Diese Dokumentation kann im Rahmen des Sicherheitsnachweises der generischen Anwendung erfolgen.

10 Prozess für die Sicherheitszulassung

Drei Arten der Zulassung sind zu unterschieden:

1. Plangenehmigung
2. Betriebsbewilligung
3. Typenzulassungen

Sie sind im Zusammenhang der verschiedenen Arten von Zulassungsgegenständen nachfolgend abgebildet:



10.1 Zulassung von spezifischen Anwendungen in der Schweiz

Für die Zulassung von spezifischen Anwendungen in der Schweiz gilt die BAV Richtline "Anforderungen an Planvorlagen" (RL VPVE).

Eine Art der Zulassung von spezifischen Anwendungen ist die Plangenehmigung.

Der Gegenstand der Plangenehmigung eine Änderung der Installation der spezifischen Anwendung.

Eine Plangenehmigung kann verschiedene Änderungen der Installation umfassen, weil verschiedene Änderungen einen inhaltlichen Zusammenhang haben können wegen des gemeinsamen Zwecks, insbesondere bei aufeinanderfolgenden Bauphasen.

Unter Berufung auf fachbereichsspezifische Richtlinien (z.B. RL SA) kann gegebenenfalls auf eine Plangenehmigung verzichtet werden.

Eine Zulassung der Änderung der Installation ist nur möglich, wenn auch die Entwicklung

derjenigen Installationen, die die Kontextsysteme bilden, entsprechend entwickelt wurden und der generische Kontext (Mitarbeiterpool und Anleitungsbibliothek) weiterhin geeignet ist, der spezifischen Anwendung gerecht zu werden.

Eine zweite Art der Zulassung ist die Betriebsbewilligung.

Die Betriebsbewilligung ist eine Voraussetzung zur Inbetriebnahme der Anwendung.

Es wird bereits in der Plangenehmigung festgehalten, ob eine Betriebsbewilligung notwendig ist.

10.2 Typenzulassungen

Der Typenzulassungsprozess ist in der entsprechenden Richtlinie des BAV (RL TZL) zur Zulassung von Elementen von Bahnanlagen beschrieben bzw. in der Richtlinie Zulassung Eisenbahnfahrzeuge.

Grundsätzlich dient die Typenzulassung dazu, die Zulassung der einzelnen spezifischen Anwendung bzw. des einzelnen Fahrzeugs zu vereinfachen.

10.2.1 Typenzulassung von Produkttypen

Mit der Typenzulassung des Produkttyps hat der Anwender die Gewähr, dass ein Produkt, das konform zum Produkttyp ist, seine bestimmten Eigenschaften besitzt.

Die Typenzulassung ist daher eine Vereinfachung in der Zulassung der spezifischen Anwendung, da die Erfüllung der Produkteigenschaften nicht in jeder spezifischen Anwendung einzeln nachgewiesen werden muss, sondern mit der Typenzulassung einmalig für alle spezifischen Anwendungen nachgewiesen wurde.

Die Produktklasse ist eine Anforderungsspezifikation für den Produkttyp. Für Anforderungsspezifikationen sieht das Typenzulassungsverfahren vor, dass eine Zwischenverfügung vergeben werden kann. Davon soll im Fall der Produktklasse Gebrauch gemacht werden, d.h. im Rahmen der Typenzulassung des Produkttyps wird eine Zwischenverfügung zur Produktklasse erwartet.

Da die Entwicklung der Produktklasse nicht zwingend in der Verantwortung des Produkttypverantwortlichen erfolgt, ist es wichtig, diese Zwischenverfügung und auch die damit verbundenen Korrekturen in der Entwicklung der Produktklasse in den Verantwortungsbereichs des Entwicklers der Produktklasse zu legen.

Der Verantwortliche der Entwicklung der Produktklasse muss mindestens für einen positiven Validierungsbericht der Produktklasse sorgen.

Es wird vorausgesetzt, dass die Zwischenverfügung eines Typenzulassungsverfahrens als Grundlage für weitere Zwischenverfügungen herangezogen wird, sofern sich diese

Typenzulassungen auf die gleiche Produktklasse beziehen.

10.2.2 Typenzulassung von generischen Anwendungen

Mit der Typenzulassung der generischen Anwendung hat der Anwender die Gewähr, dass die Sicherheitsbegründung, die die generische Anwendung bietet, verlässlich ist und zum Sicherheitsnachweis der spezifischen Anwendung herangezogen werden darf, sofern die spezifische Anwendung konform zur generischen Anwendung ist.

Die Konformität wird über die Einhaltung derjenigen Anwendungsbedingungen nachgewiesen, die sich von der generischen Anwendung an die spezifische Anwendung richten.

Die generische Anwendung ist hoch veränderlich, insbesondere gekennzeichnet von einem regen Wechsel des "Mitarbeiterpools" durch Ein- und Austritte beim Personal, aber auch durch stetige Veränderungen im Regelwerk. Solche Veränderungen müssen möglich sein, ohne dass es zwingend einer neuen Zulassung bedarf. Daher muss es auch Anwendungsbedingungen der generischen Anwendung geben, die sich nicht an die spezifische Anwendung, sondern an den Umgang mit Veränderungen der generischen Anwendung richten, um so zu steuern, welche Veränderungen der generischen Anwendung in der Verantwortung des Bahnbetreibers vorgenommen werden dürfen, ohne dass eine neue Zulassung notwendig ist. Zur Zulassung der generischen Anwendung muss der Bahnbetreiber aufzeigen, dass er diese Anwendungsbedingungen strukturell erfüllt, d.h. in der Lage ist, sie umzusetzen.

Die generische Anwendung bildet einen Standard für die spezifischen Anwendungen, d.h. sie ist der Nachweis der "Spezifikationsreife" von spezifischen Anwendungen, wie sie z.B. die RL SA vorsieht. Spezifische Anwendungen, die mit diesem Standard entwickelt (projektiert) werden, sind Standardanwendungen. Dass eine spezifische Anwendung eine Standardanwendung ist, ist eine typische Voraussetzung, um im Plangenehmigungsverfahren die Verzichtbarkeit des Gutachters zu begründen, der nach EN 50126-1 grundsätzlich optional ist. Mit der gleichen Begründung wird in den meisten Fällen die Betriebsbewilligung für verzichtbar erklärt.

In der Analogie zur Beziehung zwischen Produkttyp und Produktklasse kann für die generische Anwendungsklasse eine Zwischenverfügung erwirkt werden. Sie ist aber nicht zwingend, da sowohl die generische Anwendungsklasse als auch die generische Anwendung in den Händen der Schweizer Bahnbetreiber liegt.

10.2.2.1 Typenzulassung von Systemen

Das System, das den Anwendungsgegenstand der generischen Anwendung bildet, wird als solches mit der generischen Anwendung zugelassen. Allerdings handelt es hierbei um ein abstraktes System, weil es durchaus nicht aus Produkttypen, sondern lediglich aus Produktklassen gebildet werden kann.

Ein solches System kann mittels beliebiger Produkte realisiert werden, sofern deren Typen den entsprechenden Klassen genügen. In der Praxis ist es aber sinnvoll zu überprüfen, ob eine Konfiguration aus bestimmten Produkttypen tatsächlich geeignet ist, als gefordertes System aus Produktklassen zu wirken.

Der spezifische Anwender darf sich nur solcher Konfigurationen bedienen, deren Eignung unter Beweis gestellt wurde, die also als solche zugelassen sind. Die Zulassung der Systemkonfiguration aus Produkttypen soll nach dem abgebildeten Konzept erfolgen:

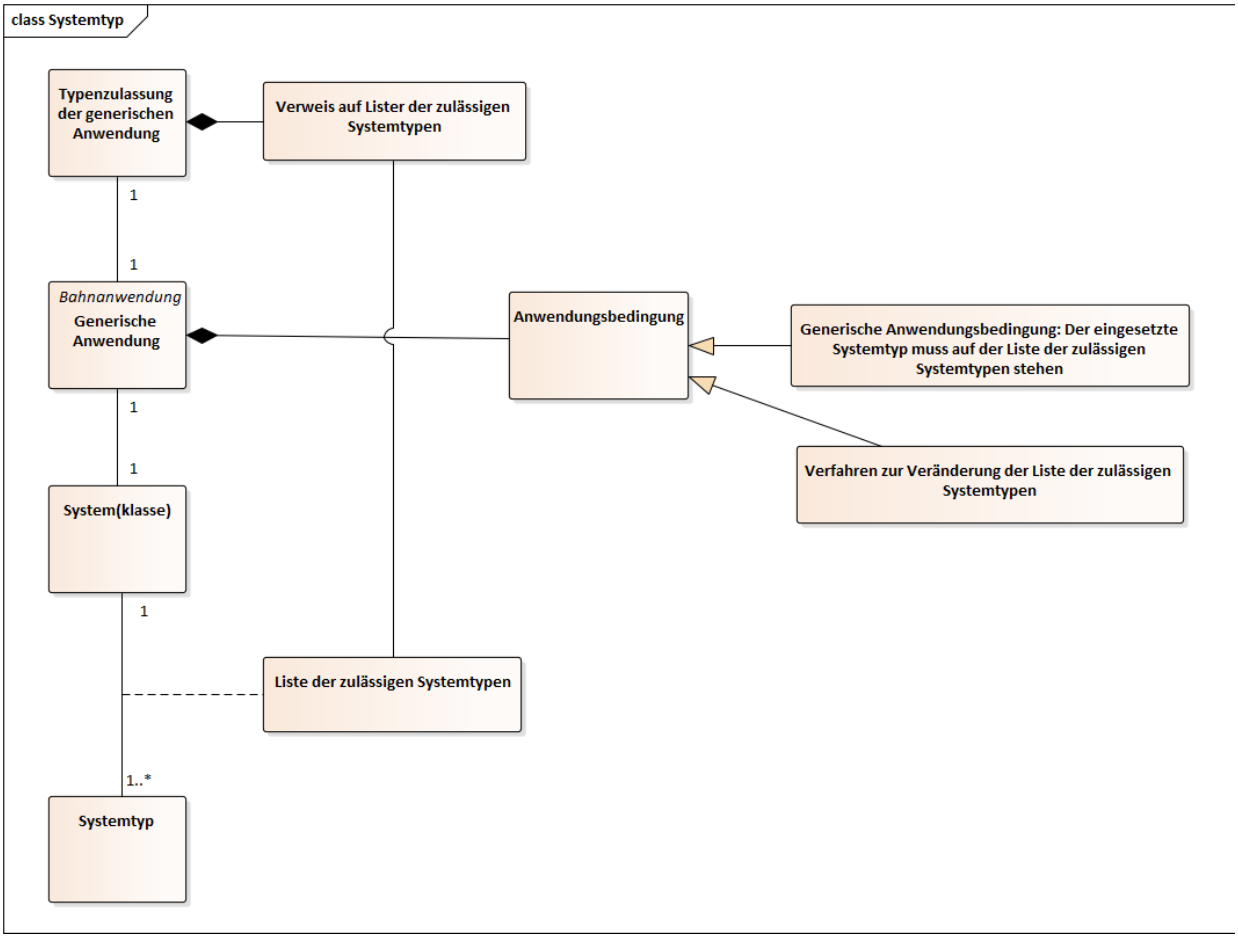


Figure 7 Zulassung von Systemen

Das System, in Abgrenzung zur Konfiguration aus Systemtypen, hier Systemklasse genannt, wird mit der generischen Anwendung zugelassen.

Diese Zulassung soll stets an eine Liste der zulässigen Systemkonfigurationen aus Produkttypen gebunden sein. Eine Systemkonfiguration aus Produkttypen wird hier als "Systemtyp" bezeichnet.

Über eine fixe Anwendungsbedingung der generischen Anwendung soll sichergestellt werden, dass die spezifische Anwendung nur dann konform zur generischen Anwendung ist, wenn der eingesetzte Systemtyp auf der Liste der zulässigen Systemtypen steht.

Mit einer zweiten Anwendungsbedingung der generischen Anwendung soll sichergestellt werden, dass die Zulassung von weiteren Systemtypen vereinfacht gegenüber dem Fall läuft, in dem sich der Systemtyp als solcher noch bewähren musste. Die Anwendungsbedingung gibt ein bestimmtes Verfahren zur Veränderung der Liste der zulässigen Systemtypen vor, das einzuhalten ist.

Das Verfahren zur Veränderung der Liste der zulässigen Systemtypen ist mit der Entwicklung der generischen Anwendung bzw. der Systemklasse zu bestimmen.

10.2.2.2 Typenzulassungen von Werkzeugen

Anwendungsbedingungen der generischen Anwendung, die sich an die spezifische Anwendung richten, können die Verwendung von bestimmten Werkzeugen fordern. Die Werkzeuge sind damit im Rahmen der generischen Anwendung zu diesem Zweck zugelassen.

Es ist anzustreben, Werkzeuge bzgl. der Eigenschaften, die sie für die generische Anwendung qualifizieren, zertifizieren zu lassen, damit sie grundsätzlich in mehreren generischen Anwendungszusammenhängen berücksichtigt werden können.

11 Prozess zur Analyse der Instandhaltungsleistung und des Betriebs

tbd

12 Prozess für die Pflege der sicherheitsbezogenen Dokumentation

tbd

13 Prozess zur Verwaltung der Hazard Logs

Der Prozess zum Mangement der Hazards, die die spezifischen Anwendungen hervorbringen, ist noch nicht definiert.

Grundsätzlich müssen die genannten Hazards betreiberspezifisch erfasst werden und das Safety Management System (SMS) des Betreibers muss dazu ein Hazard Log Management bereitstellen, das die Bearbeitung der Hazard garantiert und den Bezug zu anderen Hazard Logs des Betreibers herstellt.

Ein über die Bahnbetreiber übergreifendes Risk Management der genannten Hazards, mindestens ein Austausch über die aufgetretenen Gefährdungen, ist zu etablieren.

Der Prozess zum Management der Hazard Logs des Programms bzw. der Projekte ist noch nicht definiert.

Der Risk Assessment Prozess für die Projekte gibt vor, welche Informationen ein Hazard Log Eintrag haben muss. Der Risk Assessment Prozess sieht ferner vor, dass sich ein Projekt Risikoanalyse und Risikoevaluation eines Hazards entweder selbst zu eigen machen kann oder den Hazard übergibt. Insofern muss der programmeigene Prozess zum Management des Hazard Logs ein Austausch zwischen den verschiedenen Hazard Logs vorsehen.

Die Hazards müssen über die Programm- bzw. Projektlauflaufzeit hinweg Bestand haben, ganz unabhängig davon, ob sie als geschlossen (beherrscht) gelten oder nicht. Sie sind also spätestens mit Beendigung des Programms oder eines Projektes von den Hazard Logs des Projektes in die Hazard Logs der Bahnbetreiber zu überführen. Diese Aktivität muss ein entsprechender Prozess vorsehen.

14 Schnittstellen zu anderen in Beziehung stehenden Programmen und Plänen

Die Einführung von smartrail 4.0 hat Einfluss auf viele Bereiche des Bahnwesens. Der Bahnbetrieb wird grundlegend verändert, es wird ein neuer Typ von Sicherungsanlagen eingeführt, das mobile Funknetz wird erneuert, es wird eine Fahrzeugarchitektur vorgegeben, die Systemführerschaft ETCS L2 und die Umsetzung von ETCS in der Schweiz ist betroffen, für Wartung und Instandhaltung eröffnen sich neue Möglichkeiten, ...

Eine Abstimmung mit anderen Programmen und Projekten aber auch mit den Lifecycle Managern der betroffenen Systeme, der Systemführerschaft ETCS L2 und dem Operation Center Technik SBB (OCT SBB) ist daher unerlässlich. Bereits mit der Besetzung der Mitglieder

des Kernteams (erweiterte Programmleitung) wurde dem Abstimmungsbedarf Rechnung getragen: Alex Brand verfügt als ehemaliger Anlagenmanager des Bereichs Telekom über entsprechende Kontakte. Martin Messerli hat über viele Jahre das Lifecycle Management der Sicherungsanlagen und über einige Jahre auch das Lifecycle Management der Zugbeeinflussung geführt. Im Bereich Personenverkehr Operations wurde die Einheit P-O-AM-SR40 gegründet, die von Markus Blass, einem langjährigem Mitarbeiter aus dem Bereich Personenverkehr, geführt wird. Markus Blass nimmt ebenfalls regelmässig an den Kernteammeetings teil. Mit Martin Leu und Daniel Schnetzer von der BLS und Ivo Abrach von der SOB werden die anderen Bahnen der Bahnbranche im Kernteam vertreten.

Aus den verschiedenen smartrail 4.0 Projekten heraus erfolgt ein regelmässiger Austausch mit der betroffenen Linie. Beschaffungsstrategien (z.B. mit dem Bereich I-AT-SAZ) aber auch technische Lösungsansätze und Nachweisverfahren (z.B. mit dem Bereich SBB Cargo) werden abgestimmt. Auch bezüglich der Querschnittsthemen Safety, Security, RAM und Regulationen erfolgt ein Austausch mit der Linie.

Der Austausch auf Managementebene erfolgt durch die Steuerungsausschüsse und den Lenkungsausschuss:

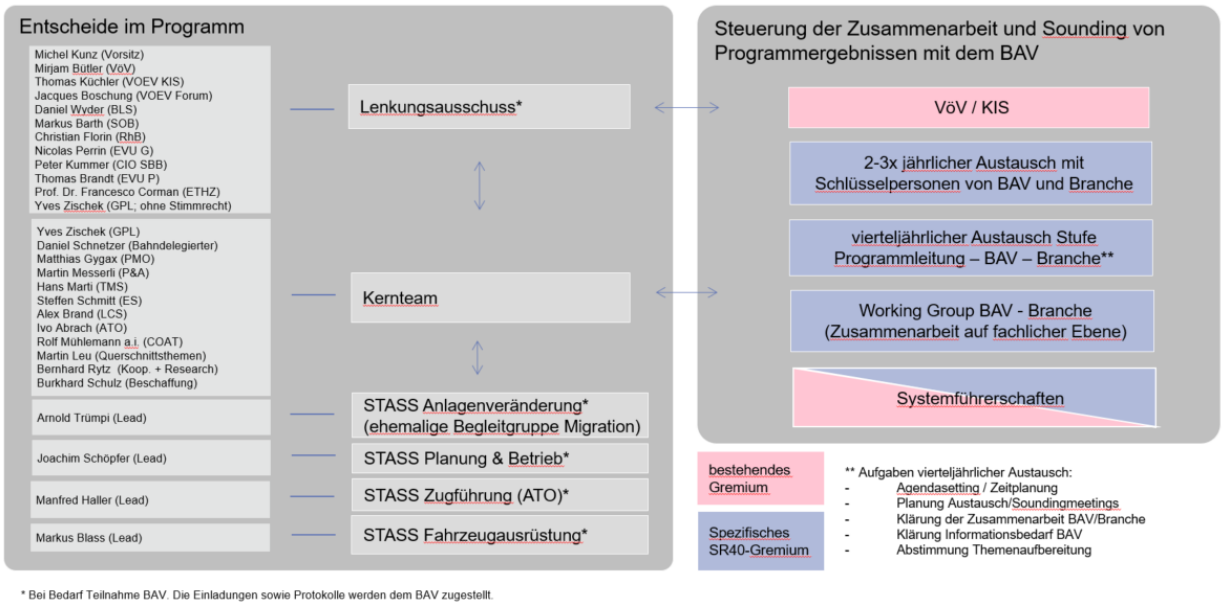


Figure 8: Programmsteuerung smartrail 4.0, Stand August 2019

Der enge Kontakt mit den anderen Bereichen in der Branche soll sicherstellen, dass smartrail 4.0 von anderen Programmen und Projekten erfährt, die an ähnlichen oder gleichen Themen arbeiten oder von den Entwicklungen in smartrail 4.0 betroffen sind. Ist das der Fall, wird aus smartrail 4.0 heraus der Kontakt mit den Projekten gesucht um eine Abstimmung der Projektaktivitäten vorzunehmen.

15 Einschränkungen und Annahmen

Alle Einschränkungen und Annahmen sind in den jeweiligen Kapiteln aufgeführt werden. Aktuell liegen darüberhinaus keine Einschränkungen und Annahmen vor.

16 Vorkehrungen zur Einbindung von Unterauftragnehmern

Dieser Aspekt muss von den einzelnen Projekten aufgegriffen werden. Er ist im Kontext dieses Safetyplans nicht relevant.

17 Regelmässige Sicherheitsaudits, Sicherheitsbewertungen und Sicherheitsüberprüfungen

tbd

18 Glossar

Term	Abbrev.	Description
Advanced Protection System	APS	ETCS FSS basiertes Stellwerk, welches das RBC umfasst. Über seine dynamische, regelbasierte und geometrische Sicherheitslogik steuert das APS alle Bewegungen von Objekten und Veränderungen an den Aussenanlagen innerhalb des Wirkbereichs. Sämtliche betrieblichen Steuerungsaufgaben sind in die übergeordneten Systeme verschoben.
Anwendung		Die Anwendung beschreibt den Einsatz eines Systems in einer Umgebung. Sie ist damit eine zielgerichtete Einschränkung der Freiheitsgrade des Systems hinsichtlich seiner Umwelt und seines Verhaltens. Das System ist dabei Teil der Anwendung.
Application Lifecycle Management	ALM	Lifecycle Management ist eine Kombination aus der Entwicklung und Betreuung von Anwendungssoftware über deren gesamten Lebenszyklus. Dies beinhaltet auch eine umfassende Anwenderbetreuung und die Weiterentwicklung

		der Software. SR40 verwendet das Polarion Application Lifecycle Management System von Siemens PLM Software.
Artefakt		Ein Artefakt repräsentiert ein Ergebnis aus einem Arbeitsprozess. Ein Artefakt ist durch menschliche oder technische Einwirkung entstanden, in Abgrenzung zum unbeeinflussten oder natürlichen Phänomen. Beispiele für solche Ergebnisse sind Dateien mit Quellcode als Ergebnis eines Softwareentwicklungsprozesses oder ein Textdokument als Ergebnis der Definition von Anforderungen an ein System.
Aussenanlage	AA	Aussenanlage, z.B. Weiche, Bahnübergang etc.
Automatic Train Operation	ATO	Der automatische Zugbetrieb besteht aus 5 Automatisierungsstufen (GoA 0 - GoA 4) • GoA 0 ist ein auf Sicht Zugbetrieb, ähnlich einer Straßenbahn im Straßenverkehr. • GoA 1 ist ein manueller Zugbetrieb, bei dem ein Triebfahrzeugführer das Starten und Stoppen, den Betrieb von Türen und die Handhabung von Notfällen oder plötzlichen Umleitungen steuert. • GoA 2 ist ein halbautomatischer Zugbetrieb (STO), bei dem das Starten und Stoppen automatisiert ist, aber ein Fahrer bedient die Türen, fährt bei Bedarf den Zug und bewältigt Notfälle. Viele ATO-Systeme sind GoA 2. • GoA 3 ist ein fahrerloser Zugbetrieb (DTO), bei dem das Starten und Stoppen automatisiert erfolgt, aber ein Zugbegleiter die Türen bedient und den Zug im Notfall fährt. • GoA 4 ist ein unbeaufsichtigter Zugbetrieb (UTO), bei dem Start und Stopp, Türbetrieb und Notfallbehandlung vollautomatisch und ohne Zugpersonal erfolgen
Automatic Train Protection	ATP	Wenn ein Zug mit ATP (Automatische Zugsicherung) gesteuert wird, stoppen Systeme (streckenseitig und bordeigen) den Zug, bevor er seine reservierte Strecke verlassen kann oder zu schnell ist.

		ATP gibt es mit unterschiedlichen Funktionalitäten und Sicherheitsstufen. ATO GoA1 ist normalerweise ein ATP-Zugbeeinflussungssystem.
Automatisierung Warnprozesse	AWAP	Über mobile Warnanlagen sollen Bauarbeiter automatisiert über herannahende Züge gewarnt werden. Dadurch kann Personal eingespart und die Sicherheit erhöht werden.
Automatisierungsgrad	GoA	GoA: "Grade of Automation" bezeichnet den Grad der Automatisierung in der Zugfernsteuerung (ATO). Die Liste der automatisierbaren Tätigkeiten des Lokführers wird in 5 Kategorien ("grade of automation", GoA) unterteilt: GoA 0: Keine Automatisierung, alles liegt in den Händen des Lokführers. GoA 1: Der Lokführer wird an unsicheren Handlungen gehindert (z.B. das Überfahren eines Signals). Dies ist der heutige Automatisierungsgrad bei der SBB und anderen Bahnen. GoA 2: Der Lokführer ist zwar anwesend, während der Fahrt übernimmt aber ein System die Geschwindigkeitssteuerung oder am Bahnhof die Türsteuerung (Autopilot). GoA 3: Im Führerstand ist keine Person mehr anwesend, die meisten Prozesse sind automatisiert. In schwierig zu automatisierenden Situationen (z.B. Fahrt auf Sicht bei Störungen) erfolgt eine manuelle Fernsteuerung z.B. durch den Zugbegleiter oder durch die Betriebszentrale. GoA 4: Alle Prozesse der Zugsteuerung sind automatisiert. Nur noch bei Lokstörungen oder Evakuationen greifen Interventionsgruppen vor Ort ein.
Bundesamt für Verkehr	BAV	Das BAV ist als Aufsichtsbehörde zuständig für den öffentlichen Verkehr in der Schweiz. Dieser basiert auf verschiedenen Verkehrsträgern: Eisenbahn, Seilbahn, Schifffahrt, Tram und Bus. Auch der Güterverkehr dieser Verkehrsträger fällt in den Verantwortungsbereich des BAV. Das BAV ist zuständig für Sicherheit, Finanzierung, Infrastrukturen sowie die rechtlichen und politischen Rahmenbedingungen der Verkehrsträger.
CCS Onboard Application Platform for trackside related	COAT	COAT soll eine modulare und standardisierte CCS-Onboard-Architektur sein, die in SR40 entwickelt wird. Es ermöglicht

functions		beispielsweise die Implementierung eines EVC oder ATO als reine Softwarelösung.
Control-Command and Signalling	CCS	Alle Ausrüstungen, die erforderlich sind, um die Sicherheit zu gewährleisten und die Bewegungen der Züge zu steuern und zu kontrollieren, die zum Fahren auf dem Netz berechtigt sind.
Europäisches Eisenbahnverkehrsleitsystem	ERTMS	Das Europäische Eisenbahnverkehrsleitsystem (ERTMS) ist das System von Normen für das Management und die Zusammenarbeit von Signalanlagen für Eisenbahnen durch die Europäische Union (EU). Es wird von der Agentur der Europäischen Union für Eisenbahnen (ERA) geleitet und ist das organisatorische Dach für die separat verwalteten Teile von • GSM-R (Kommunikation), • Europäisches Zugsicherungssystem (ETCS, Signaltechnik), • European Train Management Layer (ETML, Nutzlastmanagement) Das Hauptziel von ERTMS ist die Förderung der Interoperabilität von Zügen in der EU. Ziel ist es, die Sicherheit deutlich zu erhöhen, die Effizienz des Eisenbahnverkehrs zu steigern und die grenzüberschreitende Interoperabilität des Schienenverkehrs in Europa zu verbessern. Dies geschieht durch den Ersatz früherer nationaler Signalanlagen und Betriebsverfahren durch eine einzige neue europaweite Norm für Zugsteuerungs- und Führungssysteme.
Europäisches Zugsicherungssystem	ETCS	Das Europäische Zugsicherungssystem (ETCS) ist die Signal- und Steuerungskomponente des Europäischen Eisenbahnverkehrsleitsystems (ERTMS). Es ist ein Ersatz für alte Zugsicherungssysteme und soll die vielen inkompatiblen Sicherheitssysteme ersetzen, die derzeit von den europäischen Eisenbahnen eingesetzt werden. Die Norm wurde auch ausserhalb Europas übernommen und ist eine Option für den weltweiten Einsatz.
Future Railway Mobile	FRMCS	Künftiges GSM-R Nachfolgesystem. Die UIC hat die

Communication System		Anforderungsspezifikation abgeschlossen und an die Mobilfunk-Standardisierungsorganisation (3rd Generation Partnership Project 3GPP) übergeben.
Führerstandsignalisierung	FSS	Signalisierung im Führerstand der Lokomotive
Gefährdungsanalyse		Prozess zur Identifikation der Gefährdungen und Analyse ihrer Ursachen, und Herleitung von Anforderungen, um die Wahrscheinlichkeit und Konsequenzen von Gefährdungen auf ein akzeptiertes Niveau zu begrenzen Anmerkung 1 zum Begriff: Ähnliche Prozessaspekte werden auch bei der Risikobeurteilung betrachtet. In der vorliegenden Norm wird dieser Begriff in den Lebenszyklusphasen nach der Festlegung von AnforderungenÂäangewendet. [QUELLE: IEC 60050-821: FDIS 2016, 821-11-23]
Genau lokalisierbare allgemeinverwendbare Endgerätetechnik	GLAT	Der Entwicklungsgegenstand GLAT dreht sich um eine "genau lokalisierbare sichere und allgemeinverwendbare Endgerätetechnik".
Generisches Podukt		Ein (Teil)system oder eine Betrachtungseinheit, welche die bestimmten Anforderungen erfüllt (Produkt) und in verschiedenen Anlagen eingesetzt werden kann (generisch), ist dann ein generisches Produkt, wenn es eine Typenzulassung durch das BAV besitzt und damit klare, allgemeingültige und abschliessende Anwendungsbedingungen für seine sichere Anwendung ausweist.
Infrastrukturbetreiberin	ISB	Infrastrukturbetreiberin und in der Regel Besitzerin von Infrastrukturanlagen für den Eisenbahnverkehr (öffentliches Eisenbahnnetz).
Integration		Prozess des Zusammenfügens der Elemente eines Systems entsprechend der Architektur- und Entwurfsspezifikation und des Prüfens der integrierten Einheit
Lebenszyklus		Abfolge identifizierbarer Stufen, die eine Einheit durchläuft von ihrer Konzeption bis zur Entsorgung BEISPIEL Ein üblicher Lebenszyklus besteht aus: Konzept

		und Pflichtenheft; Entwurf und Entwicklung; Aufbau sowie Installation und Inbetriebnahme; Betrieb und Instandhaltung; Gebrauchswertsteigerung oder Verlängerung der Brauchbarkeitsdauer sowie Außerbetriebnahme und Entsorgung. Anmerkung 1 zum Begriff: Die identifizierbaren Stufen variieren abhängig von der jeweiligen Anwendung. Anmerkung 2 zum Begriff: Für den Fall, dass bei der Gebrauchswertsteigerung oder der Verlängerung der Brauchbarkeitsdauer Änderungen vorgenommen werden, fordert die vorliegende Norm eine erneute Betrachtung des Lebenszyklus. [QUELLE: IEC 60050-192:2015, 192-01-09]
Manoeuvre Train Control	MTC	Manoeuvre Train Control (MTC) ist ein System zur Zugbeeinflussung bzw. Führerstandsignalisierung von Fahrten mit niedrigen Geschwindigkeiten als Ergänzung zu ETCS in von «Full Supervision» nicht abgedeckten Anwendungsfällen. MTC wurde in Funktionsvarianten konzipiert, sodass die Überwachung von Fahrten in niedriger Geschwindigkeit bei bestehenden Technologien (z.B. ETCS L2 mit Gleisfreimeldemittel, ETCS Onboard-Ausrüstung) und die Integration von neuen Technologien (z.B. ETCS L3, genaue Lokalisierung, kostengünstige EVC light Variante) möglich ist.
Object Controller	OC	Der Object Controller verbindet das WI-1657 - Advanced Protection System (APS) mit den WI-2165 - Aussenanlagen (AA) durch Übersetzung der Befehle und Meldungen zwischen APS und AA (z.B. Weichenmotor).
Polarion		Ist die Bezeichnung für das im smartrail 4.0 Kontext eingesetzte Tool für das WI-3960 - Application Lifecycle Management (ALM). Polarion ist eine registrierte Handelsmarke (R) der Siemens AG.
Produkt		Ein Produkt ist ein System, dessen Fertigung und Installation unterscheidbare Arbeitsschritte sind und von verschiedenen Arbeitsgruppen ausgeführt werden können.

		Ein Produkt kann die Instanz eines Produkttyps oder die Instanz einer Produktklasse sein.
Produktklasse		Eine Produktklasse klassifiziert Produkte hinsichtlich der an sie gerichteten Erwartungen. Zum Beispiel alle Produkte, die eine vorgegebene Anforderungsspezifikation erfüllen.
Produkttyp		Der Produkttyp definiert ein Produkt in all seinen Eigenschaften. Der Produkttyp ist damit ein Spezialfall einer Produktklasse. Produkte gleichen Typs sind bzgl. der Entwicklungsergebnisse im RAMS-Lebenszyklus der EN 50126 bis zur Phase 6 identisch und bzgl. Phase 7 in zu entwickelnder Weise gleich.
Prüfen		Ermittlung eines oder mehrerer Merkmale an einem Gegenstand der Konformitätsbewertung nach einem Verfahren Anmerkung 1 zum Begriff: "Prüfen" gilt typischerweise für Werkstoffe, Produkte oder Prozesse. [QUELLE: IEC 60050-902:2013, 902-03-02]
Radio Block Center	RBC	Ist die wesentliche Komponente des European Train Control System (ETCS) in den ETCS-Level 2 und 3. Das RBC generiert die Movement Authority unter Berücksichtigung dynamischer und statischer Informationen und stellt die Schnittstelle der Stellwerke zur ETCS Welt dar.
RAM	RAM	Zuverlässigkeit, Verfügbarkeit und Wartbarkeit. Reliability, Availability und Maintainability (RAM) ist zusammen mit Safety und Security nach der Definition von EN 50126 ein Prozess oder eine Methodik, die mithelfen soll, Fehler schon in der Planungsphase von Projekten zu verhindern. RAM kann angewendet werden bei der Entwicklung und Einführung von neuen Produkten, aber auch bei der Planung und Realisierung von neuen Anlagen.
Risikoanalyse		systematische Auswertung verfügbarer Informationen, um Gefährdungen zu identifizieren und das Risiko einzuschätzen.

		[QUELLE: ISO/IEC Guide 51:2014, 3.10] [QUELLE: IEC 60050-903:2013, 903-01-08]
Risikobeurteilung		Gesamtheit des Verfahrens, das Risikoanalyse und Risikobewertung umfasst [QUELLE: ISO/IEC Guide 51:2014, 3.12] [QUELLE: IEC 60050-903:2013, 903-01-10]
Risikobewertung		auf der Risikoanalyse basierendes Verfahren, nach dem festgestellt wird, ob das vertretbare Risiko erreicht wurde
Safety Integrity Level	SIL	One of a number of defined discrete levels for specifying the safety integrity requirements for safety-related functions to be allocated to the safety-related systems Note 1 to entry: Safety Integrity Level with the highest figure has the highest level of safety integrity. Note 2 to entry: It is not possible to allocate a Safety Integrity Level to safety-related processes or other measures.
Sicherheitsfunktion		Funktion, deren alleiniger Zweck die Sicherstellung der Sicherheit ist Anmerkung 1 zum Begriff: Eine sicherheitsbezogene Funktion ist eine Funktion, deren Ausfall sich nachteilig auf die Sicherheit auswirkt (zu Einzelheiten siehe die Definition von sicherheitsbezogen). Deshalb sind alle Sicherheitsfunktionen sicherheitsbezogene Funktionen, aber nicht alle sicherheitsbezogenen Funktionen sind Sicherheitsfunktionen. Anmerkung 2 zum Begriff: Eine Sicherheitsfunktion kann zu einer oder mehr Sicherheitsbarrieren beitragen. Jedoch wird eine Sicherheitsbarriere nicht notwendigerweise durch eine Sicherheitsfunktion implementiert.
Sicherheitsnachweis		dokumentierter Nachweis, dass ein Produkt (z. B. ein System, ein Teilsystem oder eine Einrichtung) die spezifizierten Sicherheitsanforderungen erfüllt [QUELLE: IEC 60050-821: FDIS 2016, 821-12-53]
Sicherheitsplan		dokumentierte Aufstellung von zeitlich festgelegten Aktivitäten, Hilfsmitteln und Ereignissen, der Einführung einer Organisationsstruktur, von Verantwortlichkeiten, Verfahren, Aktivitäten, Fähigkeiten und Hilfsmitteln dienen und damit

		sicherstellen, dass eine Einheit vorgegebene Sicherheitsanforderungen für einen bestimmten Vertrag oder ein bestimmtes Projekt erfüllt [QUELLE: IEC 60050-821:FDIS2016, 821-12-57]
sicherheitsrelevant		Verantwortung für die Sicherheit tragend Anmerkung 1 zum Begriff: Funktionen, Komponenten, Produkte, Systeme oder Verfahren werden als sicherheitsbezogen bezeichnet, wenn mindestens eine ihrer Eigenschaften in der Sicherheitsargumentation für das betreffende System herangezogen wird. Diese Eigenschaften können funktionsbezogen oder nicht funktionsbezogen sein. Die der Funktion zugeordneten Anforderungen können systematische oder zufällig gewählte Integritätsanforderungen sein. [QUELLE: IEC 60050-821: FDIS 2016, 821-01-73, Anmerkung 1 zum Begriff hinzugefügt]
smartrail 4.0	SR40	Ein Branchen-Programm das die Digitalisierung und die Automatisierung der Bahnproduktion vorantreibt.
Spezifische Anwendung	SA	Die spezifische Anwendung beschreibt vollumfänglich die Bedingungen für den Einsatz eines Systems in einer Umgebung. Damit ist sie die vollständige, zielgerichtete Einschränkung aller Freiheitsgrade des Systems hinsichtlich seiner Umwelt und seines Verhaltens.
Stellwerk		Anlage zur technischen Sicherung der Fahrwege von Zügen und Rangierbewegungen.
Subsystem		Ein Subsystem ist ein System, das ein Teil eines anderen Systems ist.
System		Ein System ist eine Einheit aus einer Menge von Elementen. Die Bildung der Einheit erfolgt immer in einem Kontext. Die Beschreibung des Systems ist an den Systemkontext gebunden
System		set of interrelated elements considered in a defined context as a whole and separated from their environment

		[SOURCE: IEC 60050-351:2013, 351-42-08]
Systemkontext		Der Begriff Systemkontext hat zwei Bedeutungen: 1. Kontext im Sinne der Umgebung: Der Systemkontext ist der Teil der Umgebung eines Systems, der für die Definition und das Verständnis der Anforderungen des betrachteten Systems relevant ist. 2. Kontext im Sinne eines Zusammenhangs: Der Systemkontext ist der Kontext, in dem das System definiert wird (z.B. ein bestimmtes Projekt).
Systems-Theoretic Process Analysis	STPA	Eine Gefahrenanalyse-Technik, die auf der Steuerungs- und Systemtheorie und nicht auf der Zuverlässigkeitstheorie basiert, die den meisten bestehenden Gefahrenanalyse-Techniken zugrunde liegt, mit den gleichen Zielen wie jede Gefahrenanalyse-Technik, d.h. Informationen darüber zu sammeln, wie Gefahren auftreten können.
Topologie		Die Topologie ist eine Repräsentation der Infrastruktur-Anlagen (Weichen, Gleise, Bahnhöfe usw.) auf unterschiedlichem Abstraktionsniveau (typischerweise dem Gleis- & Streckennetz). Geschäftsobjekt-Beschreibung: SRP-9559 - Topologie
Traffic Management System	TMS	Mit dem TMS werden die Fahrpläne und die Disposition automatisiert. Es erfolgt eine optimale und durchgängige Planung über alle Zeithorizonte des Fahrplans. Das TMS steuert WI-3987 - Control-Command and Signalling (CCS)- und WI-1791 - Automatic Train Operation (ATO) Systeme.
Zulassung		Erlaubnis, ein Produkt oder einen Prozess zum angegebenen Zweck oder unter angegebenen Bedingungen auf den Markt zu bringen oder zu nutzen Anmerkung 1 zum Begriff: Die Zulassung kann auf der Erfüllung von festgelegten Anforderungen oder auf der vollständigen Durchführung von festgelegten Verfahren beruhen.

[QUELLE: EN ISO/IEC 17000:2004, 7.1]

[QUELLE: IEC 60050-902:2013, 902-06-01]