Projekt COAT, Zulassungskonzept

Erweiterter Review des Zulassungskonzepts mittels Use Cases

Arbeitsbericht

Version 1.1 I 23.04.2020

Gesamtlösungen sind unser Plus. I Emch+Berger AG Bern
Schlösslistrasse 23 I Postfach I CH-3001 Bern I Tel. +41 58 451 61 11 I bern@emchberger.ch I www.emchberger.ch

Impressum

Auftragsnummer	EBBE-MSB-190015.1.3
Auftraggeber	SBB AG, Programm smartrail4.0
Datum	23.04.2020
Version	1.1
Autor(en)	Raphael Schumacher, EBBE
Freigabe	Freigegeben durch Daniel Bürgi und Dominik Rau, SR40
Verteiler	
Datei	EBBE-MSB-190015.1.3-D1 SR40-COAT-USECASE ARBEITSBERICHT v1.1.docx
Seitenanzahl	52

Inhalt

Zusammenfassung

Im Rahmen des Branchenprogramms smartrail 4.0 erarbeitet das Projekt COAT eine neue modulare Fahrzeugplattform. Dabei sollen die sogenannten Onboard-Funktionalitäten (ETCS, ATO und weitere) neu als Applikationen auf einer gemeinsamen Plattform realisiert werden. Dies ermöglicht ein modularisierbares Zulassungsregime, sowie eine effiziente Wartbarkeit und einfache Erweiterung im Betrieb.

Parallel zur laufenden Entwicklung der COAT-Architektur wird ein entsprechendes Konzept für die Zulassung mit entwickelt. Im Sommer 2019 wurde Version 1.0 des Zulassungskonzepts erstellt. Die in diesem Bericht dokumentierte Arbeit hat zur Aufgabe, das Zulassungskonzept zu reviewen, indem es Use-Case-spezifische Durchstiche durchführt. Die Use-Cases entsprechen zu erwartenden realen Szenarien in einem zukünftigen COAT-Ökosystem. Daraus sollen Erkenntnisse über die Praktikabilität des Zulassungskonzepts gewonnen werden.

Zu Beginn der Arbeit wurden die vorliegende COAT-Architektur und das vorliegende Zulassungskonzept COAT analysiert, sowie insgesamt 36 Use Cases identifiziert, in vier Gruppen aufgeteilt: Erstzulassungen, Änderungen am Basissystem COAT, Änderungen an Peripheriegeräten sowie Änderungen an Applikationen.

Die eigentliche Durchführung des Reviews mittels der Use Cases mündete in eine Matrix, welche die Auswirkungen auf die Safety Cases gemäss Zulassungskonzept analysiert und dokumentiert. Darin wird für jeden Use Case aufgezeigt, inwiefern welche Sicherheitsnachweise tangiert werden und potenziell mit welchem Aufwand überarbeitet werden müssen. Gemäss aktuellem Wissensstand wurde dabei zwischen (aufwändigen) inhaltlichen und (einfacheren) formalen Überarbeitungen unterschieden, sowie ob langfristig mit bleibenden oder - aufgrund zunehmender Reife - zukünftig mit abnehmenden Aufwänden zu rechnen ist.
Aus der Summe der einzelnen Beobachtungen wurden schliesslich die wesentlichen Erkenntnisse gezogen.

Die vorliegende erste Runde des Reviews erfolgte in einem frühen Stadium, da die zugrundeliegende COAT-Architektur und das dazugehörige Zulassungskonzept in Erarbeitung stehen und zahlreiche Aspekte noch im Fluss sind. In diesen Fällen wurden vorläufige Annahmen getroffen. Im Einvernehmen mit dem Auftraggeber wurde die Arbeit dahingehend ausgerichtet, dass sie Anregungen und Anforderungen zuhanden der Verfeinerung des Zulassungskonzepts, zuhanden der technischen Architektur, an die Prüfung (Tests und Automatisierung) sowie an weitere Disziplinen (z.B. Konfigurationsmanagement) liefert.

Mit dieser Version des Arbeitsberichts liegen die Resultate der ersten Iteration vor, bestehend aus Erkenntnissen, Kommentare und Empfehlungen. Diese wurden mit den zuständigen COAT-Projektgruppen besprochen.

1 Einleitung

1.1 Über dieses Dokument

Dieser Arbeitsbericht dient der Dokumentation des Erweiterten Review des Zulassungskonzeptes.

1.2 Aufgabe Erweiterter Review mittels Use Cases

Der Auftrag lautet, fachliche Arbeiten als Bestandteil des Reviews des COAT-Zulassungskonzept zu erbringen, mit Fokus auf Use-Case-spezifischen Durchstichen.

Auf Basis des bestehenden COAT-Zulassungskonzepts sollen erweiterte Betrachtungen und Untersuchungen durchgeführt werden. Der Fokus liegt auf der Praktikabilität der Zulassungsentwürfe für typische Szenarien (Use Cases). Es stehen diejenigen Fahrzeuge/-flotten im Vordergrund, die für SR40 nachgerüstet werden müssen.

Ein Hauptziel ist, die Einflussfaktoren mit Hebelwirkung im Zulassungskonzept zu erkennen und zu überprüfen, in wie weit positiven Auswirkungen in der Praxis zu erwarten sind.

Im Verlaufe der Arbeit wurde im Einvernehmen mit dem Arbeitgeber der Fokus dahingehend ausgerichtet, dass sie Anregungen und Anforderungen zuhanden der Verfeinerung des Zulassungskonzepts, zuhanden der technischen Architektur, an die Prüfung (Tests und Automatisierung) sowie an weitere nahestehende Disziplinen (z.B. Konfigurationsmanagement) liefert, welche anschliessend mit den zuständigen COAT-Projektgruppen besprochen werden.

1.3 Aufbau des Dokumentes

Kapitel 1 führt in die Thematik ein.

Kapitel 2 und Kapitel 3 analysieren den aktuellen Stand der Konzeption des System COAT und sowie des Zulassungskonzeptes. Die Analyse bezweckt unterem anderem auch, temporäre Orientierungspunkte zu identifizieren, die als Arbeitshypothesen für den beauftragten Erweiterten Review und insbesondere für die Durchführung der Use Cases dienen erforderlich ist. Die aktuelle Systemarchitektur COAT in der derzeit noch frühen Projektphase ist noch vage für den Review mit konkreten Use Cases. Mit seiner fortschreitenden Weiterentwicklung werden sich die Arbeitshypothesen entweder bestätigen oder sie werden an die neuen Festlegungen angepasst werden.

Kapitel 4 beschreibt die Use Cases und deren Durchführung, sowie die zugrundeliegenden Annahmen.

Kapitel 5 fasst die gewonnenen Resultate zusammen und identifiziert Optimierungspotenziale und sonstige Diskussionspunkte und Empfehlungen, sowie Vorschläge für nächste Schritte.

Kapitel 6, der Anhang, listet die referenzierten Dokumente auf.

2 Analyse Systembeschreibung COAT

Die im Folgenden vorliegende Beschreibung des Gesamtsystem COAT stützt sich auf vorliegende Dokumentation, insbesondere die Systembeschreibung [Dok.3] und die OCORA-Architektur [Dok.6] ab, sowie auf zusätzlichen – mündlich erhaltenen – Informationen.

Im Vergleich zur OCORA-Architektur [Dok.6] ist die Systembeschreibung [Dok.3] eine vereinfachte – und unschärfere – Beschreibung. Letztere wurde einige Zeit vor der Vorstellung der OCORA-Architektur erstellt. Das gleichzeitig entwickelte Zulassungskonzept [Dok.4] erforderte eine Systembeschreibung, welche es als Referenz verwenden konnte.

Die im Rahmen des europäischen OCORA-Projektes definierte OCORA-Architektur gilt als Vorlage für die Modularisierung der Fahrzeugausrüstungen und liefert erste Grundsätze für die Schnittstellen (allerdings noch nicht konsolidiert). Es lautet die Vorgabe des Bundesamts für Verkehr (BAV), dass COAT von Beginn weg auf einem europäischen Standard, das heisst auf OCORA basieren muss. Die weiterführende Detaillierung der OCORA-Architektur ist in Arbeit.

In diesem Kontext war von Beginn weg klar, dass für den Zweck des Erweiterten Reviews eine Arbeitshypothese erstellt werden muss, indem für diverse Aspekte der Architektur Annahmen getroffen werden. Diese sind in Tabelle 4-5 zusammengestellt. Mit der fortschreitenden Weiterentwicklung der OCORA-Architektur werden sich die getroffenen Annahmen entweder bestätigen oder aber an die neuen Festlegungen anpassen.

2.1 Übersicht Systemarchitektur

Die Systembeschreibung [Dok.3] legt dar, aus welchen COAT-Komponenten das COAT-Gesamtsystem sich zusammensetzt, und auf welchen Beschreibungen und welchen Spezifikationen es basiert. Das OCORA-Dokument [Dok.6] vertieft die Architektur in Bezug auf die eingesetzten hardware- und software-basierten Komponenten. Wie in Abbildung [1] ersichtlich ist, stimmen die beiden Architekturen bezüglich ihrer Hauptfunktionsgruppen überein.

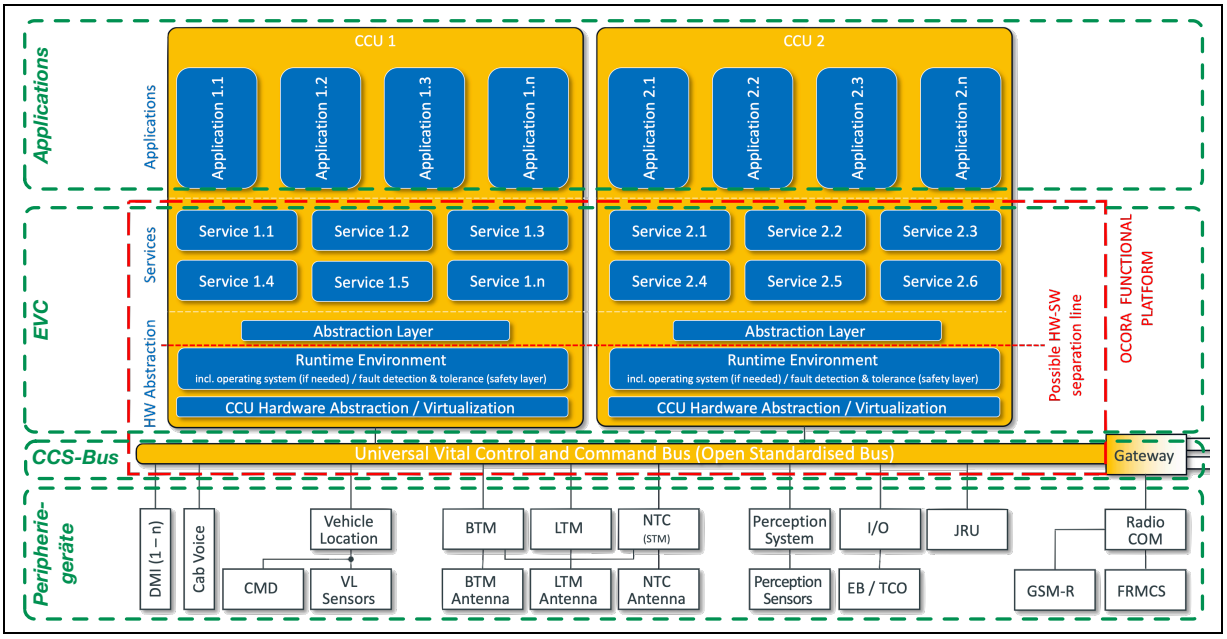

Abbildung 1: Zusammenführung Systemdefinition Enotrac und Systembeschreibung OCORA

Die Kenntnis über die Funktionalitäten in der COAT-Architektur ist für das Durchspielen des Use Cases grundlegend.

Abbildung [Abbildung 2] zeigt die hauptsächlichen Bausteine des Gesamtsystems COAT in vereinfachter Form dar.

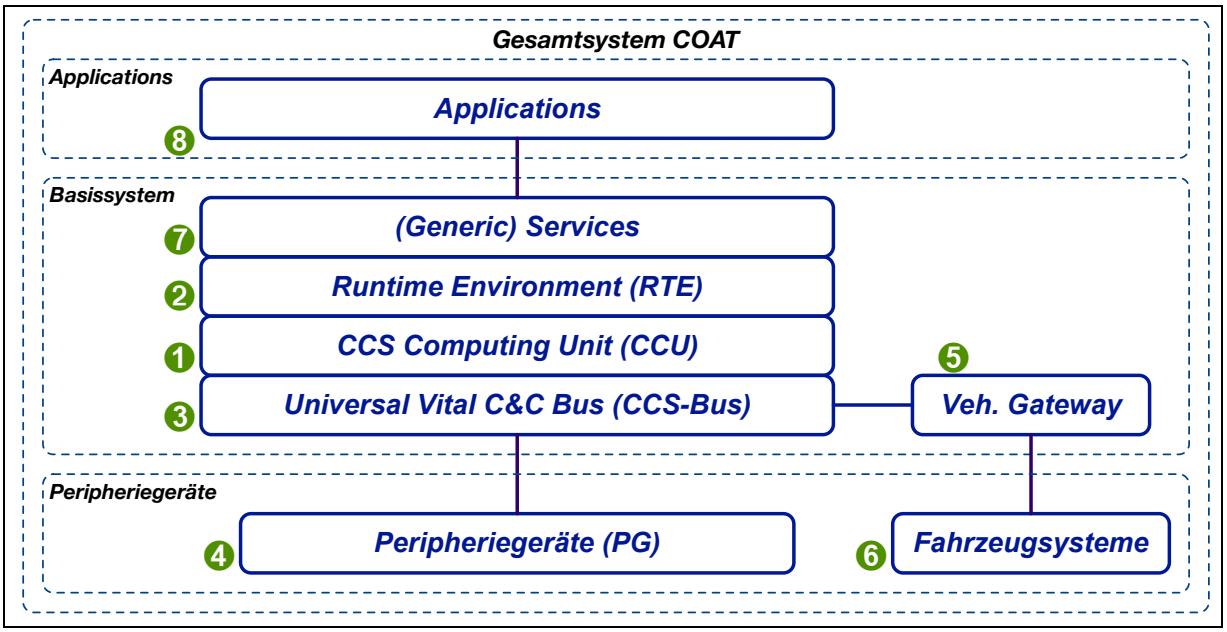

Abbildung 2: Hauptsächliche Bausteine von COAT / OCORA (Eigendarstellung)

Die Bausteine gemäss Abbildung 2 im Einzelnen:

(1) CCU – «CCS computing unit». Die Rechner-Hardware, üblicherweise eine 2oo3-Plattform (2-out-of-3).
Hinweis: die ältere alpha-Version der OCORA-Architektur verwendete den Begriff EVC, welcher bereits für ETCS-Fahrzeugausrüstungen verwendet wird. Mit der Umbenennung zu CCU wurde das potenzielle Missverständnis behoben.

(2) RTE – das Betriebssystem einschliesslich der Abstrahierung der Hardware

(3) CCS-Bus – eine universelle Plattform für Informations- und Datenflüsse zwischen den Komponenten und mit der Aussenwelt.

(4) Peripheriegeräte – eine «Assemblage» von Geräten, die spezifische Aufgaben erfüllen. Beispiele: BTM und LTM, Lokalisierungsgeräte, DMI, JRU.
Weder die OCORA-Architektur noch COAT geben eine konkrete oder minimale Auswahl resp. Zusammenstellung von Peripheriegeräten vor. Dies liegt in der Wahl der Fahrzeugbesitzer (EVUs) und Ausrüstern, von denen die EVUs COAT-Gesamtsysteme oder Teile davon beziehen. Es ist hingegen anzunehmen, dass die in einer COAT-Installation eingesetzten Applikationen (Baustein 8) bestimmen, welche Typen von Peripheriegeräten erforderlich sind (in der Regel als Informationsquellen wie Sensoren erfordern).

(5) Gateway – zur Anbindung des Systems COAT an:
- das Fahrzeug und seine Systeme → siehe (6)
- die Telekomausrüstung zur Kommunikation mit den Infrastrukturen.

(6) Fahrzeugsysteme, insbesondere:
- TIU oder TCO (train control bus) zur Ansteuerung der Bremsen, Traktion, Bezug

von Fahrzeuginformationen wie «Führerstand besetzt» oder «Fahrrichtung» usw.;
- der passenger information bus zur Verfügungsstellung von Fahrgastinformationen.

(7) Generic Services – einheitlich Dienstleistungen zuhanden aller Applikationen.
Z.B. die Aufbereitung kontext-relevanter Informationen (Businessdaten, destilliert aus den von den Peripheriegeräten erhaltenen Rohdaten); standardisierte Ausführung von Massnahmen (z.B. Ansteuerung DMI, Auslösung der Service und Emergency Brake).

(8) Applikationen – realisieren bestimmte betriebliche Zwecke wie z.B.
- VS - vehicle supervision (ETCS-Zugbeeinflussung mit Vollüberwachung)
- ATO - automatisches Fahren
Die Auswahl der benötigten Applikationen wird weder durch die OCORA-Architektur noch die COAT-Plattform vorgegeben. Es liegt in der Kompetenz der EVUs als Fahrzeugbesitzer, die zu verwendenden Applikationen gemäss ihren spezifischen operativen Bedürfnissen zu bestimmen.

2.1.1 Basissystem COAT

Im Zentrum von COAT steht als generischer Systemteil das Basissystem COAT. Es entspricht der «OCORA Functional Platform», wie es in Abbildung 1 rot umrandet wird.

Es umfasst die Bausteine CCU (Nummer 1 in Abbildung 2; zuvor EVC genannt), RTE (Nummer 2), CCS-Bus (Nummer 3), und generische Services (Nummer 7).

Das Basissystem COAT entspricht dem «OCORA Functional Platform» gemäss [Dok.6]. Es besteht aus einer Hardware (namentlich das EVC mit mehreren Rechnern, sog. Channels) sowie aus Software, die einem klassischen Betriebssystem ähneln. Letzteres weist unter anderem auf:

- Die CCU-Hardware und die Runtime-Environment (Abbildung 2, Nummern 1 & 2) decken die Grundfunktionen eines Betriebssystems ab (low level operating system);
- Die Betriebssystemfunktionalität (upper level functionality) bietet generische und standardisierte Services (Abbildung 2, Nummer 7) zuhanden aller Apps und/oder auch an Peripheriegerät an.
- Der CCS-Bus (Abbildung 2, Nummer 3) bietet einen standardisierten Austausch aller denkbaren Daten und Informationen zwischen Peripheriegeräten, dem Basissystem COAT, der Services sowie der Applikationen.
- Der Gateway (Abbildung 2, Nummer 5) bietet die Anbindung an den spezifischen Fahrzeugtyp an. Es deckt die Interaktion des Basissystem COATs mit dem Fahrzeug ab, klammert jedoch die Integration – und namentlich den Einbau – der Peripheriegeräte aus.

2.1.2 COAT Peripheriegeräte

Ziel ist, dass Peripheriegeräte über einen CCS-Bus Informationen mit anderen Komponenten austauschen und kommunizieren. Der CCS-Bus soll gemäss (noch zu wählenden) offenen Standards konzipiert sein.

Die meisten der vorgesehenen Peripheriegeräte (z.B. BTM/LTM, JRU, GSM-R resp. FRMCS etc.) stehen seit bereits geraumer Zeit im Einsatz, unter Verwendung individueller, nur teilweise normierter Schnittstellen. Es wird angenommen, dass die Schnittstellen dieser

Peripheriegeräte auf – noch zu definierende – CCS-Bus-Standards konvertiert werden, damit diese zur neuen COAT-Architektur passen werden (Abbildung 3).

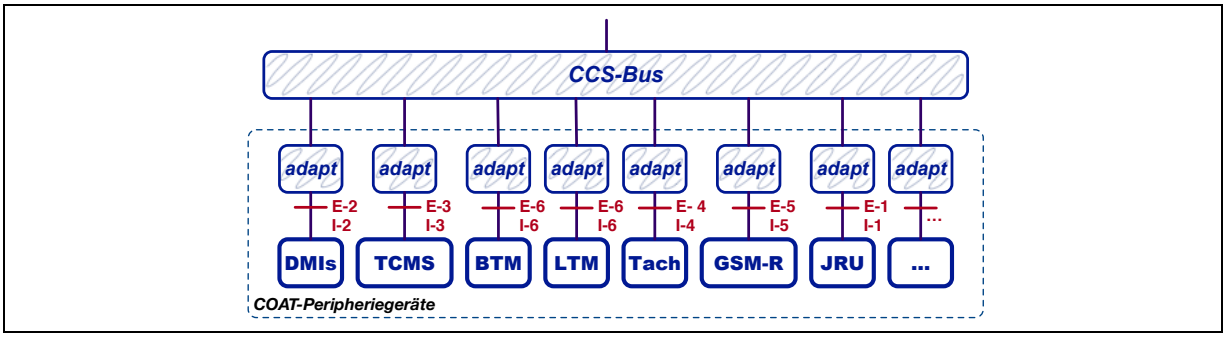

Abbildung 3: Denkbare Anpassung bestehender Peripheriegeräte an de CCS-Bus

Auf die hauptsächlichen Merkmale und Funktionalität des CCS-Busses und der Kommunikation innerhalb COAT wird in Kapitel 2.3 näher eingegangen.

2.2 Zusätzliche Begriffe

Im Folgenden werden zusätzliche Begrifflichkeiten eingeführt, die in diesem Review zur Differenzierung unterschiedlicher Sachverhalte erforderlich sind, zum Zeitpunkt der Arbeit aber dem Vernehmen nach nicht definiert waren.

COAT-Begriff	*Beschreibung*
Gesamtsystem COAT, generisch und spezifisch	Eine Gesamt-Zusammenstellung des COAT-Systems für einen bestimmten Zugstyp, welcher für einen bestimmten Einsatzform (z.B. SR40) vollständig mit Peripheriegeräten und Apps ausgerüstet ist. Ein Gesamtsystem wird zusammengestellt aus: - einem Basissystem COAT, plus - einer Auswahl von Peripheriegeräten, sowie - einer Auswahl von Applikationen. Die Auswahl wird gemäss den Bedürfnissen der Fahrzeugbesitzer getroffen. Ein generisches Gesamtsystem COAT ist noch nicht mit einem bestimmten Fahrzeugtyp integriert noch dafür zugelassen. Ein spezifisches Gesamtsystem COAT ist mit einem bestimmten Fahrzeugtyp integriert und dafür zugelassen.
Basissystem COAT	Gleichbedeutend mit «OCORA Functional Platform» gemäss OCORA-Systembeschrieb [Dok.6]. Das Basissystem COAT steht für generische Plattform COAT ohne Peripheriegeräte und ohne Apps. Es ist jedoch mit allem versehen, um jederzeit mit – ersten oder weiteren – Peripheriegeräten und Apps ergänzt werden zu können. Das Basissystem besteht im Wesentlichen aus der Hardware (EVC COAT), Betriebssystem, Abstraktionslayern und Services.

COAT-Begriff	*Beschreibung*
CCU CCS Computing Unit	Im Kontext von COAT wird an dieser als COAT-Rechner verstanden. Hinweis: der EVC ist der spezifische Begriff für ETCS-Rechner gemäss der TSI CCS, und wurde zu Beginn des COAT-Projekts auch an dieser Stelle verwendet. Um Verwechslungen zwischen COAT- und ETCS Onboard-Rechnern zu vermeiden, wurde im weiteren Projektverlauf an dieser Stelle der Begriff CCU eingeführt.
RTE Runtime Environment	Das auf dem COAT-EVC laufende Betriebssystem für COAT-Anwendungen. Es erlaubt den Einsatz von COAT-Applikationen und stellt diesen eine Anzahl von Grundfunktionen zur Verfügung (z.B. Ansteuerung von Zugsfunktionen wie Traktion und Bremsen; Kommunikation mit den an COAT-Plattform integrierten Peripheriegeräten, usw.).
PG Peripheriegerät COAT	Ein einzelnes, im Fahrzeug eingebautes Peripheriegerät, mit dem Basissystem COAT integriert, welches eine spezifische Anwendung umsetzt (Bsp. mittels der Balisenantenne Eurobalisen lesen und Telegramme auf dem CCS-Bus hinterlegen).
COAT-App, oder COAT-Applikation	Eine einzelne auf der COAT-Plattform lauffähige Applikation, die eine spezifische Anwendung umsetzt. Beispiele sind VS («vehicle supervisor» mit der ETCS fahrzeugseitigen Funktionalität und ATO («automated train operation»).
VS-App Vehicle Supervision	COAT-App, welche die fahrzeugseitige ETCS «vehicle supervision» Funktionalität gemäss der TSI CCS, Subset-026 ff. implementiert (analog zur herkömmlichen ETCS Onboard-Unit).
SiNa Sicherheitsnachweis	Gleichbedeutend mit Safety Case
GASC Generic Application Safety Case	Generischer Sicherheitsnachweis
SASC Specific Application Safety Case	Anwendungsspezifischer Sicherheitsnachweis
Plug-and-play, commodity	Standardkomponenten oder Teilsysteme, in welchen die verwendeten Technologien und Produkte basierend auf Erfahrungswerten soweit gereift haben, dass Integrations- resp. Regressionstests nicht mehr als notwendig erachtet werden (siehe Kapitel 2.4.4).

Tabelle 2-1: Ergänzende Begriffsdefinitionen, soweit für erweiterten Review erforderlich

Hinweis: in den Referenzdokumenten (Tabelle 6-1) werden gleichermassen «Sicherheitsnachweis» (SiNa) und «Safety Case» (SC) verwendet. Die beiden Begriffe gelten als Synonyme.

2.3 Kommunikation innerhalb der COAT-Plattform

Essenziell für eine nachhaltige Modularisierung der COAT-Plattform ist die Konzeption der Kommunikation und des Datenaustausches zwischen den COAT-Komponenten. Es ist demnach in Bezug auf die Wiederzulassung bei Änderungen auch für die Zulassungskonzepte von hohem Interesse.

2.3.1 Standardisierter Datenaustausch über den CCS-Bus

Bezugnehmend auf die siehe alpha-Version der OCORA-Architektur [Dok.6] ist der CCS-Bus für den Datenaustausch vorgesehen. Seine grundsätzlichen Eigenschaften und Funktionsweise (publish-subscribe o.ä.) sind derzeit noch nicht definiert.

Es wird vorerst angenommen, dass die Formate für die Daten über den CCS-Bus nicht besonders spezifiziert und harmonisiert werden. Dies bedingt jedoch, dass eine App genaue Kenntnis hat, in welchen Formaten ein bestimmtes Peripheriegerät seine Daten dem CCS-Bus zur Verfügung stellt. Die App wird daher auf bestimmte Modelle (nicht Typen) von Peripheriegeräten zugeschnitten sein müssen.

Standardisierte Datenformate – vorerst für bestimmte Informationsklassen – würden erlauben, die Beziehung zwischen App und Peripheriegeräten zu abstrahieren. Dies würde einerseits die Integration zwischen App und Peripheriegeräten vereinfachen, und andererseits den Fächer der möglichen Zusammenstellungen von Apps und Peripheriegeräten in einem Gesamtsystem COAT bedeutend öffnen:

- Ein Peripheriegerät stellt Informationen in einem vordefinierten Datenformat auf den CCS-Bus;
- Eine App ruft vom CCS-Bus bestimmte Informationen ab, ohne Kenntnis zu benötigen, welches Peripheriegerät diese Informationen bereitstellt.

Für sichere Anwendungen müssen die zu spezifizierenden Datenformate berücksichtigen, dass Informationsempfänger mit den Daten ebenso ergänzende Angaben (Klassifikationen, Anwendungsbedingungen) erhalten müssen, welche der App Aufschluss geben über die zulässige Nutzung der Daten – falls erforderlich jeweils aktualisiert.

2.3.2 Neu: Schnittstellen innerhalb des COAT-Systems

Die Weiterentwicklung der OCORA-Architektur zur beta-Version [Dok.7] sieht die Einführung standardisierter Schnittstellen vor, welche durch den CCS-Bus vermittelt, koordiniert und auch abgewickelt (Datenkommunikation) werden. Diese Schnittstellen dienen dem Daten- und Informationsaustausch insbesondere zwischen Peripheriegeräten und Applikationen (teilweise auch Services).
In verallgemeinerter Form soll pro Typ von Peripheriegerät ein Schnittstellenstandard definiert, welcher auf einheitliche Art den Informationsaustausch zwischen den betreffenden Peripheriegeräten und den «interessierten» Applikationen ermöglicht:

- Die Peripheriegeräte des Typs X stellen die Schnittstelle ∂ (z.B. delta) auf dem CCS-Bus zur Verfügung.

- Eine Applikation fragt den CCS-Bus nach der Verfügbarkeit von Peripheriegeräten (des Typs X), welche ihre Informationen über die Schnittstelle ∂ zur Verfügung stellen.

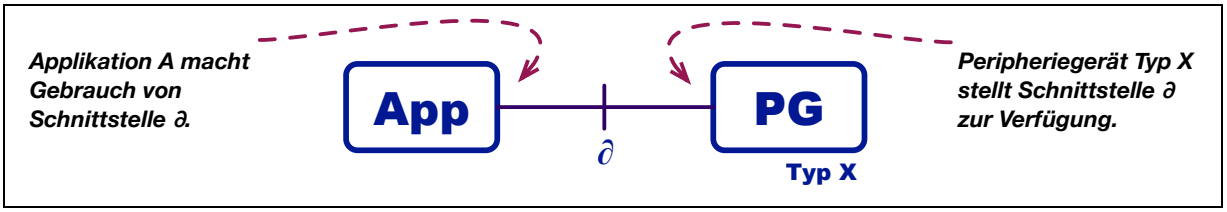

Abbildung 4: Standardisierte Schnittstelle ∂ zwischen zwei Kommunikationspartnern

Aus der Sicht der Zulassung ergeben sich folgende Beobachtungen zum Konzept der Schnittstellen:

(1) Es führt zu einer bedeutenden Entlastung der Anforderungen und der Standardisierung an den CCS-Bus, und somit auch der diesbezüglichen Zulassung. Die Festlegung der spezifischen Datenformate wird Sache der Schnittstellen. Der CCS-Bus kann sich auf die allgemeine Vermittlung und auf die Gewährleistung von Kommunikationsverbindungen zwischen Peripheriegeräten, dem Fahrzeug und den Applikationen beschränken. Die dafür zu erfüllenden Anforderungen sind generisch und erfahren wenig Änderungen im Rahmen des Lebenszyklus eines COAT-Basissystem.

(2) Das Augenmerk der Sicherheitsbetrachtung (z.B. hazard analysis) verschiebt sich deutlich vom CCS-Bus hin zu den einzelnen Schnittstellen. Die Schnittstellen werden gewisse sicherheitsrelevante Kriterien erfüllen müssen, z.B. die Gewährleistung, dass über die Schnittstelle übermittelte Daten entweder gänzlich korrekt oder gar nicht beim Empfänger (typischerweise die Applikation) ankommen werden.

(3) Auch wenn Schnittstellen von Beginn weg einen hohen Reifestand erlangen, werden diese im Verlaufe ihres Lebenszyklus durchaus Änderungen bzw. Korrekturen und Erweiterungen durchlaufen. Um die Wiederzulassung solcher Änderungen zu erleichtern, sollten die Schnittstellen von Beginn weg so konzipiert sein, dass die Verifikation einer Änderung (der Schnittstelle oder einer Seite z.B. am Peripheriegerät Typ X gemäss Abbildung 4) sich möglichst auf die geänderte Komponente beschränken kann.
Zentrale Bausteine hierfür sind die Konzeption und insbesondere das Vorhandensein intelligenter Kompatibilitätsfunktionen in den Schnittstellen, sowie zusätzlich spezifische Anforderungen an die Verifizierung der in Komponenten angewendeten Schnittstellen bereits, welche bereits bei Erstzulassungen zu befolgen sind.

2.4 Anwendung der Verifikation und Sicheren Integration

Den CENELEC-Normen (Dok.8) entsprechend muss in der Spezifikation, Entwicklung, Produktion und Verifikation einer COAT-Plattform der bekannte V-Zyklus durchlaufen werden. Der V-Zyklus beinhaltet einerseits die Aufteilung («Apportionment») des Systems in Teilsysteme und Komponenten, und andererseits müssen die Komponenten und Teilsysteme im Sinne der «sicheren Integration» zu einem Gesamtsystem schrittweise integriert und verifiziert werden.

Für die Durchführung des Reviews ist die Verifikation und Integration relevant, da sie Teil der Arbeitshypothese für den Review bildet. Deshalb wird an dieser Stelle eine – hoffentlich – praxisorientierte Auslegeordnung zur Integration in der vorliegenden Systemarchitektur aufgestellt, welche in Abbildung 5 illustriert ist.

Das Integrationskonzept ist im Weiteren relevant dafür, sichtbar zu machen und eine Auslegeordnung zu erhalten, an welchen Stellen aufwändiges Testen auch in Zukunft erforderlich sein werden, und wo mit zunehmender Reife der Technologien und Produkte der Testbedarf sich mit der Zeit vermutlich reduzieren wird. Diese Kenntnis, verbunden mit Einschätzungen darüber welche Testanteile sich hoch automatisieren lassen, haben grossen Einfluss darauf, wie schnell Änderungen die erforderliche Verifikation durchlaufen und ihre Zulassung erhalten können.

2.4.1 Gesamtsicht Integration

Im inkrementellen Vorgehen in der Integration werden Einzelteile schrittweise integriert, bis daraus schliesslich das Gesamtsystem COAT steht. Es beginnt mit dem Basissystem COAT, bestehend aus dem COAT-EVC und seiner Basis-Software (RTE, Betriebssystem) sowie Grundfunktionen des COAT-Basissystems zuhanden der Peripheriegeräte und Apps.

An dieses Basissystem COAT werden anschliessend die weiteren Teile einzeln «angedockt» und integriert.

Das hier beschriebene Vorgehen ist beispielshaft und als aktuelle Annahme zu verstehen. Insbesondere kann z.B. die Reihenfolge der Integrationsschritte teilweise variiert werden.

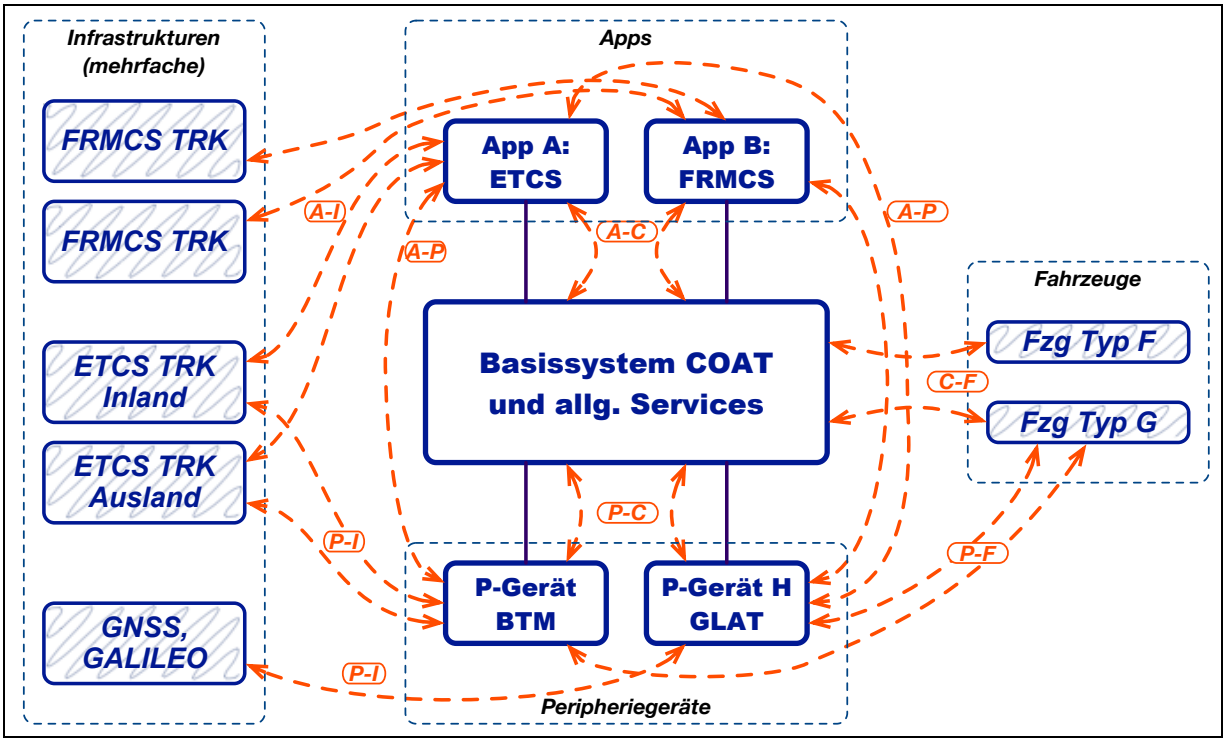

Abbildung 5: Übersicht schrittweise Integration zum Gesamtsystem COAT

2.4.2 Startpunkt: Basissystem COAT

Als Startpunkt wird vorerst das Basissystem COAT in Betracht gezogen[1], welches auf einem bestimmten Fahrzeugtyp zum Einsatz kommen soll.

[1] Es wäre möglich und zu einem passenden Zeitpunkt zielführend, auch das Basissystem COAT aus der Perspektive der Zulassung detaillierter auszuleuchten. Darauf wird vorerst verzichtet in der Annahme, dass ein solches Basissystem von einem Lieferanten angeboten wird. Die für OCORA angestrebte Businessmodelle beziehungsweise angestrebten Lieferantenstrukturen könnten hierzu Klarheit schaffen.

Die Verifikation und Integration umfasst zwei Themenkreise:

- Funktion — Prüfung der Funktionalität und Charakteristiken des Basissystems COAT gemäss Spezifikationen und Normen
- «C-F» — Integration des Basissystem COAT mit einem oder mehreren Fahrzeugtyp(en).
  Es soll sichergestellt werden, dass die COAT-Plattform gemäss Vorgaben in das Fahrzeug eingebaut ist und mit dem Fahrzeug sicher und zuverlässig interagiert. Z.B. die Auslösung der Schnellbremse durch COAT. Siehe Abbildung 6.
  Diese Integration beschränkt sich – zumindest in der Perspektive der Zulassung – nicht auf die TIU (train interface unit).

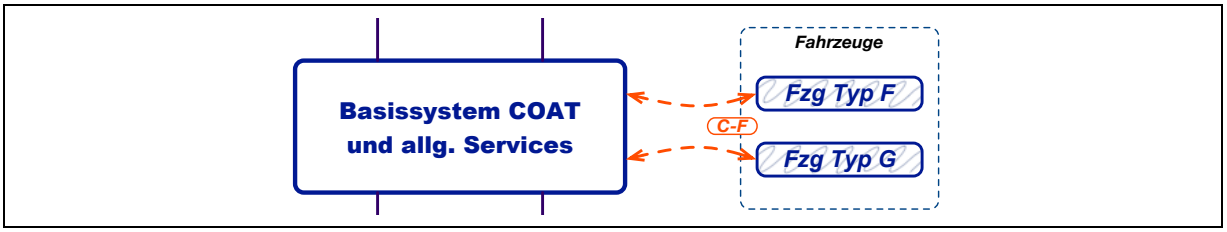

Abbildung 6: Integration Basissystem COAT mit Fahrzeug

Nach erfolgreicher Integration verfügt das Fahrzeug über ein voll funktionsfähiges Basissystem, jedoch (vermutlich) noch über keine Peripheriegeräte noch über Apps. Letztere werden mittels der nachfolgenden Integrationsschritte stufenweise ergänzt.

2.4.3 Ergänzung durch ein Peripheriegerät

Das System COAT soll um ein Peripheriegerät mit einer bestimmten Funktionalität erweitert werden. Hierfür sind mehrere Integrationsschritte notwendig, wofür die Verifikation erforderlich ist (siehe Abbildung 7):

- «P-C»: Integration des Peripheriegerätes mit der COAT-Basisplattform
- «P-F»: Integration des Peripheriegerätes mit einem oder mehreren Fahrzeugtyp(en) (Musterfahrzeug).
  Aus Sicht Zulassung umfasst es z.B. auch die Form des Einbaus im Fahrzeug.
- «P-I»: Falls zutreffend: Integration des Peripheriegerätes mit einer oder mehreren Infrastrukturen.
  Eine Infrastruktur kann z.B. ein FRMCS-Telekomnetz sein oder eine ETCS-Trackside-Infrastruktur (mit Balisen und RBC) u.v.m.

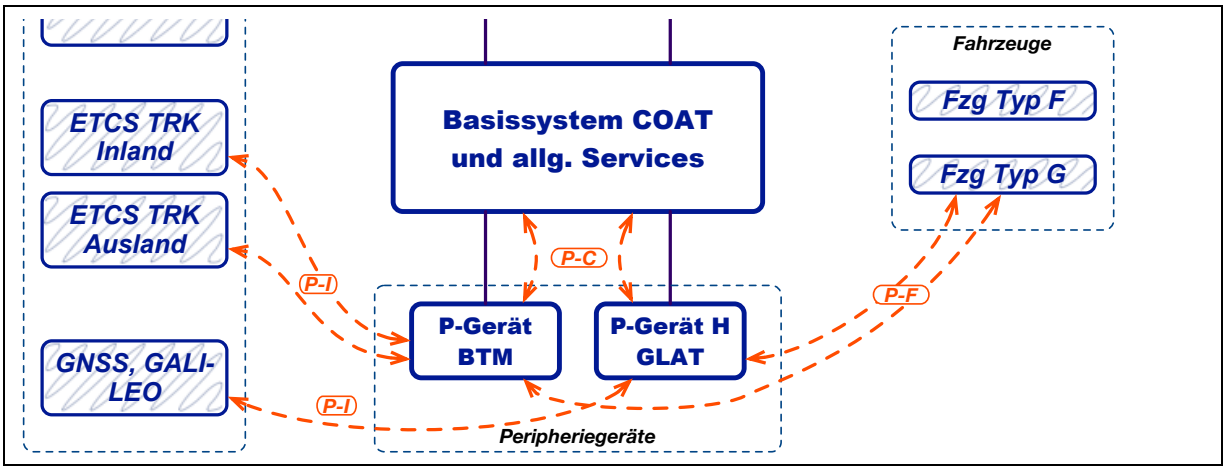

Abbildung 7: Integration Peripheriegerät COAT

Je nach Use Case kann es sein, dass ein bestimmter Integrationsschritt nicht erforderlich ist – oder in gewisser Zukunft nicht mehr erforderlich sein wird. Mögliche Gründe sind:

- Die Schnittstelle ist – oder wird in gewisser Zukunft – zur «Commodity» (Standardkomponente) werden, d.h. als «plug-and-play»-tauglich beurteilt.
- Z.B. ein sich auf GNSS/GLONASS/GALILEO abstützendes Lokalisiergerät ist dahingehend bereits vorgängig geprüft worden (z.B. in einem anderen Land), und muss deshalb in der Schweiz nicht wiederholt werden.

2.4.4 Reifung der Schnittstellen zu «Plug-and-Play»

Die plug-and-play-Tauglichkeit vieler Schnittstellen entspricht einem Hauptziel der Modularisierung und ist somit ein Kernpunkt des Projekts COAT und OCORA. Dieser Zielzustand wird allerdings nicht über Nacht erreicht werden.

Plug-and-play in verteilten Systemen ist jeweils das Ergebnis einer längeren individuellen Reifeperiode einer einzelnen Schnittstelle.

Eine geschickte Konzeption einer Schnittstelle kann ihre schnelle Reifung zu «plug-and-play» sehr wohl begünstigen. Insbesondere aber ist diese Schnelligkeit individuell und hängt klassischerweise von der Verfügbarkeit von Produkten unterschiedlicher Lieferanten ab, mit welchen im Versuch und im Betrieb Erfahrungen gesammelt werden können.

Dem gegenüber erlauben moderne und organisationsübergreifende Entwicklungsmethoden und -umgebungen (z.B. Cloudbasierte Testinstanzen und Continuous Integration inkl. automatisierter Tests), die Reife der Produkte und Schnittstellen bereits in die Entwicklungsphasen vor zu verlagern.

Die Reifephasen betreffen nebst den Produkten auch die Schnittstellen selbst – diese werden währenddessen ebenso Änderungen (Korrekturen) durchlaufen. Von ihnen kann - wie bei Produktentwicklungen - ebenso wenig erwartet werden, von Beginn weg fehlerfrei und perfekt auf «plug-and-play» ausgerichtet zu sein.

Da bei COAT/OCORA die wesentlichen Schnittstellen neu definiert werden, beginnt dieser Entwicklungs- und Reifeprozess grundsätzlich von vorne.

Die Zulassung muss deswegen die Übergangszeit bis zum plug-and-play-Zustand zwingend berücksichtigen. Wird der Wunschzustand in der nahen oder ferneren Zukunft einmal

erreicht, reduziert sich das entsprechende Thema im Zulassungskonzept auf eine kurze Formalität oder kann dann einfach weggelassen werden.

Gleichwohl und unabhängig vom Reifegrad bleibt im Safety Case der Nachweis der Konformität zu Normen und Spezifikationen jeweils erforderlich, selbst wenn sich dies auf eine reine Formalität beschränkt.

2.4.5 Ergänzung durch eine App

Das System COAT soll um eine App mit einer bestimmten Funktionalität erweitert werden. Hierfür sind mehrere Integrationsschritte notwendig, wofür die Verifikation (und schliesslich der Nachweis) erforderlich ist (siehe Abbildung 8):

- «A-C»: Integration des Peripheriegerätes mit der COAT-Basisplattform
- «A-P»: Integration resp. korrekt Interaktion der App mit dem / den relevanten Peripheriegeräten. Der Fokus liegt im korrekten Austausch von Informationen und Notifikationen.
- «A-I»: Falls zutreffend: Integration der App mit einer oder mehreren Infrastrukturen.
  Eine Infrastruktur kann z.B. für eine ETCS-App die ETCS-Trackside-Infrastruktur (mit Balisen und RBC) sein, oder für eine ATO-App die ATO-Infrastruktur des betreffenden Bahnnetzes.

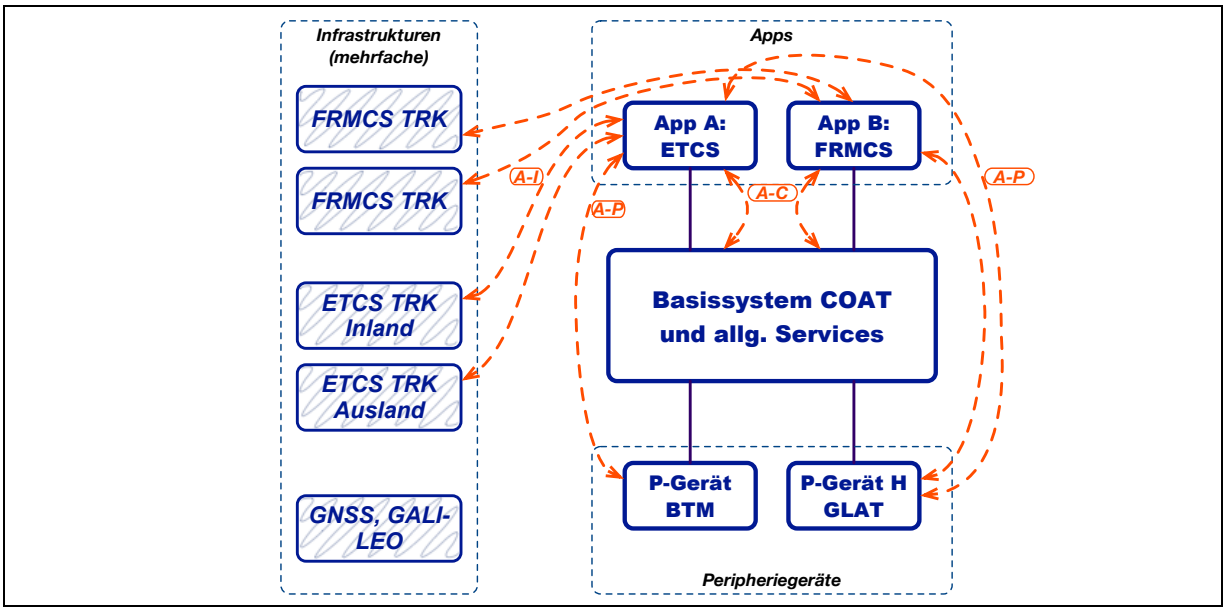

Abbildung 8: Integration COAT-App

2.4.6 Weitere möglicherweise erforderliche Integrationsschritte

Weitere denkbare, erforderliche Integrationsschritte können sein, werden jedoch nur bei konkretem Bedarf weiter betrachtet:

- P-CD Optionaler Integrationsschritt Peripheriegerät zu COAT-Datenvermittlung: betrifft die Sicherstellung bestimmter Datensätze durch das betreffende Peripheriegeräte auf den CCS-Bus.
- A-CD Optionaler Integrationsschritt App zu COAT- Datenvermittlung: betrifft die Sicherstellung dass die App die betreffenden Informationen

vom CCS-Bus abgreifen kann. Dies müsste unabhängig davon funktionieren, welches Peripheriegerät diese Daten erzeugt und den Apps (u.a.) zur Verfügung stellen tut.

- P-P Optional erforderliche Integration zwischen zwei Peripheriegeräten. Relevanz abhängig vom spezifischen Zweck eines Peripheriegerätes, insbesondere wenn dieser von einer Funktionalität/Information eines anderen Peripheriegerätes abhängig ist.
  Hinweis: alternativ zu untersuchen, ob dies auf der Ebene von Informationsdaten abgehandelt und somit auch abstrahiert werden kann.
- A-A Optional erforderliche Integration zwischen zwei Apps. Relevanz abhängig vom spezifischen Zweck der betreffenden Apps, insbesondere bei gegenseitigen funktionalen Abhängigkeiten.
  Hinweis: alternativ zu untersuchen, ob dies auf der Ebene von Informationsdaten abgehandelt und somit auch abstrahiert werden kann.
- A-F Integration App mit Fahrzeugtyp?
  Fraglich ob dieser Integrationsschritt notwendig ist - grundsätzlich wird jedoch versucht, davon absehen zu können.

Es wird angenommen, dass die Systemarchitektur COAT in nächster Zeit diesbezüglich Festlegungen treffen wird.

2.4.7 Zusammenfassung

Folgende Tabelle 2-2 fasst die einzelnen Integrationsschritte in einer Übersicht zusammen.

Die Angabe ob ein bestimmter Integrationsschritt generisch oder spezifischer Natur ist, entspricht aktuell der Annahme des Autors. Der dazu gehörende Leitgedanke ist, dass dieser Integrationsschritt der Klassifikation entsprechend in einem generischen oder spezifischen Sicherheitsnachweis (Safety Case) enthalten sein soll.

Integration von…→	*Basissystem COAT*	*Peripheriegerät*	*App*
…mit Basissystem COAT	n/a	P-C spezifisch [P-CD] generisch	A-C spezifisch [A-CD] generisch
…mit Peripheriegerät	-	[P-P] generisch	A-P spezifisch
…mit App	-	-	[A-A] spezifisch
…mit Fahrzeug(typ)	C-F spezifisch	P-F spezifisch	n/a ???
…mit Infrastruktur	n/a	P-I generisch	A-I generisch

Tabelle 2-2: Zusammenfassung der Integrationsschritte

2.5 Sourcing-Modelle

Ein zentrales Element des Business Cases für die COAT-Plattform ist die reduzierte Abhängigkeit der Fahrzeugbesitzer von Lieferanten («vendor lock-in»). Hauptmerkmal ist dabei die konsequente Modularisierung, welche es Fahrzeugbesitzern im Unterschied zu heute erlauben wird, Komponenten von unterschiedlichen Lieferanten zu beziehen und in ein Gesamtsystem zu integrieren. Ebenso sollen einzelne Komponenten durch funktional gleichwertige Produkte von anderen Lieferanten ersetzt werden können.

Die für COAT-Plattformen und -Komponenten angestrebten Sourcing-Modelle sind in der Regel Bestandteil eines Lieferanten- und Businessmodell COAT.

In diesem Zusammenhang stehen für das Zulassungskonzept COAT zwei Anforderungen im Zentrum:

- die Zuständigkeiten für die verschiedenen Teile der Nachweisführungen müssen direkt und unkompliziert organisiert sein; sowie
- die Verantwortung für eine spezifische Nachweisführung oder einen Sicherheitsnachweis muss stets einer einzigen Organisation zugeordnet werden können.

Ein Safety Case darf nur einen Autor haben, in aller Regel den Lieferanten für den betreffenden Teil des COAT-Systems oder ein spezifischer Dienstleister (z.B. Integrator).

Daraus folgt, dass das Zulassungskonzept COAT zum Sourcing-Modell COAT kompatibel sein muss. Insbesondere muss im Zulassungskonzept für jede Sourcing-Variante, welche das Businessmodell COAT vorsieht, ein oder mehrere dazu passende Module der Nachweisführung resp. Safety Case vorsehen.

Ein gesondertes Diskussionsdokument [Dok.2] vertieft das Thema und präsentiert ein denkbares Beispiel für Lieferantenrollen.

3 Analyse Zulassungskonzept COAT

Im Folgenden wird das Zulassungskonzept COAT [Dok.4] betrachtet.

3.1 Übersicht Sicherheitsnachweise

Tabelle 3-1 listet die Zulassungsdokumente auf, die gemäss dem Zulassungskonzept und basierend auf einer Standard-Ausrüstung einer COAT-Installation zu erstellen, zu unterhalten sowie bei Änderungen am COAT-System zu aktualisieren sind.

Für die einzelnen Zulassungsdokumente werden die in Kapitel 2.4 identifizierten Integrationsschritte ausgewiesen. Diese Zuordnung entstammt jedoch der Interpretation des Autors und nicht des Erstellers des Zulassungskonzepts.

#	*Kurzbez.*	*Beschreibung und Inhalte*
Generische Sicherheitsnachweise, Stufe Teilsystem		
SCA	GASC EVC	Generischer Safety Case für das Basissystem COAT. Scope (Annahme des Autors): - CCS-Bus - RTE / Betriebssystem - Services (zuhanden aller Apps; gemäss OCORA) Beinhaltet Nachweise: - Charakteristika (funktional & nicht-funktional) gemäss Anforderungen und Spezifikationen
SCB	GASC DMI	Generischer Safety Case HMI (human-man-interface) Entspricht einem Peripheriegerät und beinhaltet Nachweis: - Charakteristika (funktional & nicht-funktional) gemäss Anforderungen und Spezifikationen - «P-C» Integration DMI zum Basissystem COAT
SCD	GASC TIU	Generischer Safety Case für den Anschluss COAT an das Fahrzeug Entspricht einem Peripheriegerät und beinhaltet Nachweis: - Charakteristika (funktional & nicht-funktional) gemäss Anforderungen und Spezifikationen - «P-C» Integration TIU zum Basissystem COAT
SCD	GASC BTM	Generischer Safety Case für das Peripheriegerät Balisenleser. Beinhaltet Nachweise: - Charakteristika (funktional & nicht-funktional) gemäss Anforderungen und Spezifikationen - «P-C» Integration BTM zum Basissystem COAT - «P-I» Integration LTM zur Infrastruktur (z.Bsp. TSI- / Interoperabilität) Optionaler Nachweis:

#	*Kurzbez.*	*Beschreibung und Inhalte*
		- «P-CD» BTM hinterlegt Daten in vordefinierten Formaten
SCE	GASC LTM	Generischer Safety Case für das Peripheriegerät Loop-Leser Beinhaltet Nachweise: - Charakteristika (funktional & nicht-funktional) gemäss Anforderungen und Spezifikationen - «P-C» Integration LTM zum Basissystem COAT - «P-I» Integration LTM zur Infrastruktur (z.Bsp. TSI- / Interoperabilität) Optionaler Nachweis: - «P-CD» LTM hinterlegt Daten in vordefinierten Formaten.
SCF	GASC GLAT (Lokalisierung)	Generischer Safety Case Tachymetrie / Lokalisierung Beinhaltet Nachweise: - Charakteristika (funktional & nicht-funktional) gemäss Anforderungen und Spezifikationen - «P-C» GLAT zum Basissystem COAT - «P-I» GLAT zur Infrastruktur (z.Bsp. GPS/GLONASS) Optionaler Nachweis: - «P-CD» GLAT hinterlegt Daten in vordefinierten Formaten.
SCG	GASC Radio	Generischer Safety Case Radiokommunikation (GSM-R / FRMCS) Beinhaltet Nachweise: - Charakteristika (funktional & nicht-funktional) gemäss Anforderungen und Spezifikationen - «P-C» Integration Radio zum Basissystem COAT - «P-I» Integration Radio zur Infrastruktur (z.Bsp. GSM-R SBB) Optionaler Nachweis: - «P-CD» Radio hinterlegt Daten in vordefinierten Formaten.
SCH	GASC JRU	Generischer Safety Case Juridical Recording Unit Beinhaltet Nachweise: - Charakteristika (funktional & nicht-funktional) gemäss Anforderungen und Spezifikationen - «P-C» Integration JRU zum Basissystem COAT Optionaler Nachweis: - «P-CD» JRU hinterlegt Daten in vordefinierten Formaten.
SCI	GASC NSR-PG	Generischer Safety Case für nicht sicherheitsrelevantes Peripheriegerät Beinhaltet Nachweise: - Charakteristika (funktional & nicht-funktional) gemäss Anforderungen und Spezifikationen

#	*Kurzbez.*	*Beschreibung und Inhalte*
		- «P-C» NSR-PG zum Basissystem COAT - «P-I» NSR-PG zur Infrastruktur, sofern zutreffend Optionaler Nachweis: - «P-CD» NSR-PG hinterlegt Daten in vordefinierten Formaten.
Generische Sicherheitsnachweis, Stufe Gesamtsystem		
SCJ	GASC GS-COAT «System COAT 1.0»	Generischer Safety Case für das Gesamtsystem COAT. Bündelt Sicherheitsnachweise GASC EVC, GASC DMI, GASC TIU, GASC BTM, GASC LTM, GASC GLAT, GASC Radio, GASC JRU, sowie sofern zutreffend GASC NSR-PG und GASC SR-PG. Zusätzliche eigene Inhalte: - Für jede App, Nachweise bezüglich: o Charakteristika (funktional & nicht-funktional) gemäss Anforderungen und Spezifikationen o «A-C» Nachweis Integration App mit der COAT-Basisplattform o «A-P» Nachweis Integration App mit den Peripheriegeräten o «A-I» Nachweis Integration App mit relevanten Infrastrukturen (z.B. TSI CCS / ETCS Interoperabilität mit bestimmten Strecken)
Spezifische Sicherheitsnachweise		
SCK	SASC System COAT 1.0	Spezifischer Safety Case für das Gesamtsystem COAT auf einen Fahrzeugtyp. Basiert auf dem generischen Safety Case für das Gesamtsystem COAT, und spezifiziert die aktuelle Selektion von Peripheriegeräten und Apps[2]. Beinhaltet zusätzlich Nachweise: - «C-F» Integration EVC mit Fahrzeug (einschl. CCS-Bus) - «P-F» DMI mit Fahrzeug - «P-F» TIU mit Fahrzeug - «P-F» BTM mit Fahrzeug - «P-F» LTM mit Fahrzeug - «P-F» GLAT mit Fahrzeug - «P-F» Radio mit Fahrzeug - «P-F» JRU mit Fahrzeug - «P-F» NSR-PG mit Fahrzeug, falls zutreffend
Gutachten → nicht aufgelistet		

[2] gemäss den Arbeitshypothesen wird angenommen, dass ein generischer Safety Case die Typenzulassung mehrerer gleichartiger Peripheriegeräte und Apps beinhaltet, d.h. alle zugelassenen Modelle potenziell unterschiedlicher Lieferanten. Folglich muss der spezifischer Safety Case eine bestimmte Wahl vornehmen.

Tabelle 3-1: Übersicht Sicherheitsnachweise und ihre Inhalte bezüglich der Integration

Die Unterscheidung zwischen «generisch» und «spezifisch» wird im Zulassungskonzept COAT darin unterschieden, dass der spezifische Sicherheitsnachweis zusätzlich die Integration des Gesamtsystems auf einen bestimmten Fahrzeugtyp beinhaltet.

3.2 Verständnis «Generisch» und «Spezifisch»

Die Begriffe «generisch» und «spezifisch» sind Metabegriffe, und deren Bedeutung variieren in Abhängigkeit des betreffenden Objektes und des anwendbaren Kontextes.

Traditionell unterscheidet die Bahntechnik einzig bezüglich Fahrzeugtyp-spezifischen Belangen: ein generischer Nachweis klammert die Fahrzeugtyp-spezifischen Belange aus, während ein spezifischer Nachweis diese ergänzend behandelt. Dieser Ansatz gilt auch im Zulassungskonzept [Dok.4].

Generische Nachweise interessieren sich primär für die Funktionalitäten und Charakteristiken von (Teil-)Systemen gemäss den zuständigen Spezifikationen. Darin enthalten sind Schnittstellen mit Partnersystemen (z.B. zwischen einem Peripheriegerät und der Basisplattform COAT). Für den generischen Nachweis genügt es grundsätzlich, die Verifikation z.B. im Labor unter Verwendung von Simulatoren für die Gegenseiten einzuschränken.

Im Kontext COAT bestehen weitere denkbare und relevante Unterscheidungen zwischen «generisch» und «spezifisch». Sie sind in folgender Tabelle beispielhaft aufgeführt.

Kontext	*«Spezifisch» kann bedeuten…*
Teilsystem und Geräte in COAT	
Basissystem COAT (CCU, RTE, CCS-Bus)	…bezüglich eines Fahrzeugtyps, in welches es eingebaut wird
COAT Peripheriegerät (PG)	…bezüglich der COAT-Plattform (Basissystem COAT), an welches das PG angebunden wird.
COAT App	…bezüglich der COAT-Plattform (Basissystem COAT), auf welches es lauffähig sein muss …mit bestimmten Peripheriegeräten, mit welchen die App korrekt «arbeiten» muss.
Beispiele ausserhalb COAT	
ETCS-Infrastruktur	…bezüglich bestimmter ETCS- Strecken oder Bahnnetz
ETCS Onboard	…bezüglich Fahrzeugtyp, in welches es eingebaut wird …bezüglich bestimmter ETCS- Strecken oder Bahnnetz

Tabelle 3-2: Spezifische Anwendungen - Beispiele

In der weiteren Ausarbeitung des Zulassungskonzeptes COAT wird empfohlen, diese Unterscheidungen zu erwägen und allenfalls zu berücksichtigen.

3.3 Terminologie des Zulassungskonzepts

Die Dokumentation der Enotrac zum Zulassungskonzept nutzt Begriffe, welche in einschlägigen Standards bereits definiert sind, und verwendet diese wieder im leicht anderen Formen im Kontext von COAT. Zwei Beispiele:

- Hauptbeispiel ist der EVC (European Vital Computer), welcher bisher als reiner ETCS-Fahrzeugrechner betrachtet wurde. Im Zulassungskonzept repräsentiert der EVC den COAT-Fahrzeugrechner, welcher imstande sein wird, eine Anzahl von COAT-Applikationen zu verwenden.
  Im Verlauf der Weiterentwicklung der OCORA-Architektur zur beta-Version wurde EVC in CCU («CCS Computing Unit») umbenannt.
- IK / Interoperabilitätskomponente: das Anwendungsgebiet dieses Begriffs bezieht sich gemäss der TSI CCS auf die ETCS-Thematik. Im COAT-Zulassungskonzept wird deren Bedeutung dahingehend erweitert (Irrtum vorbehalten), dass sie die Interoperabilität innerhalb COAT betrifft, selbst wenn Letzteres nicht in direktem Kontext mit ETCS steht.

Aufgrund der Tatsache, dass die Entwicklung von COAT und der OCORA-Architektur noch jung und in Erarbeitung sind, ist die temporäre Verwendung vertrauter Begriffe sehr verständlich. Mit der Zeit und mit zunehmender Reifung und Konsolidierung der Konzepte sollten allfällige Konflikte in Begriffsdefinitionen bereinigt werden.

3.4 Use Cases Enotrac

#	*Was*	*Beschreibung*
Erstzulassungen		
Gesamtsystem		Erstzulassung des COAT-Gesamtsystems einschliesslich aller IK / Geräte.
Funktionale Erweiterungen		
Zusätzliches Peripheriegerät		Anschluss eines zusätzlichen Peripheriegeräts an den CCS-Bus
Zusätzliche Information von einem Peripheriegerät		Von den bestehenden Peripheriegeräten sollen zusätzliche Informationen verlangt werden, die zuvor noch nicht über die Bus-Schnittstelle übertragen werden
Zusätzliche Applikation		Entwicklung und Einführung einer zusätzlichen Applikation auf dem EVC.

Tabelle 3-3: Use Cases aus dem Enotrac Zulassungsverfahren COAT

Diese Use Cases sind verallgemeinert genügen daher nicht für den Erweiterten Review mittels Use Cases. In Kapitel 4.1 wurden die Use Cases identifiziert und aufgelistet, die für die Durchführung des Erweiterten Reviews relevant sind.

3.5 Gedanken zum vorliegenden Zulassungskonzept

3.5.1 Modularisierung

Bei der Zulassung eines Gesamtsystems COAT sind viele sehr unterschiedliche Sachgebiete als auch zahlreiche Integrationsthemen (wie in Kapitel 2.4.1 beispielshaft ausgewiesen) zu behandeln. Deswegen empfiehlt sich ein modulares Vorgehen, indem die Zulassungsdokumentation in Form mehr oder weniger autonomer Module aufgeteilt geführt wird. Im Wesentlichen orientieren sich diese Module entlang der COAT-Architektur sowie der einzelnen erforderlichen Integrationsschritte, und sie definieren und unterscheiden sich über individuelle thematische Zuständigkeiten und Verantwortlichkeiten.

Der Vorteil der Modularität in der Zulassungsdokumentation kommt primär bei Änderungen an einem bestehenden Gesamtsystem COAT zugute. Im Lebenszyklus eines Gesamtsystems COAT werden insbesondere Änderungen punktueller Natur an spezifischen Modulen sein, die vergleichsweise häufig vorkommen. Das heisst, dass jeweils nur ein Teil der Integrationsthemen betroffen sein wird und somit überarbeitet werden muss. Die restlichen werden unangetastet bleiben. Demnach gilt die Erwartung, dass auch die Zulassungsdokumentation nur selektiv überarbeitet werden muss.

Voraussetzung hierfür ist, dass der modulare Zulassungsbaukasten bereits bei der Erstzulassung praktiziert und eingehalten wird. Andernfalls führen auch triviale, nicht-relevante Änderungen am COAT-System zu substanziellen Aufwänden bei der Überarbeitung der Zulassungsdokumentation. Der Grund liegt darin, dass es die aus der Erstzulassung resultierende Dokumentation ist, welche bei Änderungen am System entsprechend überarbeitet werden muss. Ohne Modularisierung würde auch bei trivialen Änderungen nur ein sehr kleiner Teil der Dokumentation unangetastet bleiben.

Motivation hierfür ist die Vermeidung von Redundanz und Wiederholungen gemäss dem ‘DRY principle’[3].

3.5.2 Offene Fragen bezüglich des Durchspielens der Use Cases

Das Zulassungskonzept von Enotrac und der beigestellte Analysebericht lassen ein paar Fragen offen, die zu klären sind.
Die nachstehend getroffenen Annahmen gelten als Hypothese resp. Referenz für die Durchführung des Erweiterten Use Case-Reviews:

I. Als Referenz für diesen Auftrag gilt das Zulassungskonzept Version 1.0 einschliesslich der Systembeschreibung Version 1.0 von ENOTRAC. Hingegen hat sich unterdessen das OCORA massgeblich weiterentwickelt.
   → Vereinbartes Vorgehen: im Verlauf der Arbeit erkannte Unterschiede resp. Komplikationen ausweisen und dokumentieren.

II. Für COAT-Apps sind keine SiNa ersichtlich, ist dies korrekt?
   In welchen SiNa-Dokumentationen werden diese abgedeckt sein?

[3] DRY = Don’t Repeat Yourself

→ Getroffene Annahme: für Apps werden keine dezidierten SC geführt, sondern die Apps werden derzeit im generischen SC für das Gesamtsystem behandelt geführt.

III. Generischer SC Gesamtsystem:
Wird es einen globalen geben, der – im Sinne eines Werkzeugkasten – die zulässigen (typenzugelassenen) Peripheriegeräte auflistet, wie z.B. zwei Modelle von Balisenlesern unterschiedlicher Hersteller, und die spezifische Applikation legt fest welches der beiden Modelle in einem bestimmten Fahrzeug konkret zur Anwendung kommt?
Oder wird für unterschiedliche Zusammensetzungen (Konfigurationen) eines COAT-Gesamtsystems je ein separater SC notwendig sein?
→ Getroffene Annahme: es gilt Ersteres.

IV. Es ist im Enotrac-Zulassungskonzept nicht ersichtlich, in welcher Dokumentation die Integration der Peripheriegeräte auf den einzelnen Fahrzeugtyp behandelt werden muss. Vermutlich nur im spezifischen Gesamt-SiNa.

V. Nicht detailliert umrissener Scope / Umfang:
- des COAT-EVCs (gemäss Definition in Dok.3 / Systembeschreibung ENOTRAC),
- der Scope des generischen SiNa EVC (Dok.4 / Zulassungskonzept ENOTRAC).
→ Getroffene Annahme: COAT-EVC steht für das ganze Basissystem COAT gemäss November-Ausgabe OCORA

VI. Integrationsschritte, wie sie beispielshaft in Kapitel 2.4 beschrieben sind, sind im Zulassungskonzept nicht vollständig ausgearbeitet. Sie werden teilweise angesprochen. Z.B.:
- Interoperabilität ETCS mit Strecke
→ Vereinbartes Vorgehen: eigenes Verständnis dokumentieren (siehe Kapitel 2.4).

VII. An verschiedenen Stellen im Zulassungskonzept werden ETCS-Belange angesprochen. Es wird daraus jedoch nicht klar, welche dieser Belange wo behandelt werden müssen, eine entsprechende Aufschlüsselung fehlt. Wir sehen z.B.
- IOP PG mit Strecke müsste im SiNa für PG behandeln werden, und dies wäre je nach Betrachtung ein generisches oder spezifisches Thema
- IOP App mit Strecke müsste im SiNa für die App behandelt werden
- etc. bis alle ETCS-IOP-Themen damit abgedeckt sind.
Ohne diese Aufschlüsselung wird das Thema ETCS in allen Safety Cases zu diskutieren sein. Ohne eindeutige und verständliche gegenseitige Abgrenzungen wird dies potenziell zu Redundanzen und Inkonsistenzen führen.
→ Getroffene Annahme: wird als Beobachtung notiert.

4 Anwendung der Use Cases an das Zulassungskonzept

4.1 Übersicht

4.1.1 Zielsetzung

Die Vorbereitung für den Erweiterten Review strebt unter anderem folgende Ziele an:

- Die Use Cases müssen so detailliert beschrieben sein, wie sie für das Durchspielen relevant sind.
- Das Durchspielen eines Use Cases soll allfällige offene Fragen (zum Zulassungskonzept, zur OCORA-Architektur) identifizieren, sowie den Einfluss der möglichen Antworten auf die Zulassungsarbeit abschätzen.
- Identifikation der zu behandelnden Punkte im Zulassungskonzept
  (zB. Vorgehensweise in einer Zulassung, z.B. Integrationsschritte, nicht nur über Dokumente sprechen)

4.1.2 Fokus für die Durchführung des Erweiterten Reviews

Das Augenmerk des erweiterten Reviews durch Use Cases liegt primär auf den Sicherheitsnachweisen und deren Inhalte sowie deren gegenseitigen Abgrenzungen.

Die Sachverständigenberichte und Bescheinigungen durch NoBos werden in diesem Erweiterten Review nicht besonders behandelt. Diese Dokumente reviewen die Safety Cases und prüfen diese auf Vollständigkeit. Deswegen kann pauschal angenommen werden, dass die Aufwände dieser Beteiligten und für die Erstellung ihrer Berichte analog zum Überarbeitungsaufwand der Safety Cases stehen.

Als Nebenprodukt des Reviews wird eine – allerdings unvollständige – Identifikation von Referenzen zu Normen oder Spezifikationen sein, auf welche sich diese Unabhängigen allenfalls abstützen können.

4.2 Use Cases

4.2.1 Beschreibung der Use Cases

Im Folgenden werden die Use Cases aufgelistet, die für den erweiterten Review in Frage kommen. Für die Durchführung wird eine repräsentative Auswahl getroffen.

Die Use Cases sind in vier Gruppen aufgeteilt:

- Gruppe E: Erstzulassungen
- Gruppe AB: Änderungen am Basissystem COAT
- Gruppe AP: Änderungen an Peripheriegeräten
- Gruppe AA: Änderungen an COAT-Applikationen

Die Gruppe der Erstzulassungen führt unter anderem Use Cases auf, die sich auf Vorleistungen anderer Use Cases (ebenso Erstzulassungen) abstützen. Darin eingeschlossen sind insbesondere auch, dass COAT-Systeme oder -Bestandteile bereits im Ausland zugelassen sein können, für welche die Erstzulassung für die Schweiz ansteht.

Hinweis: in Bezug auf die Verwendung der Begriffe «generisch» und «spezifisch» wird auf das Zulassungskonzept [Dok.4] verwiesen. Der Unterschied bezieht sich darauf, ob das System auf einen bestimmten Fahrzeugtyp integriert ist / wurde.
Beispiel: ein generisches Gesamtsystem COAT zielt grundsätzlich darauf, auf beliebigen Fahrzeugen eingesetzt werden zu können, ist als solches aber (noch) nicht mit einem bestimmten Fahrzeug integriert. Wenn Letzteres der Fall ist, wird es ein spezifisches Gesamtsystem.

UC#	*Use Case, (Federführende Instanz)*	*Beschreibung, Voraussetzungen*
E*	**Erstzulassungen**	
EGG	Erstzulassung generisches Gesamtsystem COAT (Lieferant COAT)	Erstzulassung eines COAT-Gesamtsystems für die Bedürfnisse in der Schweiz (z.B. smartrail4.0), ohne Zulassung auf bestimmte Fahrzeugtypen. Entspricht im Wesentlichen dem Lieferumfang eines COAT-Lieferanten Schweiz. [Annahme: es wird diese Rolle geben] Ausgangslage: - Zusammenstellung: COAT-Basissystem mit einer Anzahl Peripheriegeräten (DAMI, TIU, BTM/LTM, GLAT, DMI) sowie einer Anzahl Apps (ETCS, ATO). - Keine Teilsysteme sind in der Schweiz bereits zugelassen. - Das Gesamtsystem COAT ist/wird - vorerst - für keinen Fahrzeugtyp zugelassen.
EGF1	Erstzulassung COAT-Gesamtsystem auf einen Fahrzeugtyp (Gesamtintegrator COAT)	Erstzulassung eines COAT-Gesamtsystems zur Anwendung in einem bestimmten Fahrzeugtyp. Entspricht im Wesentlichen dem Lieferumfang eines COAT-Gesamtintegrators. [Annahme: es wird diese Rolle geben] Ausgangslage: - Zusammenstellung: COAT-Basissystem mit einer Anzahl Peripheriegeräten (DAMI, TIU, BTM/LTM, GLAT, DMI) sowie einer Anzahl Apps (ETCS, ATO). - Keine Teilsysteme sind in der Schweiz bereits zugelassen. - Das Gesamtsystem COAT soll für einen bestimmten Fahrzeugtyp zugelassen werden. Unterschied zu Use Case EGG: zusätzliche Integration mit einem Fahrzeugtyp.

UC#	*Use Case,* *(Federführende Instanz)*	*Beschreibung,* *Voraussetzungen*
EGF2	Erstzulassung COAT-Gesamtsystem auf zusätzlichen Fahrzeugtyp (Gesamtintegrator COAT)	Erstzulassung eines COAT-Gesamtsystems zur Anwendung in einem weiteren bestimmten Fahrzeugtyp. (Das in EGF1 Erreichte solle mit einem weiteren Fahrzeugtyp integriert werden.) Ausgangslage: - Zusammenstellung: COAT-Basissystem plus Anzahl Peripheriegeräten (DMI, TIU, BTM/LTM, GLAT, DMI) sowie Anzahl Apps (ETCS, ATO). - Das Gesamtsystem COAT ist bereits für einen anderen Fahrzeugtyp zugelassen. - Die Teilsysteme sind bereits für den Einsatz in der Schweiz zugelassen.
EGCH	Erstzulassung für die Schweiz eines im Ausland zugelassenen generischen COAT-Gesamtsystems. (Gesamtintegrator COAT)	Erstzulassung eines generischen COAT-Gesamtsystems zur Anwendung in der Schweiz, (noch) ohne spezifische Fahrzeugintegration. Ausgangslage: - Zusammenstellung: COAT-Basissystem plus Anzahl Peripheriegeräten (DAMI, TIU, BTM/LTM, GLAT, DMI) sowie Anzahl Apps (ETCS, ATO). - Generisches Gesamtsystem COAT sowie die Teilsysteme sind in einem anderen Land zugelassen, jedoch nicht in der Schweiz.
EGFCH	Erstzulassung für die Schweiz eines im Ausland zugelassenen COAT-Gesamtsystems für ein bestimmtes Fahrzeug (Gesamtintegrator COAT)	Erstzulassung eines COAT-Gesamtsystems eines Fahrzeugs für die Anwendung in der Schweiz. Das im Ausland zugelassene COAT-ausgerüstete Fahrzeug soll in der bestehenden Konfiguration auch in der Schweiz zugelassen werden. Ausgangslage: - Generisches Gesamtsystem COAT inkl. Teilsysteme sind in einem anderen Land zugelassen. - Gesamtsystem COAT ist bereits für einen bestimmten Fahrzeugtyp zugelassen. - Zusammenstellung: COAT-Basissystem plus Anzahl Peripheriegeräten (DAMI, TIU, BTM/LTM, GLAT, DMI) sowie Anzahl Apps (ETCS, ATO).
EPF	Erstzulassung neues Peripheriegerät (Lieferant Peripheriegerät)	Entwicklung und Einführung eines zusätzlichen Peripheriegerätes und Erstzulassung auf einer COAT-Plattform. Beinhaltet den Nachweis für: - (Generisch) Charakteristika gemäss Spezifikation - (Generisch) Integration mit Basisplattform COAT - (Spezifisch) Integration mit Fahrzeugtyp(en) - (Generisch) Integration mit Infrastruktur

UC#	*Use Case,* *(Federführende Instanz)*	*Beschreibung,* *Voraussetzungen*
EPNSR	Erstzulassung neues nicht-sicherheitsrelevantes Peripheriegerät (Lieferant Peripheriegerät)	Entwicklung und Einführung eines zusätzlichen Peripheriegerätes, und Erstzulassung auf einer COAT-Plattform und für den Einsatz auf einem Fahrzeugtyp. Beinhaltet den Nachweis für: - (Generisch) Charakteristika gemäss Spezifikation - (Generisch) Integration mit Basisplattform COAT - (Spezifisch) Integration mit Fahrzeugtyp(en) - (Generisch) Integration mit Infrastruktur Im Unterschied zum UseCase EPF wird in diesem Use Case das NSR-Peripheriegerät zusätzlich für den Einsatz in einem Fahrzeugtyp zugelassen.
EAG	Typenzulassung für eine neue COAT-Applikation (Lieferant COAT-App)	Entwicklung und Einführung einer (neuen) Applikation auf der CCU und Erstzulassung auf einer COAT-Plattform. Beinhaltet den Nachweis für: - Funktionalität gemäss Spezifikationen und/oder Standards [soweit relevant] - Integration mit COAT-Plattform (eine oder mehrere Typen) - Integration mit Peripheriegeräten (eine oder mehrere Typen) - Integration mit Infrastruktur (eine oder mehrere Strecken) Die Integration mit Fahrzeugtypen ist hier nicht enthalten.
EAF	Neue COAT-Applikation auf Fahrzeugtyp einsetzen (Lieferant COAT-App)	Entwicklung, Einführung und Erstzulassung einer (neuen) Applikation für einer COAT-Plattform auf einem Fahrzeugtyp. Beinhaltet den Nachweis für: - Gemäss Typenzulassung für die App (Use Case EAG) - Integration in den bestimmten Fahrzeugtyp
AB	**Änderung am Basissystem COAT**	
AB-1	Kuratives Wartungsupdate für Bug-Fixes (Lieferant COAT)	Das Basissystem COAT muss zum Vorschein gekommene Defekte (in Hardware und/oder RTE) zeitgerecht - d.h. innert weniger Wochen – beheben. Keine funktionalen Erweiterungen.
AB-2	Kuratives Wartungsupdate, Schliessung Cybersecurity-Lücke(n) (Lieferant COAT)	Eine oder mehrere dringliche Cybersecurity-Lücke(n) müssen zeitgerecht (d.h. innert möglichst weniger Tage oder Wochen) geschlossen werden.
AB-3	Wartungsupdate Präventiv (Lieferant COAT)	Das Basissystem COAT wird im Sinne eines Substanzerhaltes gewartet und technologisch à jour gehalten. Z.Bsp. Aufdatierung des grundlegenden RTE-Betriebssystems. *[Die Wahrscheinlichkeit solcher Updates ist zu klären.]*

UC#	*Use Case,* *(Federführende Instanz)*	*Beschreibung,* *Voraussetzungen*
AB-4	Minor Funktionsupdate für neue/verbesserte Funktion (Lieferant COAT)	Das Basissystem COAT wird bezüglich ihrer Funktionalität weiterentwickelt. Minor Update. Keine direkte Änderung an Interaktion mit Peripheriegeräten. (Kleinere) neue Funktionen kommen dazu, oder bestehende Funktionen oder Charakteristiken werden verbessert, z.B. zwecks Steigerung der Plattformstabilität, zusätzliche Information auf dem CCS-Bus zur Verfügung stellen.
AB-5	Schliessung SRACs (Lieferant COAT)	Funktionsupdate zur Schliessung einer oder mehrerer Anwendungsbedingungen (SRACs). Unterscheidung zu AB-1 und AB-4: Zeitachse - weniger dringlich als bei AB-1 und AB-4.
AB-6	Medium Funktionsupdate, mit Relevanz Interaktion zu Komponenten (Lieferant COAT)	Das Basissystem COAT erfährt eine Änderung einer Funktionalität, welche mit einer Änderung in der Interaktion mit Komponenten (Apps und/oder Peripheriegeräte) einherkommt, z.B. erweiterte API für COAT-Apps. Medium Update. *Praxisbeispiel ergänzen!*
AB-7	Medium Funktionsupdate, mit Relevanz Interaktion zum Fahrzeug (Lieferant COAT)	Das Basissystem COAT erfährt eine Änderung einer Funktionalität, welche mit einer Änderung in der Interaktion mit dem Fahrzeugtyp einherkommt. Medium Update. *Eher futuristisch!*
AB-8	Konfigurationsupdate (geänderte Einstellungen) Varianten: A: sicherheitsrelevant B: nicht sicherheitsrelevant (Lieferant COAT)	Änderung der statischen Konfiguration der App mit oder ohne Sicherheitsrelevanz, z.B. root-certificate erneuern für Datenkommunikation im Telecom-Netz der Bahn.[4] [Relevanz fraglich, zu klären]
AB-9	Austausch Basissystem COAT	Der Fahrzeugeigentümer will/muss – für eine bestimmte Flotte/Fahrzeugtyp - das Basissystem COAT (CCU & CCS-Bus) durch ein anderes Modell des Basissystem COAT (des gleichen oder eines anderen Lieferanten) ersetzen. Annahmen für das neue Basissystem COAT: - es besitzt grundsätzlich bereits eine Typenzulassung; - die Apps sind darauf bereits lauffähig und zugelassen; - die Peripheriegeräte sind grundsätzlich bereits zugelassen.

[4] Keine Modifikation der Funktionalität der App, abgesehen vom Umstand, dass die Konfiguration eine - eigentlich bereits vorhandene – Funktionalität erstmals zur Anwendung kommen lässt, folglich im Sicherheitsnachweis bisher nicht bearbeitet wurde.

UC#	*Use Case,* *(Federführende Instanz)*	*Beschreibung,* *Voraussetzungen*
AB-10	Major Upgrade (Lieferant COAT)	Einführung einer neuen Baseline des Basissystem COAT welche eine Kombination von Use Cases (AB*) umfasst: - (AB) Defekte schliessen - (AB) Funktionalität erweitern (schliesst Verbesserungen nicht-funktionaler Aspekte ein) - (AB) Substanzerhalt - (AB) Austausch Hard- und Software
AP	**Änderung an Peripheriegeräten**	
AP-1	Kuratives Wartungsupdate zur Behebung von Defekten (Lieferant Peripheriegerät)	Dringliches Update, beispielsweise ein Firmware-Update für ein Peripheriegerät, oder eine notwendige Hardware-Anpassung (z.B. in der Mechanik). Das Peripheriegerät muss zum Vorschein gekommene Defekte zeitgerecht (d.h. innert weniger Wochen) beheben. Keine funktionalen Erweiterungen. Defekte können nicht sicherheitsrelevant sein oder aber eine Sicherheitslücke schliessen.
AP-2	Wartungsupdate Präventiv (Lieferant Peripheriegerät)	Das Peripheriegerät wird im Sinne eines Substanzerhaltes gewartet und technologisch à jour gehalten. Z.Bsp. Aufdatierung des Embedded Operating System. *[Wahrscheinlichkeit & Relevanz solcher Updates zu klären.]*
AP-3	Minor Funktionsupdate für neue/verbesserte Funktionen (Lieferant Peripheriegerät)	Minor Update: Verbesserungs-Release, z.B. das Peripheriegerät wird bezüglich ihrer Funktionalität weiterentwickelt. (Kleinere) neue Funktionen kommen dazu, oder bestehende Funktionen oder Charakteristiken werden verbessert (z.B. zwecks Steigerung der Stabilität).
AP-4	Medium Funktionsupdate, mit Interaktion COAT-Apps (Lieferant Peripheriegerät)	Medium Update: das Peripheriegerät erfährt eine Änderung ihrer Funktionalität, die Änderungen in der Interaktion mit COAT-Apps bedeuten können. Z.B. ein Sensor wird durch das Nachfolgemodell gleicher oder ähnlicher Eigenschaften ersetzt.
AP-5	Zusätzliche Information zur Verfügung stellen	Vom bestehenden Peripheriegerät sollen zusätzliche Informationen verlangt werden, die zuvor noch nicht über die Bus-Schnittstelle übertragen werden resp. verwendet werden. [Trifft tendenziell nur zu, falls beim CCS-Bus das publish/subscribe-Prinzip gilt. Alternativen dazu sind z.B. P2P-request/response-Prinzip.]
AP-6	Major Upgrade (Lieferant Peripheriegerät)	Neue Softwareversion welche eine Kombination von Fehlerbehebung aller vorgängigen Use Cases. Das heisst, dieser AF entspricht einer Kombination von beliebigen AP*.

UC#	*Use Case,* *(Federführende Instanz)*	*Beschreibung,* *Voraussetzungen*
AP-7	Schliessung SRACs (Lieferant Peripheriegerät)	Funktionsupdate zur Schliessung einer oder mehrerer Anwendungsbedingungen (SRACs). Unterscheidung zu AP-1 und AP-x: Zeitachse - weniger dringlich als bei diesen.
AP-8	Austausch Peripheriegerät	Der Fahrzeugeigentümer will/muss – für eine bestimmte Flotte/Fahrzeugtyp – ein bestimmtes Peripheriegerät durch ein funktional gleichwertiges anderes Modell des gleichen oder eines anderen Lieferanten) ersetzen. Annahmen für das neue Peripheriegerät: - es besitzt grundsätzlich bereits eine Typenzulassung mit dem Basissystem COAT; - die Peripheriegeräte sind grundsätzlich bereits zugelassen.
AA	**Änderung an COAT-Applikationen**	
AA-1	Kuratives Wartungsupdate für Bug-Fixes (Lieferant COAT-App)	Die COAT-App muss zum Vorschein gekommene Defekte zeitgerecht (d.h. innert weniger Wochen) beheben. Keine funktionalen Erweiterungen.
AA-2	Wartungsupdate Präventiv (Lieferant COAT-App)	Die COAT-App wird im Sinne eines Substanzerhaltes gewartet und technologisch à jour gehalten. Z.Bsp. Aufdatierung einer SW-Bibliothek/-Frameworks. *[Wahrscheinlichkeit solcher Updates zu klären.]*
AA-3	Minor Funktionsupdate für neue/verbesserte Funktion (Lieferant COAT-App)	Die COAT-App wird bezüglich ihrer Funktionalität weiterentwickelt. Minor Update. Keine Änderung an Interaktion mit Peripheriegeräten. (Kleinere) neue Funktionen kommen dazu, oder bestehende Funktionen oder Charakteristiken werden verbessert (z.B. zwecks Steigerung der Stabilität).
AA-4	Medium Funktionsupdate, mit Relevanz Interaktion Peripheriegerät	Die COAT-App erfährt eine Änderung einer Funktionalität, welche mit einer Änderung in der Interaktion mit Peripheriegeräte(n) einherkommt. Medium Update.
AA-5	Konfigurationsupdate (geänderte Einstellungen)	Änderung der statischen Konfiguration der App mit oder ohne Sicherheitsrelevanz. Keine Modifikation der Funktionalität der App, abgesehen vom Umstand, dass die Konfiguration eine - eigentlich bereits vorhandene – Funktionalität erstmals zur Anwendung kommen lässt, die im Sicherheitsnachweis bisher nicht bearbeitet wurde.
AA-6	Schliessung dringlicher Cybersecurity-Lücke(n) (Lieferant COAT-App)	Eine oder mehrere dringliche Cybersecurity-Lücke(n) müssen zeitgerecht (d.h. innert möglichst weniger Tage oder Wochen) geschlossen werden.

UC#	*Use Case, (Federführende Instanz)*	*Beschreibung, Voraussetzungen*
AA-7	Daten-Update (Lieferant COAT-App oder Fahrzeugbetreiber)	Update von Daten für die App, z.B. Update der Topologie Schweiz (allenfalls bei einer GLAT-App für die Lokalisierung erforderlich). Die Annahme ist, dass diese Daten-Updates sehr unregelmässig vorkommen und ohne Sicherheitsrelevanz sind. [Wahrscheinlichkeit und Sicherheitsrelevanz unklar, also vorerst lieber mitberücksichtigen.]
AA-8	Schliessung SRACs (Lieferant COAT-App)	Funktionsupdate zur Schliessung einer oder mehrerer Anwendungsbedingungen (SRACs). Unterscheidung zu AP-1 und AP-x: Zeitachse - weniger dringlich als bei diesen.
AA-9	Major Upgrade (Lieferant COAT-App)	Neue Softwareversion welche eine Kombination von Fehlerbehebung aller vorgängigen Use Cases Kombination von: - Defekte schliessen - Funktionalität erweitern (schliesst Verbesserungen nichtfunktionaler Aspekte ein) - Substanzerhalt
AA-10	Austausch App (Lieferant COAT-App)	Der Fahrzeugeigentümer will/muss – für eine bestimmte Flotte/Fahrzeugtyp – eine bestimmte App durch eine funktional gleichwertige andere App des gleichen oder eines anderen Lieferanten) ersetzen. Annahmen für die neue App: - es besitzt grundsätzlich bereits die Typenzulassung mit dem Basissystem COAT.
AA-11	Funktionsupdate bei ETCS-/ ATO-App (Lieferant COAT-App)	Das ETCS-/ATO-App erfährt eine Änderung ihrer ETCS- resp. ATO-Funktionalität, mit Änderung bei der Interaktion mit der Infrastruktur. Keine Änderung in der Interaktion mit Komponenten (Apps und/oder Peripheriegeräte).

Tabelle 4-1: Use Cases als Basis für Erweiterten Review

4.2.2 Wahrscheinlichkeit und Kritikalitäten bei Änderungen

Die Relevanz der Use Cases bestimmt sich im Wesentlichen aufgrund zwei Kriterien:

a) Wahrscheinlichkeit des Vorkommens des Use Cases,
b) Kritikalität des Use Cases hinsichtlich des effizienten Nachzugs der Zulassung.

Die Beurteilung der Kritikalität bei Erstzulassungen liegt definitionsgemäss eher tief, da Erstzulassungen - wie in Kapitel 3.5.1 angesprochen - oft die umfassende Ersterstellung von Sicherheitsnachweisen erfordert und somit bezüglich notwendiger Änderungen irrelevant sind. Trotzdem gibt es bestimmte Erstzulassungs-Szenarien, die sie sich auf frühere

Erstzulassungen abstützen und deren Sicherheitsnachweise unangetastet wiederverwenden sollen.

Es ist zudem von Bedeutung, dass Sicherheitsnachweise - oder thematische abgegrenzte Teile davon – deshalb möglichst ohne Modifikation übernommen werden können, weil andernfalls eine unerwünschte Vielfalt von stets noch zulassungstechnisch gültiger Versionen eines Sicherheitsnachweis entstehen wird.
In solchen Fällen werden Auflistungen der untergeordneten Sicherheitsnachweise, die in den Gesamt-Sicherheitsnachweisen geführt werden, zu unterschiedlichen Versionen eines - eigentlich gleichen - Sicherheitsnachweis-Dokuments referenzieren. Demnach müssen ältere stets noch referenzierte Version weiter unterhalten werden und dürfen nicht als obsolet behandelt werden. Eine allfällige weiterführende Arbeit (siehe Abschnitt 5.4.2, «Erweiterung mit der Sicht Fahrzeug-Instanz») wird diese Thematik weiter beschreiben können.

Das Resultat der Klassifizierung ist in Tabelle 4-2 zusammengestellt.

UC#	*Use Case*	*Wahrscheinlichkeit des Vorkommens*	*Kritikalität hinsichtlich Nachzug bei Änderungen*
E	**Erstzulassungen**		
EGG	Generisches Gesamtsystem COAT	1	Keine
EGF1	COAT-Gesamtsystem Fahrzeug	1	Mittel
EGF2	COAT-Gesamtsystem auf zusätzlicher Fahrzeugtyp	1	Hoch
EGCH	COAT aus Ausland, generisch	3	Mittel
EGFCH	COAT-Fahrzeug aus Ausland	2	Hoch
EPF	Erstzulassung neues PG auf Fzg	1	Sehr hoch
EPNSR	Erstzulassung neues NSR-PG	2	Mittel
EAG	Typenzulassung neue COAT-App	1	Hoch
EAF	Neue COAT-App auf Fahrzeugtyp	1	Mittel
AB	**Änderungen an Basissystem COAT**		
AB-1	Wartungsupdate Kurativ	1	Sehr hoch
AB-2	Cybersecurity-Lücke(n)	1	Sehr hoch
AB-3	Wartungsupdate Präventiv	1	Sehr hoch
AB-4	Minor Funktionsupdate	1	Hoch
AB-5	Schliessung von SRACs	1	Sehr hoch
AB-6	Medium Update m/Interaktion PG	*2*	Hoch
AB-7	Medium Update m/Interaktion App	*2*	Mittel
AB-8	Konfigurationsupdate	1	Hoch
AB-9	Austausch Basissystem COAT	2	Eher tief
AB-10	Major Upgrade	3	Eher tief
AP	**Änderungen an Peripheriegerät COAT**		
AP-1	Wartungsupdate Kurativ	1	Sehr hoch
AP-2	Wartungsupdate Präventiv	1	Sehr hoch

UC#	*Use Case*	*Wahrscheinlichkeit des Vorkommens*	*Kritikalität hinsichtlich Nachzug bei Änderungen*
AP-3	Minor Funktionsupdate	1	Hoch
AP-4	Medium Update m/Interaktion App	1	Hoch
AP-5	Zusätzliche Informationen	2	Sehr hoch
AP-6	Major Upgrade	3	Mittel
AP-7	Schliessung SRACs	1	Hoch
AP-8	Ersatz PG durch anderes PG	2	Sehr hoch
AA	**Änderungen an App COAT**		
AA-1	Wartungsupdate Kurativ	1	Sehr hoch
AA-2	Wartungsupdate Präventiv	1	Sehr hoch
AA-3	Minor Funktionsupdate	1	Hoch
AA-4	Medium Update mi/Interaktion PG	1	Hoch
AA-5	Konfigurationsupdate	2	Hoch
AA-6	Cybersecurity-Lücke(n)	1	Sehr hoch
AA-7	Daten-Update	2	Sehr hoch
AP-8	Schliessung SRACs	1	Hoch
AA-9	Major Upgrade	3	Mittel
AA-10	Ersatz durch neue App	2	Mittel
AA-11	Funktionsupdate ETCS-/ATO-App	2	Hoch

Tabelle 4-2: Klassifizierung Use Cases nach Vorkommen und Kritikalität bei Änderungen

4.3 Vorbereitung Durchlauf der Use Cases

4.3.1 Checkliste

Beim Durchspielen der Use Cases wird folgende Checkliste beigezogen:

Identifikation Klärung Use Case

- Bezeichnung, Beschreibung
- Verantwortlichkeiten / Federführung bei der Erarbeitung der Inhalte
- Präzisierungen / Unklarheiten / Unsicherheiten zum Use Case
- Arbeitshypothesen
  Relevante Arbeitshypothesen für den Review des Use Case?
- Varianten des Use Cases
  Varianten des Use Cases berücksichtigt, resp. später zu berücksichtigen?
- Erfolgskriterien
  Sind auf den bezogenen Use Case besondere Erfolgskriterien zu berücksichtigen?

Detaillierung der Änderung

- Einflussgebiet der Änderungen
  Eingrenzung resp. Einflussgebiet der Änderungen. Welche COAT-Teilsysteme sind mitbetroffen?

- Eingrenzende Effekte der Schnittstellen
  Effekt der Schnittstellen (tatsächlich und/oder potenziell) zur Eingrenzung der im Use Case zutreffenden Änderungen
- Betroffene Nachweis- und Integrationsthemen
  Identifikation der durch die Änderung betroffenen Themen relevant für die Nachweisführung, einschliesslich Integrationen.
- Sonstiges
  Weitere Ausführungen und Bemerkungen zur Änderung

Erforderliche Zulassungsarbeiten

- Überarbeitung der Zulassungsdokumentation
  Welche qualitativen Auswirkungen auf die Zulassungsdokumentation ergeben sich?
- Auswirkungen durch das Zulassungskonzept
  Nicht wünschbare Auswirkungen aufgrund des Zulassungskonzepts? Relevante Umstände?
- Weitere Auswirkungen bezüglich der Zulassung
  Nicht wünschbaren Auswirkungen, die nicht das Zulassungskonzept betreffen? Umstände?
- Kommentare
  Qualitativen Auswirkungen auf die Zulassungsdokumentation?

Tests, Verifikation & Validierung

- Qualifizierung V&V und Tests
  Qualifizierung der aufgrund der Änderung notwendigen Verifikation und Validierung und Tests.
- Erforderliche Testumgebungen
  Erforderliche Ausstattungen. Dies kann zum Beispiel bis hin zur Einschätzung der Komplexität einer benötigten Testumgebung führen
- Automatisierte Tests
  Relevanz von Durchführungsformen; Automatisierung der Prüfung (nicht nur bezgl. Testing)

Erkenntnisse

- Bewertung auf Agilität & Upgrade-Ability
  Einflüsse auf die Agilität / Upgradeability in der COAT-Produktpflege und -Evolution;
- Bewertung Zulassungskonzept
  - welche Elemente des Zulassungskonzepts bringen Erleichterung (oder eben nicht)?
  - Auffälligkeiten; entfallene oder zusätzliche Komplexitäten?
- Rahmenbedingungen für Reduktion Aufwand
  Potentielle u/o erforderliche Rahmenbedingungen zur Minimierung des Aufwands.
- Risiken
  Z.B. ungewohnte Komplexität kann zu Vereinfachungen und Helvetismen führen
- Chancen & Potentiale
- Handlungsbedarf

4.3.2 Überarbeitungsaufwände bei den Safety Cases

Individuell pro Use Case werden die erforderlichen Überarbeitungen der Safety Cases in tabellarischer Form im Anhang [Dok.1] erfasst und zusammengestellt.

Nachfolgende Tabelle 4-3 listet eine beispielhafte Zusammenstellung von Sicherheitsnachweisen auf, die bei einer realistischen Zusammenstellung eines Gesamtsystem COATs zu erstellen und zu unterhalten sein werden.

Exemplarisch wurden zwei separate spezifische Gesamtsicherheitsnachweise in die Liste aufgenommen, die stellvertretend für unterschiedliche Fahrzeugtypen stehen. Damit soll der Umstand berücksichtigt werden, dass COAT auf zahlreichen Fahrzeugtypen eingesetzt werden wird. Im Zulassungskonzept (Zulassungskonzept [Dok.4], Abbildung 10) erfolgt die Fahrzeugintegration dokumentarisch an letzter Stelle der Nachweiserbringung.

#	*Safety Case*	*Fazit*
GASC EVC		
SCA	GASC EVC	
GASC Peripheriegeräte		
SCB	GASC DMI	
SCC	GASC TIU	
SCD	GASC BTM	
SCE	GASC LTM	
SCF	GASC GLAT (Lokalisierung)	
SCG	GASC Radio	
SCH	GASC JRU	
SCI	GASC NSR-Gerät	
GASC System COAT 1.0		
SCJ	GASC GS-COAT - “Assemblage”	
SASC System COAT 1.0		
SCK-A	SASC Fzgtyp-Alpha - System COAT 1.0	
SCK-B	SASC Fzgtyp-Beta - System COAT 1.0	
Gutachten → nicht aufgelistet		

Tabelle 4-3: Template - Exemplarische Auflistung vorhandener Safety Cases

Die gemäss dem Template der Tabelle 4-3 identifizierten Konklusionen sind in Tabelle 5-1 in Kapitel 5.2.3 aufgeführt.

4.3.3 Kategorisierung erforderlicher Änderungen an Safety Cases

Die erforderlichen Änderungen an den Safety Cases beim Durchspielen eines Uses Cases können wie in Tabelle 4-4 kategorisiert werden:

	M - *Mandatory / Zwingend*	O - *Optional*
Generische Bedeutung	*Die identifizierte Aufarbeitung wird auch auf lange Sicht hin zwingend notwendig bleiben.*	*Die erforderliche Aufarbeitung ist fallweise zu identifizieren. Aufwand reduziert sich mit kontinuierlicher Reifung der Schnittstellen und Produkte allmählich, um langfristig als interoperables Teilsystem («plug-and-play») vollständig zu entfallen.*
E - Ersterstellung	ME inhaltliche Ersterstellung des Nachweises	n/a
I - Inhaltlich	MI Zwingende inhaltliche Aufarbeitung erforderlich.	OI fallweise inhaltliche Aufarbeitung erforderlich
R - Regression / Rückwirkungsfreiheit	MR Zwingender Nachweis einer Rückwirkungsfreiheit.	OR fallweise oder allgemeine (vereinfachte) Prüfung der Rückwirkungsfreiheit erforderlich
V - Versionierung nachführen	V Nachführen der Konfiguration aufgrund erfolgter Aktualisierung untergeordneter Nachweise	n/a
Ok Ok	kein Änderungsbedarf	n/a
n/a nicht zutreffend	nicht zutreffend	n/a

Tabelle 4-4: Kategorien von Änderungen an Safety Cases

Die Kategorie «Optional» Arbeit an Sicherheitsnachweisen ist dahingehend zu verstehen, dass diese Überarbeitungen von Safety Cases mit der Zeit zunehmender Reife von Technologie, Schnittstellen und realisierter Systeme abnehmen werden, sowohl qualitativ als auch quantitativ. Hierzu zwei denkbare Beispiele:

- Sobald eine Komponente (z.B. eine Schnittstelle) zur «commodity» wird, reduziert sich der Überarbeitungsaufwand zur reinen Formalität, in Form einfacher Aktualisierung im Konfigurationsmanagement. Letzteres lässt sich zudem mittels geeigneter IT-Werkzeuge noch weiter vereinfachen.
- Stehen – allfällige oder zwingend notwendige – Regressionstests zur Diskussion und lassen sich diese automatisieren, so reduziert sich der händische Aufwand auf die Prüfung des Endresultats. Ebenso reduziert der erforderliche Bearbeitungszeitraum um einen hohen Faktor gegenüber dem Zeitbedarf herkömmlicher Testmethoden bei Bahnsystemen.

4.4 Getroffene Annahmen

Anhand der Use Cases wurden Annahmen definiert und in nachfolgender Tabelle 4-5 zusammengestellt. Diese Arbeitshypothesen ergänzen die aktuellen verfügbaren COAT Systemarchitekturen und das Zulassungskonzept insoweit, dass die Durchführung des Erweiterten Reviews zu konkreteren Erkenntnissen führen kann.

#	*Getroffene Annahme / Arbeitshypothese*	*Bemerkung / Alternative*
Gesamtsystem COAT		
1	Intention für COAT primär für ETCS-Betrieb mit Lokalisierung gemäss SR40. ATO ist optional.	
2	Generischer SC Gesamtsystem: für die Schweiz wird ein einziger solcher SC bestehen, der im Sinne eines Werkzeugkastens die zulässigen (typenzugelassenen) Peripheriegeräte auflistet, wie z.B. zwei Modelle von Balisenlesern unterschiedlicher Hersteller. Eine Applikation legt fest, welches der beiden Modelle in einem bestimmten Fahrzeug konkret zur Anwendung kommt.	Alternative: für jede spezifische Zusammenstellung (Konfigurationen) eines COAT-Gesamtsystems wird ein separater SC geführt werden.
3	Ein spezifischer Safety Case für ein Gesamtsystem muss eine bestimmte Wahl der Applikationen und Peripheriegeräte vornehmen.	
Basissystem COAT		
4	GASC EVC steht für das ganze Basissystem COAT gemäss November-Ausgabe OCORA	Falls nein: Alternative?
5	Der GASC EVC beinhaltet die erforderlichen Nachweise für den CCS-Bus.	Falls nein: dann wo abgedeckt?
6	Der GASC EVC beinhaltet die erforderlichen Nachweise für das RTE / Betriebssystem.	Falls nein: wo abgedeckt?
7	Der GASC EVC beinhaltet die erforderlichen Nachweise für die Services gemäss OCORA-Architektur.	Falls nein: wo abgedeckt?
Schnittstellen und Integration		
8	Es werden die in Kapitel 2.4 beschriebene, und in Abbildung 5 dargestellte Gesamtsicht und Auflistung der erforderlichen Integrationsaufgaben zugrunde gelegt.	Allfällige Alternative zu klären.
9	Schnittstellen werden triagiert bezüglich ihrem zukünftigen Bedarf für händische Integrationsaufwände: - auf Dauer Integrationsleistungen erfordernd; - mit der Zeit zur «Commodity» reifend.	Auflistung zu Reviewen. Hat Einfluss auf die Matrix resp. die Klassifizierung der Überarbeitungsaufwände eines SC hinsichtlich des Nachweises der Rückwirkungsfreiheit: optional (orange) oder muss (mandatory, rot).

#	*Getroffene Annahme / Arbeitshypothese*	*Bemerkung / Alternative*
CCS-Bus		
10	Nicht festgelegt: welche Verantwortlichkeiten garantiert der CCS-Bus für den Austausch / Übermittlung von Informationen insbesondere zwischen Peripheriegeräten und den Applikationen? Z.B. bei einem publish/subscribe-Konzept würde der CCS-Bus gewährleisten, dass entgegengenommene Daten an die abonnierten Empfänger zugestellt werden.	Ja: ermöglicht zusätzliche Entkopplung zwischen App und PG. Applikation erfordert keine besondere Kenntnis über die Identität und Merkmale des Absenders. Falls Nein: Apps müssen mit spezifischen PG interagieren und mit ihren Besonderheiten bezgl. Informationslieferung umgehen können.
11	Nicht festgelegt: vordefinierte Datenformate für den Austausch / Vermittlung von Informationen?	Falls Ja: bildet Grundlage für obige Annahme, d.h. ermöglicht zusätzliche Entkopplung zwischen App und PG. Falls Nein: Apps müssen mit spezifischen PG interagieren und mit ihren Besonderheiten bezgl. Informationslieferung umgehen können.
12	Nicht festgelegt: die Kommunikation und Informationsaustausch unter Applikationen und Services kann über den CCS-Bus erfolgen.	Falls Ja: eine bereits zur Verfügung stehende vereinfachte und standardisierte Methode wird genutzt. Und vereinfacht die Integration zwischen Apps und Services und untereinander. Falls Nein: potenziell publiziert jeder Service seine eigene API zuhanden der Applikationen. Zwei Applikationen, die zu-/miteinander Informationen austauschen, müssen dies auf proprietäre Weise tun, was zu festen gegenseitigen Abhängigkeiten führt.
Peripheriegeräte		
13	Der Nachweis der Integration eines Peripheriegerätes in einen bestimmten Fahrzeugtyp wird inhaltlich im SASC GS-COAT (spezifischer SC Gesamtsystem) behandelt.	Aktuelles Verständnis des Zulassungskonzepts, welches diesen Punkt nicht explizit klärt. Alternative wäre ein dezidierter SC dafür, welcher überdies Duplikate aufgrund der Existenz mehrerer SASCs vermeiden würde.
14	Der Nachweis der Integration eines Peripheriegerätes in einer bestimmten Infrastruktur wird inhaltlich im GASC PG (Typenzulassung PG) behandelt.	Konklusion aus dem Zulassungskonzept.

#	*Getroffene Annahme / Arbeitshypothese*	*Bemerkung / Alternative*
Applikationen		
15	Für die einzelnen Apps werden keine dezidierten SC geführt, sondern sie werden im generischen SC für das Gesamtsystem geführt.	

Tabelle 4-5: Getroffene Annahmen für den Erweiterten Review

4.5 Durchlauf der Use Cases

Die Matrix in [Dok.1] dokumentiert die detaillierten Ergebnisse der Einflüsse der Uses Cases auf die (vorhandene) Sicherheitsnachweise dar.

Bei der Erfassung der notwendigen Überarbeitungen gelten die in Tabelle 2-1 definierten Kürzel und Beschreibungen.

5 Zusammenfassung der Resultate

5.1 Zielsetzung

Aus den Erkenntnissen der einzelnen Use Case-Untersuchungen werden nachfolgend summarisch Auffälligkeiten hinsichtlich der Life Cycle-Perspektive von Zulassungsdokumentationen festgestellt und beurteilt.

Insbesondere folgende Punkte:

- Welche Safety Cases müssen ungewöhnlich häufig angepasst werden?
- Welche Elemente und Teilsysteme in COAT sind inwiefern bezüglich ihrer Volatilität eingeschränkt (Funktionalitäten, Konfigurationsbereiche u.v.m.)?
  Schafft es das Zulassungskonzept, die gewünschte Agilität konzeptionell zuzulassen?
- Indikatoren, die für ein noch nicht optimales Arrangement der Safety Cases sprechen? Sei es die thematische Aufteilung der Safety Cases oder eher unscharf definierte Abgrenzungen zwischen diesen (Stichwort akzeptable SRACS)?
- Welche ersten Empfehlungen und Handlungsrichtungen können formuliert werden in Bezug auf das Zulassungskonzept; die COAT-Architektur? Allenfalls sogar als Input für Anforderungswerke und der Gestaltung der Schnittstellen?

5.2 Überarbeitungsaufwände bei den Safety Cases

5.2.1 Allgemeine Beobachtungen

Generell ist zu beobachten, dass selbst bei kleinen und punktuellen («chirurgischen») Änderungen am System COAT zahlreiche und vermeintlich themenfremde Safety Cases angerührt werden müssen.

Modularisierung der Safety Cases

Die einzelnen Safety Cases umfassen (zu) grosse Themengebiete, und folglich besteht eine hohe Wahrscheinlichkeit, dass Änderungen inhaltliche Überarbeitungen notwendig machen.

Die Safety Cases müssten deshalb verstärkt modularisiert werden. Dies aufgrund der bei COAT zu erwarteter Häufigkeit von Änderungen an den Systemen, die mit den Usanzen bei bisheriger Fahrzeugausrüstungen nicht (mehr) vergleichbar sind. Mit dieser Massnahme würde die - durch COAT letztendlich geforderte - Wiederverwendbarkeit der Safety Cases gesteigert und summarisch die Volatilität der einzelnen Safety Cases gesenkt.

Es ist nachvollziehbar, dass das Zulassungskonzept es bewusst vermieden hat, die Themenfelder für die einzelnen Safety Cases zu spezifizieren, da dies nicht die Aufgabe einer regulierenden Instanz ist (oder in diesem Fall ein «verlängerter» Arm des Systemführers und der Zulassungsbehörde). Zu Recht liegt dies in der Verantwortung des Erstellers der Sicherheitsnachweise - er ist dafür verantwortlich, alle notwendigen Sachverhalte zu identifizieren und zu behandeln, soweit es die Thematik des Safety Cases erfordert. Das Zulassungskonzept könnte hingegen Themen im Sinne von Minimalforderungen aufführen, welche die Safety Cases zu bearbeiten haben. Damit würde die Verantwortlichkeit nicht angetastet.

Trotz detaillierter Modularität bleibt der Umstand, dass zahlreiche Safety Cases ihre Verweise auf neue Versionen der untergeordneten Safety Cases nachführen müssen. Sofern sich die Modifikation eines Safety Cases daraufhin beschränken lässt, so reduziert sich die Modifikation auf eine reine Formalität. Im Unterschied zu inhaltlichen Überarbeitungen von Safety Cases sind formale Aufdatierungen von Konfigurationen wesentlich weniger aufwändig, insbesondere seitens deren Begutachtungen.

Man kann sich dabei die Anwendung eines eigentlichen Konfigurationsmanagements für Safety Cases vorstellen, welches - allenfalls unterstützt durch geeignete IT-Werkzeuge - vergleichsweise sehr effizient mit Änderungen umgehen kann. Als konkretes Beispiel könnte eine internationale Konfigurationsdatenbank für COAT-Komponenten die Agilität eines globalen COAT-Marktes bedeutend begünstigen.

Integrationsnachweise

Aufgrund mangelnder Klärung, welche Integrationsnachweise in welchen Safety Cases zu behandeln sind, mussten im Rahmen des vorliegenden Erweiterten Reviews entsprechende Annahmen getroffen werden.

Diese Annahmen haben beispielsweise dazu geführt, dass alle spezifischen Sicherheitsnachweise für das System COAT inhaltlich nachgeführt werden müssen, wenn sich bezüglich des Einbaus eines Peripheriegerätes in ein Fahrzeug (sei es bezüglich des betreffenden Fahrzeugtyp, oder selbst auch falls allgemein bezüglich aller Fahrzeugtypen) etwas ändern sollte, selbst wenn die Änderung minim ist. Aus der Aufwandsperspektive wäre es in diesem Fall wünschbar, dies im Rahmen eines safety cases für das Peripheriegerät abhandeln zu können, und somit der spezifische Gesamtsicherheitsnachweis schliesslich nur noch die Verweise auf seine untergeordneten Safety Cases aktualisieren müsste.

Mit einer Klärung durch das Zulassungskonzept kann der Review entsprechend nachgezogen und die gewonnenen Erkenntnisse angepasst werden.

Standardisierte Schnittstellen

Im Konzept COAT kommen eine Anzahl standardisierter Schnittstellen zur Anwendung, teilweise spezifisch auf das Konzept COAT bezogen, andere bezüglich des Einsatzes von ETCS, ATO usw.

Wie in Kapitel 2.4.4 bereits erläutert, wird von zahlreichen Schnittstellen erhofft, dass bei diesen - zumindest sobald als möglich - der Nachweis der Konformität zur Schnittstelle genügen würde. Es kann jedoch nicht verlässlich vorausbestimmt werden, ab welchem Zeitpunkt in der Zukunft dies für welche Schnittstelle zutreffen wird.

Heute entsprechende Annahmen zu treffen ist spekulativ. Gleichwohl hat sich gezeigt, dass in der Analyse der Use Cases eine sehr pauschale Unterscheidung zwischen potenziell bleibendem hohen und mit der Zeit nachlassendem Integrationsaufwand versucht werden muss. Dies erfolgte im Review schliesslich mittels der Klassifikation «optional» versus «mandatory», zum Beispiel OR oder MR (optionale oder zwingende Regressionsprüfung). Bei den als «optional» bewerteten Aufwänden setzt man darauf, dass sich diese mit zunehmender Reife der Technologien und Produkte zunehmend reduzieren und schliesslich einmal entfallen werden.

Diese im Review erfolgten Bewertungen sollten mit den zuständigen COAT-Projektteams besprochen werden.

5.2.2 Beobachtungen bezogen auf Use Cases

Erstzulassungen (Use Cases Gruppe E)

Bei Erstzulassungen von ausländischen Gesamtsystemen in der Schweiz fällt auf, dass die Safety Cases für Peripheriegeräte, welche als Typenzulassungen gedacht sind, bezüglich der Integration mit Schweizer Infrastrukturen inhaltlich überarbeitet werden müssen (insbesondere die BTM/LTM, GLAT, JRU etc.). Dies gilt selbst dann, wenn sich der Nachweis auf reine Formalitäten beschränkt.

Beim Use Case EPF, der Erstzulassung neuer Peripheriegeräte, fällt auf, dass die Integrationsnachweise dokumentarisch nicht gebündelt gehandhabt werden können, sondern diese in unterschiedlichen Safety Cases aufgehoben sein werden. Alternative dokumentarische Strukturierungen könnten die Minimierung der Zulassungsaufwände begünstigen.

Bei den Use Cases (z.B. EPNSR, EAG, EAF), welche Rückwirkungen auf bestehende Applikationen zur Folge haben können, müssen die entsprechenden Rückwirkungsnachweise jeweils im generischen Systemsicherheitsnachweis für das (Gesamt-)Systemsystem COAT inhaltlich nachgeführt werden. Das Verständnis ist zu klären darüber, ob ein solcher Safety Case solche ausführlichen inhaltlichen Ausführungen enthalten sollte, oder lieber auf untergeordnete Safety Cases verweisen will, die diese Thematik behandeln. Dieser Punkt entspricht der allgemeinen offenen Frage, wo und wie gemäss Zulassungskonzept die Nachweise für die Applikationen geführt werden sollen.

Änderungen am Basissystem COAT (Use Cases Gruppe AB)

Im Allgemeinen hat sich aufgrund der Use Cases mit einer Ausnahme gezeigt, dass Änderungen am Basissystem COAT (dem EVC, RTE, CCS-Bus u.v.m.) erwartungsgemäss innerhalb der entsprechenden Safety Cases (GASC EVC) gehandhabt werden können.

Die Ausnahme bezieht sich auf den Umstand, dass die Überprüfung möglicher Regressionen auf die Applikationen im Safety Case für das Gesamtsystem COAT behandelt werden müssen. (Siehe analoge Beobachtung bei Erstzulassungen.)

Änderungen an Peripheriegeräten (Use Cases Gruppe AP)

Diese Gruppe von Use Cases ähneln sich sehr und unterscheiden sich im wesentlich nur in Bezug auf die Integration mit den umgebenden Komponenten wie Basissystem und den Applikationen.

Da davon ausgegangen werden kann, dass jedes Peripheriegerät von einer oder mehreren Applikationen in Anspruch genommen wird (z.B. davon Information verarbeitet), muss die Regression auf die Applikationen (und Services) behandelt werden. Gemäss Verständnis des Zulassungskonzepts geschieht dies jeweils im GASC-GS-COAT, was thematisch eher unnatürlich wirkt und daher vermutlich unerwünscht ist.

Es wird deshalb empfohlen zu untersuchen, in welchen alternativen Safety Cases oder Dokumenten die Nachweise der Integration zwischen Applikationen und Peripheriegeräte behandelt werden können. Auf diese könnte dann der GASC-GS-COAT verweisen.

Bezüglich der Integrationsnachweise zwischen Peripherie und Infrastrukturen (z.B. BTM) gilt wiederum die analoge Beobachtung aus den Use Case-Gruppen Erstzulassungen und Änderungen am Basissystem COAT.

Änderungen an Applikationen (Use Cases Gruppe AA)

In Analogie zu obigen Beobachtungen fragt sich, ob die inhaltliche Behandlung von COAT-Applikationen im GASG-GS-COAT sinnvoll ist.

Die Applikationen gehören zu den hauptsächlichen Komponenten der COAT-Architektur, welche ausserdem von beliebigen und dezidierten Lieferanten stammen sollen[5]. Es bedeutet, dass die entsprechende Safety Case-Dokumentation von diesen Lieferanten stammen werden, und somit dokumentarisch separat zu den Safety Cases anderer Lieferanten gehandhabt werden müssen.

Dies erfordert Klärung mit dem Zulassungskonzept. Es wird erhofft, dass sich das Bild danach wieder relativieren wird.

5.2.3 Beobachtungen bezogen auf Safety Cases

In folgender Tabelle 5-1 werden spezifische Beobachtungen zu den einzelnen Safety Cases festgehalten.

#	*Safety Case*	*Feststellungen*
Allgemeines		
…	Alle Safety Cases	- Generell ist zu beobachten, dass die thematischen Inhalte der Safety Cases sehr weit definiert sind, mit der Folge, dass selbst bei kleinen und punktuellen («chirurgischen») Änderungen am System COAT eine grössere Anzahl von Safety Cases von der Nachführung betroffen sind. - Notwendig ist eine stärkere Modularisierung mit expliziten Zuteilungen / Verteilung der minimal zu behandelnden Themen auf die Safety Cases. - Eine Unterscheidung zwischen untergeordneten und übergeordneten Safety Cases könnte nutzbringend sein: Eine Sammlung untergeordneter Safety Cases würden die unterschiedlichen Teilthemen inhaltlich behandeln. Die übergeordneten Safety Cases, normalerweise auf Stufe des Gesamtsystems COAT (generisch oder spezifisch) angesiedelt, würden primär Konfigurationen zusammenstellen und hierzu eine Anzahl relevanter untergeordneter Safety Cases referenzieren.
GASC System COAT 1.0		
SCA	GASC EVC	- Die Entflechtung zwischen EVC (inkl. RTE etc) und dem CCS-Bus resp. der Schnittstellen sollte in Betracht gezogen werden. Ein solcher Entscheid wird letztendlich vor allem davon abhängen, wie der CCS-Bus konzipiert werden wird, und insbesondere mit welchen - allenfalls - volatilen Eigenschaften dieser konzipiert werden wird (z.B. vordefinierte Datenformate, die regelmässige Nachführungen zur Folge haben werden). Es kann sein, dass dieser Punkt sich eher an die Gestaltung der

[5] Dem Vernehmen nach besteht noch kein Businessmodell für die COAT-Plattform resp. OCORA-Architektur, jedoch kommt aus Gesprächen im COAT-Projekt klar zum Vorschein, dass dies ein Muss darstellt.

#	*Safety Case*	*Feststellungen*
		OCORA-Schnittstellen richten als an den CCS-Bus selbst (im Projekt zu klären). - Bezüglich der OCORA-Architektur ist die Zuständigkeit für die sog. Services undefiniert. In diesem Review wurden die Services allerdings nicht behandelt.
SCB SCC SCD SCE SCF SCG SCH	GASC DMI GASC TIU GASC BTM GASC LTM GASC GLAT (Lokalisierung) GASC Radio GASC JRU	Summarisch für die Safety Cases der Peripheriegeräte: - GASCs: die generischen Nachweise sind inhaltlich in sich abgeschlossen. Es wird dabei angenommen, dass darin die Integration mit dem CCS-Basissystem enthalten ist. - Es wird angenommen, dass der Nachweis der Integration / Zusammenarbeit mit Applikationen durch Safety Cases der Applikation behandelt wird. - Das Zulassungskonzept wird so verstanden, dass der Nachweis der Integration / Zusammenarbeit mit Applikationen durch die Safety Cases für die Applikation behandelt wird. - Es wäre wünschbar, dass ein separater (allenfalls spezifischer) Safety Case den Nachweis der Integration / Zusammenarbeit mit Infrastrukturen sicherstellt. Es ist denkbar, einen solchen gewissermassen als SASC-Peripheriegerät zu bezeichnen.
SCI	GASC NSR-Gerät	- Es fehlt derzeit die Klärung durch die COAT-Architektur, inwieweit diese gewährleisten kann, dass bei der Einführung/Änderung eines nicht sicherheitsrelevanten Peripheriegerätes keine Regression/Rückwirkung auf das System einschliesslich der sicherheitsrelevanten Funktionen entstehen kann. Falls nicht oder teilweise der Fall, welcher Safety Case ist verantwortlich für den entsprechenden Nachweis? (SC für PG oder z.B. SC GASC-EVC?)
GASC System COAT 1.0		
SCJ	GASC GS-COAT System Version 1.0	- Dieser Safety Case ist sehr divers und weist (gemäss getroffener Annahmen) eine Mischung unterschiedlicher Inhalte auf: einerseits listet er eine Sammlung zugelassener Peripheriegeräte und Applikationen für die Anwendung Schweiz (Auflistung mehrerer PGs gleichen Zwecks z.B. mehrere BTMs) auf, andererseits muss er bedeutende Themen inhaltlich behandeln (sämtliche Applikationen). - Da der SC die Applikationen und deren Integration mit den zutreffenden Peripheriegeräten behandelt, wird dieser SC von vielen Use Cases tangiert. Eine Auslagerung der Nachweise für die Applikationen würde Entlastung bringen und die Nachführung auf die Aktualisierung zulässiger Konfigurationen reduzieren. - Oft muss die Integration zwischen Applikationen mit Peripheriegeräten auf Rückwirkungen überprüft werden. Diese Nachweisführung wird vorteilhafterweise in separaten Dokumenten geführt.

#	*Safety Case*	*Feststellungen*
		- Es fällt auf, dass der GASC GS-COAT Inhalte aufweist, die von unterschiedlichen Lieferanten stammen werden. Jede Applikation kann von einem unterschiedlichen Lieferanten stammen. Dieser Umstand stellt infrage, wie solche GASCs praktisch gehandhabt und bei Änderungen wiederverwendet werden können. - Aus dem Zulassungskonzept heraus gilt das Verständnis, dass für die Anwendung COAT in der Schweiz ein einziger solcher SC erarbeitet und unterhalten wird. Dieses Konzept erfordert eine zentrale gesamtschweizerische Verwaltung dieses einen SC, stellvertretend für alle EVUs welche in der Schweiz Fahrzeuge betreiben, was zu Interessenkonflikten (z.B. unterschiedliche Prioritäten in der Evolution des SC) führen kann. Ein alternatives Verständnis wäre, dass ein GASC GS-COAT für jede zulässige - respektive zur Anwendung kommende - Konfiguration eines Gesamtsystems COAT Schweiz erstellt und unterhalten wird. Auf dieser Basis bewahren die EVUs ihre Autonomie über ihre bevorzugten Konfigurationen (d.h. Zusammensetzungen ihrer COAT-Plattform). Diese Flexibilität wäre für den Lebenszyklus ihrer COAT-Ausrüstungen vorteilhaft. - Diese Safety Cases werden versioniert geführt werden müssen, und mehrere Versionen werden gleichzeitig ihre Gültigkeit erhalten müssen. Es kann nicht erwartet werden, dass eine neue Version des GASC automatisch zur Nachführung aller SASC führen muss.
SASC System COAT 1.0 für jeden Fahrzeugtyp		
SCK-A SCK-B	SASC Fzgtyp-Alpha System COAT 1.0 SASC Fzgtyp-Beta System COAT 1.0	- Diese Safety Cases beschränken sich auf die Fahrzeugintegration ihrer Peripheriegeräte. Dank diesem eher eingegrenzten Scope sind sie nur wenigen Änderungen ausgesetzt. - Das Handling der spezifischen Safety Cases könnte dahingehend optimiert werden, indem für den Nachweis der Integration / Zusammenarbeit mit Fahrzeugen separate spezifische Safety Cases oder Dokumentationen erstellt werden. Der Nutzen wäre, dass dieser SASC sich dann vermehrt auf die Zusammenstellung einer gültigen Konfiguration COAT fokussieren kann. - Diese Safety Cases werden versioniert geführt werden müssen, und mehrere Versionen werden ihre Zulassung erhalten können. Es kann nicht angenommen werden, dass eine neue Version des SASC nicht zwingend auf alle Fahrzeuge des Typs angewendet (upgrade) werden wird, weshalb die Vorgängerversion des SASC weiterhin gültig bleibt bis zu einer expliziten Deklaration der Obsolenz.
SASC System COAT 1.0 – für jedes einzelne Fahrzeug		
SCL	SASC Fahrzeug #X	Folgt nach. Damit sollen allfällige Anforderungen resp. Rückwirkungen an die GASC und SASC veranschaulicht werden.

Tabelle 5-1: Summarische Beobachtungen zu den einzelnen Sicherheitsnachweisen

5.3 Empfehlungen

An dieser Stelle wird eine erste Anzahl von Empfehlungen abgegeben, welche, wenn berücksichtigt, zu reduzierten Aufwänden und beschleunigten Verarbeitung in der Zulassung führen können.

Nach Diskussion und Klärung dieser Punkte im COAT-Projekt kann der Review nachgeführt und anschliessend weiterführende Empfehlungen identifiziert werden.

5.3.1 Empfehlungen an das Projekt COAT

(1) Die in dieser Arbeit getroffenen und in Tabelle 4-5 zusammengestellten Annahmen und Hypothesen sollten auf ihre Richtigkeit hin diskutiert, bestätigt oder korrigiert werden.

(2) Ein Businessmodell, oder Anforderungen vom Business an COAT/OCORA, wäre hilfreich. Es sollte insbesondere die durch OCORA zu unterstützenden Lieferantenrollen deklarieren.
In Gesprächen im COAT-Projekt wird offensichtlich, dass gewisse Lieferantenrollen (zB. ein unabhängiger Lieferant für COAT-Applikation) zwingend ermöglicht werden sollen; aber es fehlt eine entsprechende Referenzdokumentation.

5.3.2 Empfehlungen an die Systemarchitektur COAT

(3) Konkretisierung der Funktionalität des CCS-Busses, insbesondere welche Dienstleistung dieser welchen anderen Komponenten des COAT-Ökosystems erbringen wird.
Je nach Ausgestaltung würden Änderungen am System potenziell die Tragweite notwendiger Modifikationen an COAT-Komponenten als auch die Aufwände bei der Verifikation reduzieren:

- Ein standardisierter CCS-Bus, der neu hinzugefügte Datenformate (z.B. aufgrund des Einsatzes neuer Peripheriegeräte) generisch verarbeiten kann, ohne dass dies eine Modifikationen des Basissystem erfordert.
- Funktionalität in Erwägung ziehen, welche gewährleisten, dass von Peripheriegeräten zur Verfügung gestellte Informationen zu den betreffenden Applikationen gelangen und von diesen empfangen werden können.
  Gelingt dies, muss bei zahlreichen Änderungen die Integration zwischen Applikationen mit Peripheriegeräten nicht zwingend neu geprüft werden (Check auf Rückwirkungen).

5.3.3 Empfehlungen an das Zulassungskonzept COAT

(4) Das Zulassungskonzept sollte die bei modularen Systemen erforderliche Gewaltentrennung, das heisst die Entflechtung der Themenbereiche COAT, ETCS und ATO, strikt einhalten.
Die grundlegenden COAT-Konzepte müssen universell bearbeitet werden, unabhängig vom offensichtlichen geplanten Einsatz mit ETCS- und ATO-Onboardfunktionalität. Das Basissystem COAT darf spezifische ETCS-Funktionen und Sachverhalte nur indirekt ansprechen.
Anders gesagt, ein COAT muss bestehen können als wären ETCS und ATO kein Thema; hypothetisch z.B. als wenn in den Fahrzeugen keine oder aber weiterhin nationale Zugbeeinflussungssysteme eingesetzt würden.

(5) Die Systembeschreibung [Dok.3] der ENOTRAC sollte an die zwischenzeitlich publizierte OCORA Alpha-Architektur angepasst und überarbeitet werden.
In diesem Rahmen wäre es auch sinnvoll, im Basissystem COAT (resp. dem Umfang des GASC EVC) die wesentlichen Komponenten wie EVC, RTE, Services u.s.w. zu unterscheiden. Je nach angestrebtem Sourcing-/Lieferantenmodell wird dies zulassungsrelevant sein werden.
Allenfalls müsste anschliessend auch das Zulassungskonzept [Dok.4] dahingehend konkretisiert werden.

(6) Das Zulassungskonzept sollte Apps als eigenständige Entität behandeln (allenfalls als COAT-Interoperabilitätskomponente betrachten). Es ist zu prüfen, ob hierfür separate generische und spezifische SiNa-Dokumentationen sinnvoll sind.

(7) Aufgrund der vorliegenden Resultate sollte geprüft werden, ob die Safety Cases noch weiter modularisiert, und somit in weitere untergeordnete Safety Cases aufgeteilt werden sollen. Die Beobachtung ist, dass das Handling von - insbesondere inhaltlich eingrenzbarer - Änderungen am System COAT vereinfacht werden könnte.
Beispiele:

- Use Case AA-6, der Nachweis für die Schliessung einer Cybersecurity-Lücke in einer Applikation kann in einem Bündel von Teilnachweisen spezifisch zu dieser Applikation geführt werden. Der generische Gesamtsystem-SC erhält eine aktualisierte Referenz zum Teilnachweis. Keine inhaltliche Aufarbeitung erforderlich.
- Use Case AP-6, ein aktualisiertes Peripheriegerät, wird im Bündel von Teilnachweisen spezifisch zu diesem Gerät geführt. Die – wahrscheinlich zahlreich bestehenden – spezifischen Gesamtsystem-SCs erhalten eine aktualisierte Referenz. Eine – potenziell mehrfach duplizierte – inhaltliche Aktualisierung entfällt.
- Die nachstehende Forderung (8) bezüglich der Verantwortlichkeit pro Safety Case wird erfüllt.

(8) Die Safety Cases müssen ausweisen, wer - oder welcher Lieferant - dafür verantwortlich zeichnet. Für den einzelnen Safety Case soll jeweils nur ein Lieferant (oder andere Organisation) verantwortlich sein müssen.
Dies ist derzeit bei generischen und spezifischen Gesamtsystem-SCs nicht der Fall: deren Inhalte stammen grundsätzlich von unterschiedlichen Lieferanten.

(9) Es stellt sich die Frage bezüglich der Integration, und inwiefern diese im Zulassungskonzept (oder anderswo?) behandelt werden müssen, insbesondere:
- Identifikation der notwendigen Integrationsschritte
- Identifikation der integrationsrelevanten Schnittstellen
- Klassifikation Reifegrade der Schnittstellen, aktuell und die Tendenz f.d. Zukunft
- Einschätzung der aktuellen Integrationsaufwände für die Schnittstellen (qualitativ)
- entsprechend als erforderliche inhaltliche Bestandteile der SiNa identifizieren?

(10) Es sollte wiedererwägt werden, ob weiterhin ein einziger zentraler, für die gesamte Schweiz allgemeingültiger GASC GS-COAT (generischer Gesamtsystemnachweis) geführt wird, oder aber das Prinzip individueller GASC GS-COAT für jede zulässige Zusammensetzung eines Gesamtsystems COAT Schweiz anzuwenden ist.

5.4 Nächste Schritte

5.4.1 Verarbeitung der Erkenntnisse des Erweiterten Reviews

Mit dem vorliegenden Bericht werden folgende nächsten Schritte empfohlen:

- Spiegelung der Erkenntnisse mit der COAT Systemarchitektur
- Weitere Angleichung an die OCORA-Architektur
- Spiegelung der Erkenntnisse mit dem Zulassungskonzept COAT
- Einbezug des Eisenbahnpakets 4
- Korrelation respektive Auswirkungen auf das Bolli-Konzept

5.4.2 Weiterarbeit am Erweiterten Review

Für die vorliegende Arbeit sind nachstehende fortführende Arbeiten sinnvoll (gemäss Vereinbarung mit smartrail 4.0):

- Übersetzung des Berichtes in englische Sprache
- Matrix: Erweiterung und Verfeinerungen:
  - Verfeinerung Inhalte der SiNa: Auflistung untergeordneter SiNa
  - Verfeinerung der Art der erforderlichen Änderung
  - Ergänzung durch Bewertungen / Würdigungen (gut, fraglich, kritisch, sollte verhindert/verbessert werden)
  - Erweiterung mit der Sicht Fahrzeug-Instanz, welche zu Einsichten über die Praktikabilität in der Handhabung unterschiedlicher Versionen der Safety Cases führen kann.
- Überarbeitungsbedarf gemäss den Resultaten aus COAT Systemarchitektur und Zulassungskonzept
- Evaluation der Potenziale durch verstärkte Automatisierungen, sei es bei den Nachweisführungen (z.B. zur Beschleunigung mittels automatisierter Integrationstest) als auch bei der Zusammenstellung aktualisierter Gesamtsicherheitsnachweise (KM für Safety Cases).
- Behandlung der Services (gemäss OCORA-Architektur) mittels spezifischer Use Cases.

6 ANHANG

6.1 Referenzliste

# Titel	*Beschreibung, Datei / Link*	*Quelle*
Erweiterter Review mittels Use Cases		
Dok.1: Erweiterter Review mittels Use Cases: Matrix Änderungen an Safety Cases	EBBE-MSB-190015.1.3-D2 Version 1.0	EBBE
Dok.2: Erweiterter Review mittels Use Cases: Lieferantenmodelle für COAT-Systeme	EBBE-MSB-190015.1.3-D4 Version 1.0	EBBE
COAT Zulassungskonzept		
Dok.3: Systembeschreibung COAT, Version 1.0	ECH-429.03-003.V1.0.Systembeschreibung_COAT.pdf	Enotrac
Dok.4: Zulassungsverfahren COAT, Version 1.0	ECH-429.03-005.V1.0.Zulassungsverfahren_COAT.pdf	Enotrac
Dok.5: Analysebericht Zulassung COAT, Version 1.0	ECH-429.03-004.V1.0.Analysebericht_Zulassung_COAT.pdf	Enotrac
OCORA-Projekt		
Dok.6: OCORA Architecture - Alpha Release - Architecture Diagrams	dd. 04.11.2019 «OCORA Architecture - Alpha Release - Architecture Diagrams.pptx» OCORA Public	SR40 Projekt COAT; OCORA project
Dok.7: OCORA Architecture - Beta Version	Draft dd. 19.04.2020 OCORA-20-002-Beta_Technical-Slide-Deck	SR40 Projekt COAT
CENELEC-Normen		
Dok.8: EN 50126 Bahnanwendungen - Spezifikation und Nachweis von RAMS	dd. Oktober 2017 Teil 1: SN-EN 50126-1:2017 Teil 2: SN-EN 50126-2:2017	EN / SN / Electro-Suisse

# Titel	*Beschreibung, Datei / Link*	*Quelle*
Dok.9: EN 50128 Bahnanwendungen – Software für Eisenbahnsteuerungs- und Überwachungssysteme	dd. Juni 2011 SN-EN 50128:2011	EN / SN / Electro-Suisse
Dok.10: EN 50129 Bahnanwendungen – Sicherheitsrelevante Kommunikation in Übertragungssystemen	dd. September 2010 SN-EN 50129:2010	EN / SN / Electro-Suisse
Dok.11: EN 50657 Railways Applications - Software on Board Rolling Stock	dd. August 2017 SN-EN 50657:2017	EN / SN / Electro-Suisse

Tabelle 6-1: Referenzierte Dokumente

(Ende des Dokumentes)