Grundkonzept APS (Innenanlage)

Firma:	**SBB**
Vertraulichkeit:	Intern
Zuletzt geändert:	27.11.2019 10:02
Zuletzt geändert durch:	SOMMERFELD MARCO (IT-SWE-CC1-JV2)
Dokumenten-Status:	Freigegeben
Version:	1.2
Dateiname:	bcon_aps.docx

Abstract

Das Advanced Protection System (APS) ist ein Ersatz für heutige Stellwerkinnenanlagen, basierend auf einem geometrischen Stellwerklogikansatz. Das vorliegende Konzept geht von bestehenden Technologien (wie ETCS L2 mit Gleisfreimeldeeinrichtungen) aus, wurde jedoch soweit offen konzipiert, dass eine Integration von neuen Technologien (z.B. ETCS L3, genaue Lokalisierung) möglich ist und die damit verbundenen Verbesserungspotenziale jeweils ausgeschöpft werden können.

Die Bewertung der bisherigen Resultate zeigt, dass ein neues Stellwerk wie APS grundsätzlich machbar ist. Das APS ermöglicht dabei einen Umbau der Prozesse und Systeme der Bahnproduktion hin zu hoher Automatisierung, Kapazität, Anlagenvereinfachung und Sicherheit.

1. Änderungsnachweise

Version	Datum	Autor	Änderungshinweise
1.0	04.07.2019	Martin Kaufmann Lucien Weller	Initialversion
1.1	10.10.2019	Marco Sommerfeld	Kommentare aus Review verarbeitet
1.2	08.11.2019	Marco Sommerfeld / Martin Kaufmann	Kommentare aus formalen STASS Review eingearbeitet.

2. Verarbeitete Reviews

Reviewer	Datum	Link Review-Bericht / Verifikationsbericht	Verarbeitung abgeschlossen am/vom
Samuel Urfer	04.07.2019	Reviewkommentare wurden als 'Kommentar' im Dokument erfasst und nach erfolgreicher Abarbeitung entfernt	04.07.2019
Steffen Schmidt	6.10.2019	Reviewkommentare wurden als 'Kommentar' im Dokument erfasst **Kommentare bitte beantworten, nicht löschen**	
Formales Review STASS	06.11.2019	Grundkonzept APS.xlsx	08.11.2019

Achtung: Reviewbemerkungen werden grundsätzlich über Kommentare angebracht. Der Reviewverarbeiter beschreibt im Kommentar (Kommentar ergänzen), wie er mit dem Kommentar umgegangen ist. Kommentare werden nie gelöscht.

3. Freigegeben durch Autor, (Verifizierer), Projektleiter

Version	Datum	Freigebender	Unterschrift / Gez.
1.0	25.07.2019	Samuel Urfer	
1.1	10.10.2019	Marco Sommerfeld	
1.2	11.11.2019	Marco Sommerfeld	

Inhalt

1. Änderungsnachweise 2
2. Verarbeitete Reviews 2
3. Freigegeben durch Autor, (Verifizierer), Projektleiter 2
1 Zusammenfassung 4
2 Ausgangslage und Aufgabenstellung 4
3 Ziele und Akzeptanzkriterien 4
4 Konzept 5
4.1 Kernkonzepte 5
4.1.1 Gleisnetz-Topologie 6
4.1.2 Betriebsabbild 6
4.1.3 Occupancies und Movable Objects 7
4.1.4 Movement Permissions 7
4.1.5 Risk Buffer & Risk Path 7
4.1.6 Danger Areas 8
4.1.7 Drive Protection Sections 8
4.1.8 Allocation Sections 8
4.1.9 Safety Actors 8
4.2 Übersicht Funktionale Architektur 8
4.2.1 Schnittstellen 9
4.2.2 Funktionsblöcke 9
5 Bewertung des Konzeptes (mit Alternativen) 10
5.1 Bewertung der Zielerreichung 10
5.2 Bewertung der Machbarkeit 11
5.3 Bewertung der Wirtschaftlichkeit 12
5.4 Offene Punkte 12
6. Verzeichnisse 14
6.1. Glossar / Glossar-Referenz 14
6.2. Grafik-Verzeichnis 14
6.3. Tabellenverzeichnis 14
6.4. Quellen / Referenzen 14

1 Zusammenfassung

APS steht für *«Advanced Protection System»* und ist eine Stellwerksoftware, die auf einer geometrischen, generisch einsetzbaren Sicherheitslogik basiert.
Das Grundprinzip dieser Sicherheitslogik besteht darin, das sämtliche Bewegungen auf dem Gleisnetz ausschliesslich innerhalb einer sogenannten Movement Permission erfolgen dürfen. Movement Permissions können, anders als heutige Fahrstrassen, eine beliebige Ausdehnung auf dem Gleisnetz haben.

Da mit der neuen Stellwerksgeneration eine strikte Trennung zwischen betrieblicher und sicherheitsrelevanter Funktionalität angestrebt wird, wird APS lediglich SIL4 Funktionalität beinhalten. Betriebliche Funktionalität wird auf die übergeordnete Systemebene (TMS) verlagert.

Die wesentliche Aufgabe von APS ist es daher lediglich atomare Anfragen auf Sicherheit (OK / NOK) zu prüfen und diese gegebenenfalls an die Aussenwelt weiter zu leiten.

Anfragen zur Infrastrukturbeeinflussung (Weichen, Bahnübergänge, …) werden von TMS initiiert und von APS lediglich auf Sicherheit geprüft. Auch die gewünschte Ausdehnung/Ausprägung einer Movement Permission für ein Movable Object (Fahrzeuge/Fahrzeuggruppen) und die Anfrage an APS zur Genehmigung dieser, wird von TMS getrieben.

Unter anderem durch die Vereinigung klassischer Stellwerks- und RBC-Funktionen innerhalb des APS, kann APS ETCS L2 und ETCS Level 3 («full moving block») unterstützen. Aber auch ein gemischter Einsatz von ETCS Level 2 und 3 ist möglich und für die mind. 20-jährige Migrationsphase (2020 bis 2040) auch zwingend nötig.
Die Zukunftssicherheit ist durch eine von Ortungstechnologien unabhängige Sicherheitslogik gegeben. So erlaubt APS zukünftig den Anschluss von zuggestützten und mobilen Lokalisierungstechniken (siehe auch [7]).

Im Verlaufe dieses Dokuments wird auf die hier stark komprimiert beschriebenen Grundprinzipien eingegangen (siehe Kapitel 4 Konzept). Zuvor werden im Kapitel 3 die Ziele und Akzeptanzkriterien von APS erläutert. Die Ausgangslage und Aufgabenstellung werden im Kapitel 2 beschrieben.

2 Ausgangslage und Aufgabenstellung

Die Ausgangslage und Aufgabenstellung sind ausführlich im Abschnitt Management Summary in [4] ETCS Strategie V1.0 beschrieben. Dennoch seien an dieser Stelle die wesentlichen Punkte erwähnt.

Ausgangslage:

- Integration von ETCS L2 mit konventioneller Stellwerklogik ist aufwändig zu realisieren und wenig flexibel. Auch die die erwarteten Ziele bzgl. Kosten- und Kapazitätsoptimierung, die mit der ETCS Führerstandsignalisierung möglich sind, können mit konventioneller Stellwerkslogik nicht erreicht werden.
- Das BAV beauftragte die SBB, im Rahmen von smartrail4.0 (SR40) eine ETCS Strategie zu entwickeln mit der künftig ein landesweites ETCS L2/L3 gesichertes Bahnnetz wirtschaftlicher eingeführt und betrieben werden kann.

Aufgabenstellung:

- Vollständiger Ersatz der bestehenden Stellwerkfunktionalitäten mit einem System, dass sich ausschliesslich auf die Sicherheitslogik beschränkt und sowohl ETCS L2 als auch L3 kompatibel ist. Betriebliche Funktionalität ist dabei an das TMS auszulagern.
- Striktere Trennung von Hard- und Software, zwecks Entkoppelung der unterschiedlichen Lifecycles
- Einhaltung von gesetzlichen Rahmenbedingungen und Standardisierungsgremien. Insbesondere die RCA-Architektur gilt es dabei zu berücksichtigen

3 Ziele und Akzeptanzkriterien

Auch die Ziele und Akzeptanzkriterien können im Detail dem Kapitel Management Summary aus [4] ETCS Strategie V1.0 entnommen werden. Folgend lediglich ein Auszug der wichtigsten Punkte.

Auszug Ziele ES Programm

- Schnelle und günstige netzweite industrialisierte Einführung der ETCS Führerstandsignalisierung, einsetzbar auch für ETCS L3 und mit neuen Lokalisierungstechnologien
- Starke Vereinfachung und Modernisierung der Stellwerkinnenanlagen, Aufbau von zentralisierten und redundanten Stellwerkrechenzentren und Trennung der Lebenszyklen von Innen- und Aussenanlagen, starke Vereinfachung der Stellwerkprojektierung.
- Konzeption einer standardisierten Sicherheitslogik, die ohne länder- oder betreiberspezifische Besonderheiten funktioniert.

Auszug Akzeptanzkriterien ES Programm

- Projektierungsaufwände sind geringer als bei konventionellen Stellwerken und den Anteil der spezifischen Zulassung kann auf einem Minimum reduziert werden.
- Erhöhung der Kapazität ohne Einbussen bei der Sicherheit mit bestehenden Gleisnetz
- Funktionierendes Stellwerk zur praktischen Anwendung auf den Erprobungsstecken (2025) zwecks Erhalt einer Typenzulassung ab 2026 und anschliessendem Rollout in der Fläche
- Bei der Überprüfung der Praxistauglichkeit des APS sollen Pilotprojekte sowohl mit Fokus auf Level 3 - Fahrzeuge, wie auch mit Fokus auf Level 2 – Fahrzeuge, sowie mit gemischtem Betrieb L2/L3, erfolgreich erprobt werden können.

Das Projekt APS ist Bestandteil des ES Programms und unterstützt die Zielerreichung des ES-Programms wie folgt:

Das zentralisierte geometrische Stellwerk, welches mit beliebiger Gleisnetztopologie funktioniert, sorgt für Kurze Zugfolgezeiten, erhöht die Gleisnetzkapazität und vereinfacht deutlich die Stellwerkslogik.
Die ETCS Kompatibilität ermöglicht einen wirtschaftlichen schweizweiten ETCS L2/L3 Rollout.
Die Vollständige Trennung der Lebenszyklen von Innen- und Aussenanlagen ermöglichen eine einfache Produktherstellung/-zulassung und Betrieb des Gesamtsystems.
Die Auslagerung betrieblicher Funktionen an TMS, womit APS ausschliesslich sicherheitsrelevante Funktionen beinhaltet, ermöglicht eine flexible Anpassung von Betriebsprozessen und reduziert die kostspielige SIL 4 Implementierung auf ein Minimum. Zusätzlich sei noch die Rangier-Führerstandsignalisierung erwähnt, die die Sicherheit insbesondere bei Rangiermanövern erhöht.

4 Konzept

4.1 Kernkonzepte

Das Advanced Protection System (APS) ist Teil des Gesamtsystems smartrail 4.0 und prüft Steuerungs- und Lenkungsanfragen vom übergeordneten Traffic Management System (TMS) ob diese Anfragen sicher (safe) ausführbar sind. TMS plant und steuert jegliche Bewegung auf dem Gleisnetz in Echtzeit (near realtime).

TMS-Lenkung ist Teil des TMS-Systems und steuert das APS. APS besitzt keine eigene Geschäftslogik zur Fahrwegsteuerung, sondern ausschliesslich zur Fahrwegsicherung. APS und TMS-Lenkung zusammen ersetzen die heute existierenden Stellwerks-Innenanlagen sowie die heute existierende Zuglenkung.

Die folgende Abbildung zeigt eine schematische Darstellung des smartrail 4.0 System. TMS sendet Steuerungsanfragen (Bsp. Änderung Weichenlage) sowie Lenkungsanfragen (Bsp. gewünschte Bewegung von A nach B) an APS. Jede Anfrage wird von APS auf Zulässigkeit geprüft. Stellt eine Anfrage kein Sicherheitsrisiko dar, wird diese Anfrage als Auftrag an den oder die entsprechenden Controller zur Ausführung weitergeleitet. Ein Controller übersetzt einen Auftrag in Form von zum Beispiel elektrischen Signalen an ein Element der Aussenanlage und nimmt anfallende Rückmeldungen in Form von Zuständen entgegen. Informationen über Zustände von Aussenanlagenelementen werden an APS weitergegeben. APS empfängt und speichert Zustandsinformationen im sogenannten ‘Betriebsabbild’ welches von Umsystemen wie zum Beispiel TMS konsumiert wird. Im Betriebsabbild findet sich die aktuell gültige Gleisnetztopologie, darauf abgebildet werden Zustandsinformationen von Elementen, an Züge ausgegebene Bewegungserlaubnisse sowie sogenannte Gefahrenbereiche (z.B. Sperren, Langsamfahrstellen).

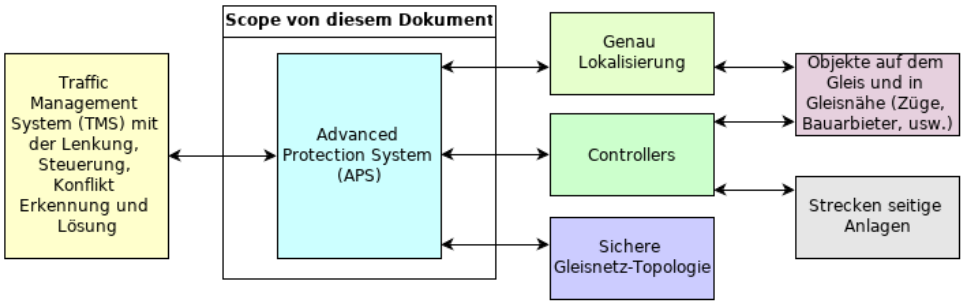

Abbildung 1: Übersicht der smartrail 4.0 Gesamtsystems

APS ist ausschliesslich für die Sicherung von Bewegungen auf und allenfalls entlang der Gleisanlage zuständig. APS besitzt keinerlei Funktionalität zur Feststellung von betrieblichen Auswirkungen, wie zum Beispiel das Verhindern einer Überfüllung. APS prüft Anfragen ausschliesslich auf deren Sicherheit (safety). Diese absichtliche Designentscheidung erzwingt eine scharfe Abgrenzung zwischen sicherheitsrelevanten und nicht-sicherheitsrelevanten Aufgaben. Ebenfalls bei der manuellen Bedienung, die es auch zukünftig geben wird, wird strickt zwischen sicherheitsrelevanter und nicht-sicherheitsrelevanter Bedienung unterschieden. APS stellt hierfür eine „APS-App“ zur Verfügung, über die ausschliesslich sicherheitsrelevante Bedienungen möglich sein werden, beispielsweise das Aufheben von Danger Areas oder die Bedienung von „Degraded Modes“
Durch diese Abgrenzung soll die Komplexität von APS als hochgradig sicherheitsrelevantes System reduziert werden und somit zu geringeren Entwicklungs- und Wartungskosten führen. Dies erlaubt, nicht sicherheitskritische Funktionalitäten wie beispielsweise betriebsrelevante Funktionen in einem System oder Systemverbund zu realisieren, welcher im Bereich no-SIL oder SIL-0 abgesiedelt ist.

4.1.1 Gleisnetz-Topologie & Projektierung

Die Gleisnetz-Topologie ist eine essentielle Grundlage für APS um Sicherungsaufgaben überhaupt wahrnehmen zu können. Auf diese Gleisnetz-Topologie bildet APS beispielsweise empfangene Gleisnetz-Belegungsinformationen ab oder prüft die Fahrwegfreiheit vor Erteilung einer Bewegungserlaubnis.
Die Gleisnetz-Topologie wird in APS in Form eines Knoten-Kanten-Modells vorgehalten und vom Systemverbund EDP, TOPO4 zur Verfügung gestellt.

Gleisnetz-Topologiedaten sind Bestandteil der sogenannten ‘Engineering Data’. Engineering Data sind das Resultat des Projektierungsprozesses (unterstützt durch die Systeme EDP/TOPO4) und beschreibt statische Daten der spezifischen Applikation und umfasst:

- Gleisnetz-Topologiedaten (Eng.: ‘Railway Network Topology’) wie beispielweise Bahnübergänge, Weichen, Geschwindigkeitsschwellen und Balisen welche auf diesen Kanten positioniert sind.
- Konfigurationsdaten (Eng.: ‘Configuration Data’) für die spezifische Anwendung wie beispielweise Port Konfiguration eines OC’s oder der Umlaufzeit einer Weiche.

Die Projektierung eines APS Systems besteht im Kern aus der gesicherten Erfassung der Gleisnetz-Topologiedaten. Falls eine für APS zugelassene Aussenanlage verändert, entfernet oder ergänzt wird, werden im Wesentlichen folgende Schritte für eine Inbetriebnahme nötig:

- Es findet eine SioP B statt (technische Anlagenprüfung)
- Engineering Data werden sicher erfasst und an APS übermittelt

APS berücksichtigt von nun an die veränderte Aussenanlage.

4.1.2 Betriebsabbild

APS stellt ein sogenanntes ‘Betriebsabbild’ (eng.: Operating State) zur Verfügung. Das Betriebsabbild ist eine sichere Repräsentation der aktuell gültigen, produktiv genutzten Gleisnetztopologie innerhalb eines geografischen APS-Segments. Auf dieser bildet APS ab und führt kontinuierlich nach:

- Zustandsinformationen von allen festen und beweglichen Aussenanlagenelementen. Zustandsinformationen sind heute bekannt unter Begriffen wie beispielweise Weichenlage, Belegung. Zu Zustandsinformationen zählen auch Störungen.
- Der von APS als sicher (safe) freigegebene Bewegungserlaubnisse und deren Übermittlungszustand
- Allfällige Einschränkungen wie beispielsweise Sperren und Langsamfahrstellen

In den nachfolgenden Kapiteln werden diese Aspekte detaillierter beschrieben.

4.1.3 Occupancies und Movable Objects

Wird ein Topologie-Abschnitt als belegt gemeldet und diese Belegung kann nicht eindeutig einem Fahrzeug oder Fahrzeuggruppe zugeordnet werden, wird diese Zustandsinformation als sogenannte 'Occupancy' im Betriebsabbild von APS festgehalten, was die Nutzungsbedingen für andere Anfragen, die diesen Topologie-Abschnitt betreffen, einschränkt. Kann die Belegung eindeutig einer Bewegung zugeordnet werden wird anstelle des Belegungsobjekts (Occupancy) ein 'Movable Object' mit allen bekannten Eigenschaften (z.B. die aktuelle Geschwindigkeit) im Betriebsabbild von APS geführt.

4.1.4 Movement Permissions

Die Sicherung von Bewegungen erfolgt in APS mittels lückenloser, fahrbarer Abschnitte auf der Gleisnetz-Topologie. Im Gegensatz zu blockbasierten Stellwerken kann ein solcher Abschnitt mit APS, unter Berücksichtigung der Fahrbarkeit, an einem beliebigen Ort beginnen und an einem beliebigen anderen Ort auf der Gleisnetz-Topologie enden ("geometrische Sicherungslogik").

Ein solcher, von APS gesicherter Abschnitt zur Durchführung einer Bewegung, wird 'Movement Permission' genannt. Eine Movement Permission enthält immer ein Set an Nutzungsbedingungen (eng.: Utilisation Conditions) wie zum Beispiel zulässige Richtung, zulässige Höchstgeschwindigkeit, zulässige Betriebsart.

Eine Movement Permission umfasst innerhalb ihrer geometrischen Ausdehnung immer mindestens die geometrische Ausdehnung des Movable Objects für welche diese Movement Permission gilt. Eine Movement Permission gilt immer für genau ein Movable Object. Auch im Stillstand wird die geometrische Ausdehnung eines Movable Objects geometrisch von einer Movement Permission umschlossen. Zum Beispiel ist eine Nutzungsbedingung einer Movement Permission für ein abgestelltes Movable Object 'Höchstgeschwindigkeit 0 km/h'.

Eine Movement Permission bildet zudem die Grundlage für die Visualisierung der Signalisierung auf einem Fahrzeug oder/und an der Strecke. In Abhängigkeit der vorhandenen Signalisierungssysteme auf dem Fahrzeug und der Strecke wird eine Movement Permission von APS an ein Movable Object und/oder an einen oder mehrere Object Controller übermittelt. Beispiel: Eine Movement Permission muss in Form von fahrtzeigenden Rangiersignalen visualisiert werden da beim betroffenen Movable Object keine technische Ausrüstung zur Führerstandsignalisierung vorhanden ist.

4.1.5 Risk Buffer & Risk Path

Solange kein Movable Object seine Movement Permission (MP) verlässt, kann keine Kollision erfolgen, da APS sicherstellt, dass sich MPs niemals geometrisch überlappen. Das ein Movable Object seine MP nicht verlässt, wird beispielswese von einer ETCS On Board Unit mit sichergestellt. Damit es jedoch im sehr unwahrscheinlichen Fall des Verlassens der MP dennoch zu keiner Kollision kommt, wird zusätzlich zur MP ein RiskBuffer allokiert. Der RiskBuffer stellt sicher, dass in Abhängigkeit von der Geschwindigkeit, Topographie, Gefahrengut,… Movable Objects stets einen gewissen Abstand zueinander einhalten.
Je höher die Geschwindigkeit, je gefährlicher das Gefahrengut,…. desto grösser fällt der Riskbuffer aus.

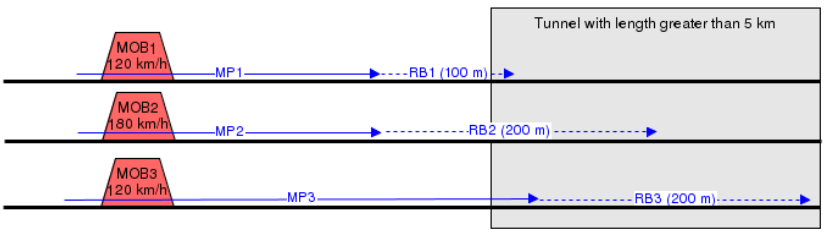

Abbildung 2: Schematische Darstellung RiskBuffer

Der Teil der Topologie, welcher zum Schutz vor dem Eindringen einer fremden Bewegung in eine Movement Permission reserviert werden muss (Flankenschutz), wird als ‘Risk Path’ bezeichnet. APS prüft bei jeder Anfrage einer neuen oder zu verlängernden Movement Permission immer auch, ob die mitangefragten Risk Buffer und Risk Path zulässig und genügend sind.
Da APS zur Laufzeit den notwendigen Risk Path bestimmen kann, ist es anders als heute nicht mehr notwendig die schutzgebenden Weichen zu projektieren. Hinzu kommt, dass die Ausprägung/ Ausdehnung des RiskPath abhängig ist von der Geschwindigkeit (weitere Kriterien denkbar). Theoretisch ist also bei einer Geschwindigkeit unter einem Schwellwert x kein Risk Path notwendig.

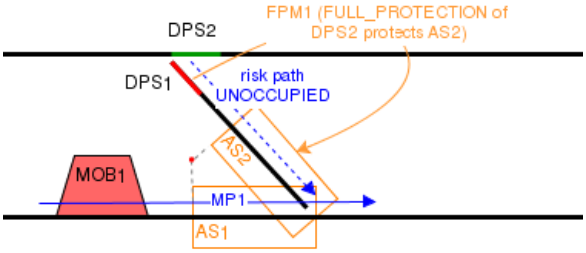

Abbildung 3: Schematische RiskPath Darstellung

4.1.6 Danger Areas

Im Gegensatz zu einer Movement Permission muss eine Danger Area nicht notwendigerweise aus einer lückenlosen Abfolge von Gleisabschnitten bestehen. Beispielsweise kann eine Danger Area Gleisabschnitte von zwei geografisch parallel nebeneinander liegenden Gleisen enthalten.
Die Nutzungsbedingen können auch an andere Anspruchserheber (z.B. zu Wartungszwecken) vergeben werden. Diese temporäre Abgabe von Nutzungsbedingungen an Prozesse ausserhalb des Einflussbereichs von APS wird mittels des Konzepts der Danger Areas abgedeckt, welche ebenfalls im Betriebsabbild von APS festgehalten werden. Eine Danger Area kann entweder von der TMS-Lenkung angefragt werden (z.B. um Wartungsarbeiten durch zu führen) oder eigenständig von APS erstellt werden als Reaktion bei einer Verletzung der APS Sicherheitsregeln (Beispiel Weiche verliert Lageinformation).

4.1.7 Drive Protection Sections

Abschnitte auf der Gleisnetz-Topologie, welche aktiv gesteuert werden müssen, um eine bestimmte Nutzung der Topologie zu ermöglichen (z.B. Weiche, die gestellt oder Bahnübergänge, die geschlossen werden müssen) werden als ‘Drive Protection Sections’ (DPS) abstrahiert. Der ‘Drive Protection Level’ (DPL) einer DPS entspricht dabei der konkreten Nutzungsmöglichkeit im aktuellen Zustand.

4.1.8 Allocation Sections

Abschnitte auf der Gleisnetz-Topologie, welche geometrisch in Konflikt stehen (Bsp. 3-Schienen Gleis) und deshalb exklusiv nur von einem Movable Object zur gleichen Zeit belegt werden können, werden als Allocation Section bezeichnet. Sobald eine Allocation Section belegt ist, schränken sich die Nutzungsmöglichkeiten der anderen in Abhängigkeit stehenden ein.

4.1.9 Safety Actors

Werden sicherheitsrelevante Zustände auf Grund von gewissen Rahmenbedingungen zugelassen (z.B. eine Movement Permission mit einer gewissen Höchstgeschwindigkeit), dann muss auch immer definiert werden, wer (kann ein System oder ein Mensch sein) dafür verantwortlich ist, dass diese eingehalten werden.

4.2 Übersicht Funktionale Architektur

Das Advanced Protection System (APS) wird in unterschiedliche Funktionsblöcke zerlegt. Die folgende Übersicht zeigt die wesentlichen davon sowie die zugehörigen Datenflüsse und Interaktionen.

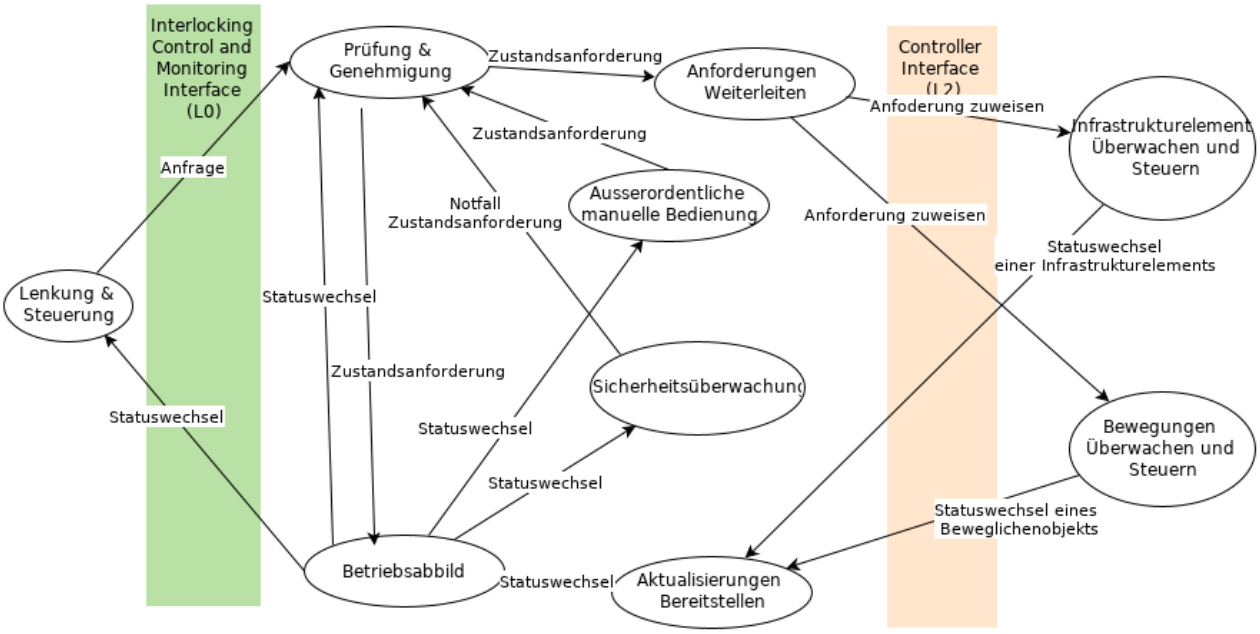

Abbildung 4: Grobe Datenflüsse rund um APS

4.2.1 Schnittstellen

Schnittstelle	Zweck
Interlocking Control and Monitoring Interface (L0)	Das Interlocking Control and Monitoring Interface bildet die Trennung zwischen den sicherheitsrelevanten und nicht sicherheitsrelevanten Systemen. Alle Anfragen werden immer erst geprüft bevor sie zur Ausführung weitergegeben werden.
Controller Interface (L2)	Das Controller Interface bildet die Verbindung zur Aussenwelt. Darüber werden Anfragen zu Ausführung übermittelt, sowie Aktualisierungen von Zuständen entgegengenommen. Die Aussenwelt kann allgemein in zwei Kategorien von Objekten unterteilt werden: nicht bewegte Objekte (Streckenseitige Anlagen) und bewegte Objekte (Fahrzeuge, Arbeiter in Gleisnähe, usw.).
Device and Configuration Management Interface	Über das Device and Configuration Management Interface bekommt das APS alle statischen Informationen, welche zur korrekten Funktionsweise notwendig sind. Dies sind insbesondere Gleisnetz-Topologiedaten und Konfigurationsdaten.

Tabelle 1: Übersicht Der Schnittstellen und deren Zwecke

4.2.2 Funktionsblöcke

Nachfolgend ist der Zweck der einzelnen funktionalen Komponenten beschrieben. Die letzte Spalte ordnet die funktionalen Komponenten den entsprechenden RCA Komponenten zu. RCA steht für «Reference CCS Architecture» Inhalt, Sinn und Zweck sind in [5] SR40 Konzeptbericht 2019 beschrieben.

Funktionsblock	Zweck	RCA Komponente
Lenkung & Steuerung	Die Lenkung & Steuerung setzt die geplanten Zug- und Rangierbewegungen um. Um eine reibungslose Produktion zu gewährleisten, werden rechtzeitig alle Anfragen für Infrastrukturelementzustände und Bewegungserlaubnisse an APS gestellt.	TMS Plan Execution

Prüfung & Genehmigung	Die Prüfung & Genehmigung überprüft alle Anfragen auf Machbarkeit und Sicherheit (Safety). Sobald eine Bedingung nicht erfüllt ist, wird die Anfrage abgelegt.	APS Safety Logic
Anforderungen Weiterleiten	Anfragen, welche angenommen werden, werden entsprechend aufbereitet und den betroffenen Kontrollern zur Ausführung weitergeleitet.	APS Object Aggregation
Aktualisierungen Bereitstellen	Die Rückmeldungen von allen Kontrollern werden aufbereitet und zu einem gesamten Betriebsabbild konsolidiert, so dass ein möglichst vollständiges und präzises Abbild der Aussenwelt zur Verfügung gestellt werden kann.	
Infrastrukturelemente Überwachen und Steuern	Die Überwachung und Steuerung von Infrastrukturelementen führt bei den streckenseitigen Anlagen die nötigen Umstellungen aus, so dass der Zustand, der in dem Anfangen gefordert wurde, effektiv eintritt. Die Veränderung des Zustandes wird dann wieder zurückgemeldet.	
Bewegungen Überwachen und Steuern	Die Überwachung und Steuerung von Bewegungen übermittelt den Fahrzeigen die Bewegungserlaubnis gemäss den Anfragen. Im Gegenzug werden die Informationen über den Status und Position zurückgemeldet.	
Betriebsabbild	Das Betriebsabbild hält die Zustände aller Objekte im System vor. Es bildet die massgebende Quelle der Wahrheit für alle beteiligten Systeme.	
Sicherheitsüberwachung (Safety)	Die Sicherheitsüberwachung überwacht permanent das Betriebsabbild auf Gefährdungen. Sobald ein sicherheitskritischer Zustand erkannt wird eine Nothandlung automatisch ausgelöst, um die Gefährdung abzuwenden oder zumindest deren Auswirkung zu minimieren.	APS Safety Manager
Ausserordentliche manuelle Bedienung	Dieser Funktionsblock deckt alle ausserordentlichen manuellen Handlungen, welche direkt im APS ausgeführt werden müssen (z.B. wenn bei gewissen Initialisierungsprozessen oder in Störfällen). Er beinhaltet einerseits eine Visualisierung des Betriebsabbildes und andererseits die Bedienmöglichkeiten für menschliche Aktoren. Im Gesamtsystem kann es auch noch weitere Benutzerinterfaces geben, welche jedoch ausschliesslich normal Anfragen absetzen können, welche wie üblich auf Sicherheit geprüft werde und nicht direkt durchgreifen können.	APS App

Tabelle 2: Übersicht der Funktionsblöcke und deren Zweck

5 Bewertung des Konzeptes (mit Alternativen)

5.1 Bewertung der Zielerreichung

Ziel	Bewertung Beitrag APS
Schnelle und günstige netzweite industrialisierte Einführung der ETCS Führerstandsignalisierung (Auftrag des Eigners, Erhöhung der Sicherheit), aufwärtskompatibel zu ETCS L3 und zu neuen Lokalisierungstechnologien	• Fähigkeit Gleisnetz-Topologiedaten im laufenden Betrieb zu übernehmen • Geometrische Sicherheitslogik erlaubt Umgang sowohl mit klassischen Blocklängen sowie Moving Block • Unterstützung neuer Lokalisierungstechniken zur Sicheren

	Abbildung von Gleisbelegungen auch ohne Gleisfreimeldemittel • Funktionalität Warnen von MAIN im Gleis als integraler Bestandteil des Stellwerks
Starke Vereinfachung und Modernisierung der Stellwerkinnenanlagen, Aufbau von zentralisierten und redundanten Stellwerkrechenzentren und Trennung der Lebenszyklen von Innen- und Aussenanlagen, starke Vereinfachung der Stellwerkprojektierung (Kostensenkungspotential bis zu CHF 50 Mio p.a., 20% weniger SA-Störungen)	• Fokus ausschliesslich auf safety-relevante Funktionen und somit Reduktion der Komplexität • Standardisierung von Schnittstellen unterstützt standardisierten Rollout • Stellwerk- und RBC-Projektierung sind nicht mehr getrennte Welten. • Train Position Reports (TPR) der Zugspitze bereits nutzbar zur genaueren Lokalisierung in Verbindung mit Gleisfreimeldeabschnitten • Modelltechnische Abstraktion auf wenige generische Objekte zur Repräsentation des Gleisnetzes inklusive der verbleibenden Aussenanlagen • Anwendung von bewährten IT-Architekturprinzipien im Bereich der Höchstverfügbarkeit
Schaffung der Grundlagen für die starke Reduktion der Stellwerk-Aussenanlagen durch verbesserte Zuglokalisierung und Rangier-Führerstandsignalisierung (Kostensenkungspotential bis zu CHF 220 Mio p.a., 30% weniger SA-Störungen)	• Geometrische Sicherheitslogik in Verbindung mit erweiterter Führerstandsignalisierungsfunktionalität (nicht beschränkt auf reine ETCS-OBU's) für jede Art von zu sichernder Bewegung auf dem Gleis, also auch Rangiermanöver und Rangierfahrten • Unterstützung neuer Lokalisierungstechniken zur sicheren Abbildung von Gleisbelegungen auch ohne Gleisfreimeldemittel
Migrationsfähigkeit von Beginn an über die gesamte, min. 20-jährige Migrationsphase.	• Fähigkeit, in zunächst reinen L2-Bereichen frühestmöglich die heutige Technologie (RBC und heutiges eStw mit klassischen Fahrstrassen) zu ersetzen • Schaffung von Synergien und Einsparungen auch schon in reinen L2-Projekten bspw. durch eine automatische Projektierung • Unterstützung neuer Lokalisierungstechniken zur sicheren Abbildung von Gleisbelegungen auch ohne Gleisfreimeldemittel

Tabelle 3: Bewertung des Beitrags von APS zur Zielerreichung des ES-Programms

5.2 Bewertung der Machbarkeit

5.2.1 Zulassungsfähigkeit

Die Zulassungsfähigkeit wurde auf Basis von ‚Funktionales Konzept zum ETCS-Stellwerk im Gesamtsystem SmartRail 4.0' vom 31.August 2017 und ‚General Concept ETCS Interlocking' vom 01.November 2017 durch einen unabhängigen Gutachter Prof.Dr.-Ing. Nils Niessen von der RWTH Aachen begutachtet und liegt in Form eines ‚Gutachten zur grundsätzlichen Machbarkeit der Innenanlagen im Rahmen des ETCS-Stellwerks' [3] vom 30.März 2018 vor. Dieses sagt aus, dass „Insgesamt kann bestätigt werden, dass das Konzept ES-Innenanlagen grundsätzlich realisierbar ist und zulassungsfähig erscheint. [sic.]" Das Gutachten weist zudem eine Menge an Themen auf, welche „im weiteren Projektverkauf" zu bearbeiten sind:

- Ausfall der Lokalisierung
- Umgang mit Topologieänderungen

- Kuppeln von Wagen
- Gegenfahrschutz

Seit Veröffentlichung des Gutachtens wurden sämtliche Themen adressiert und zwar in Form von bereits ausgeführten oder geplanten

- Konzeptdetaillierung, Ergänzungen bestehender Konzepte, beispielweise für den Umgang mit Topologieänderungen, Gegenfahrschutz
- Software-Implementierungen (PoC), beispielweise für Vereinen, Trenne, Wenden, Bewegung von Zügen

5.2.2 Betriebstauglichkeit

Die Tauglichkeit eines produktiven Einsatzes wurde auf Basis der bis dato erarbeitete Spezifikationen und Konzepten geprüft. Dazu wurden sämtliche Funktionen der bestehenden Stellwerke sowie der Zuglenkung (ILTIS) als Basis genommen und identifiziert, welche Funktionalitäten zukünftig von APS und welche von TMS-PE erfüllt werden müssen und welche aufgrund von zum Beispiel Wegfall von Aussenanlagenelementen oder Änderungen von Prozessen wegfallen und welche angepasst werden müssen.
Des Weiteren wurde auf Basis von bestehenden sowie zukünftigen Betriebsprozessen ein Set an betrieblichen Szenarien definiert um festzustellen, dass diese mit dem zukünftigen APS vollständig unterstützt werden können*. Die Betriebstauglichkeit erster Betriebsprozesse konnte mit Hilfe des APS Prototypens nachgewiesen werden, Beispielsweise konnten die Prozesse Trennen, Wenden und Vereinen erfolgreich im Prototypen abgebildet werden. Auch erste ETCS-Prozesse (Start-/ End of Mission) konnten im Prototypen abgebildet werden. Das Ziel ist es bis Ende 2020 ca. 80% aller Betriebsprozess im APS Prototypen abzubilden.

*) Vorgang dauert an

5.2.3 Entwicklung durch die Industrie

An mehreren sogenannten Industrietagen wurden Konzepte, grobe Wirkprinzipien und Lösungsansätze von smartrail 4.0 gegenüber Industrievertretern aus verschiedenen Branchen (Bsp. Transportation, Automotive) vorgestellt. Die Industrie zeigt und äussert Interesse an einer Mitarbeit. Um festzustellen, ob das Interesse in belastbaren Angeboten mündet, wird in einem nächsten Schritt eine ‚Ausschreibung zur Präqualifikation' erarbeitet. Deren Publikation soll zwischen 12/2019 und 04/2020 stattfinden. Der Abgabetermin für die Antworten auf die Präqualifikation soll zwischen 04/2020 und 06/2020 stattfinden. Um Vorgehensdetails sowie die geplante Terminlage zu verifizieren ist Ende 2019 ein Hearing mit der Industrie vorgesehen.
Die geplante Zusammenarbeit mit der Industrie und der gültige Zeitplan, kann dem Kapitel „Beschaffung" in [5] SR40 Konzeptbericht 2019 entnommen werden.

5.3 Bewertung der Wirtschaftlichkeit

Die Bewertung der Wirtschaftlichkeit ist ausführlich in [6] Business Case SR40 beschrieben.

5.4 Offene Punkte

Die folgenden Punkte konnten während der Konzeptionsphase nicht ganz abschliessend geklärt werden. Es gibt jeweils erste Lösungsansätze, die jedoch noch zu verifizieren sind. Die Verifikation erfolgt mittels APS-Prototyp, welcher derzeit implementiert wird und/oder gemeinsam mit den Industriepartnern während der Alpha Phase

- Finalisierung der ausgetauschten Informationen zwischen den zukünftigen, neuen Lokalisierungstechnologie(n) und APS in Form einer abschliessenden Liste definierter Objekte und Attribute
- Detaillierung von Mechanismen zur konsistenten Verteilung und Aktivierung der Topologie und Konfigurationsdaten über die Systeme von smartrail 4.0
- Detaillierung von Mechanismen zur Authentifizierung und Aktivierung der Systembenutzer von smartrail 4.0
- Detailierung von Wirkprinzipien und Konzepten im Umfeld von
    - Rangier- und Sperrprozessen
    - Notbedienungen
    - Sicherung durch Warnanlagen
    - Wartung von Infrastrukturobjekten
    - Zentrale Gefahrenerkennung und -minderung

    - Sicherung der Bewegung von nicht spurgeführten beweglichen Objekten
    - Steuerung des Status von beweglichen Objekten
- Systemunterstützte Aufhebung von gesicherten Bereichen (Baustellen, Sperrungen, Langsamfahrstellen)
- Systemunterstützte Übergabe und Überwachung von sogenannten Safety-Verantwortungen (Bsp. Fahrt von Full Supervision nach On Sight)
- Betriebsunterstützung (Monitoring und Diagnose)

6. Verzeichnisse

6.1. Glossar / Glossar-Referenz

Siehe SR40 Glossar: https://trace.sbb.ch/polarion/#/project/library/workitems/definition

6.2. Grafik-Verzeichnis

Abbildung 1: Übersicht der smartrail 4.0 Gesamtsystems 6
Abbildung 2: Grobe Datenflüsse von und zu APS 9

6.3. Tabellenverzeichnis

Tabelle 1: Übersicht Der Schnittstellen und deren Zwecke 9
Tabelle 2: Übersicht der Funktionsblöcke und deren Zweck 10
Tabelle 3: Bewertung des Beitrags von APS zur Zielerreichung des ES-Programms 11

6.4. Quellen / Referenzen

Referenz	
[1]	Vorstudie ATC in Bapro35: https://sbb.sharepoint.com/:b:/r/teams/p-230/617/Oeffentlich/0002%20Vorstudie%20Bericht/Vorstudie%20ATC%20in%20Bapro35%20V24.pdf?csf=1&e=RHTizC
[2]	General Concept of the Advanced Protection System (APS): https://trace.sbb.ch/polarion/#/project/ES_IA/wiki/40_outputs/General%20Concept%20ETCS%20Interlocking
[3]	Gutachten_SBB_ES_Innenanlagen_20180330_final.pdf
[4]	ETCS Strategie V1.0 https://sbb.sharepoint.com/teams/p-230/617/Oeffentlich/0001%20Berichte%20und%20Reportings/Doks_Chapters%20Konzeptbericht%202019/APS/ETCS%20Strategie/ETCS%20Strategie%20V1.0.docx?web=1
[5]	SR40 Konzeptbericht 2019 \\Sbb.sharepoint.com@ssl\davwwwroot\teams\p-230\944\Oeffentlich\0060 Kommunikation und Stakeholder\0010 BAV\Konzeptbericht 2019
[6]	Business Case SR40 https://sbb.sharepoint.com/teams/p-230/951/_layouts/15/DocIdRedir.aspx?ID=P0230-1737198652-40883
[7]	General Concept for LLL https://sbb.sharepoint.com/teams/p-230/617/_layouts/15/DocIdRedir.aspx?ID=P0230-1526596073-48263