Entwicklung des Systemzusammenspiels nach SN EN 50126

Um die volle Kapazität der Gotthard-Basislinie (GBL) nutzen zu können, galt es, die Auflagen des Bundesamtes für Verkehr (BAV) zu erfüllen. Ein Teil dieser Auflagen betraf die Verbesserung der Gebrauchstauglichkeit im Hinblick auf das Zusammenspiel von Leit- und Sicherungssystemen. Die dafür notwendigen Verbesserungen waren Gegenstand des nach SN EN 50126 durchgeführten Projekts «Entwicklung RTI», bei welchem Mitarbeitende der AFRY Schweiz AG die Schweizerischen Bundesbahnen (SBB) unterstützen durften.

Ein ETR 610 verlässt den Gotthard-Basistunnel durch das Südportal. © SBB CFF FFS

Axel Bomhauer-Beins und David Grabowski

Am 1. Juni 2016 wurde der Öffentlichkeit mit der Eröffnung des ca. 57 km langen Gotthard-Basistunnels (GBT) nach einer Bauzeit von rund 17 Jahren der längste Eisenbahntunnel der Welt übergeben: Das Jahrhundertbauwerk ist Kernstück der «Flachbahn durch die Alpen», deren Scheitelpunkt nun auf nur rund 550 (statt zuvor auf ca. 1150) m ü. M. – und damit nur etwa 300 m höher als Basel bzw. Chiasso – liegt. Mit der Eröffnung des etwa 15 km langen Ceneri-Basistunnels (CBT) im September 2020, wodurch nochmals rund 130 Höhenmeter weniger zu überwinden sind, wurde die GBL komplettiert. In beiden Tunneln kommt das Zugsicherungssystem ETCS Level 2 (L2) mit Führerstandssignalisierung zur Anwendung; es sind Geschwindigkeiten von bis zu 230 km/h zulässig.

Insbesondere zwei Eigenschaften der GBL – die hohe Geschwindigkeit und die aussergewöhnliche Länge der Tunnel – bergen Risiken, die andernorts kaum relevant sind. Deshalb ist in beiden Tunneln ein zusätzliches System im Einsatz, welches diesen besonderen Umständen Rechnung trägt: Die Tunnelautomatik (TA). Gemeinsam mit den netzweit im Einsatz befindlichen Systemen «Integrales Leit- und Informationssystem» (Leitsystem Iltis) und «Rail Control System» (Dispositionssystem RCS) sowie weiteren spezifischen Umsystemen wie Tunnelleittechnik (TLT) und Einsatzleitsystem (ELS) unterstützt die TA die Betriebsmitarbeiter:innen der SBB dabei, einen reibungslosen Betrieb zu gewährleisten sowie Störungs- und Ereignisfälle effizient und zielgerichtet zu bewältigen.

Einige Mängel im Gesamtsystem, die bereits bei der Übergabe des GBT an die SBB bekannt waren, führten in der Betriebsbewilligung zu Einschränkungen und Auflagen. Einige der Mängel waren auf Unzulänglichkeiten im komplexen Zusammenspiel der Leit- und Sicherungssysteme zurückzuführen. Dieses zu verbessern und damit die Gebrauchstauglichkeit des Systemverbunds RTI – bestehend aus RCS, TA und Iltis – zu steigern, war Gegenstand des Teilprojekts «Entwicklung RTI», welches im Rahmen der «Abschlussarbeiten SA GBT» durchgeführt wurde.

Die EN 50126 im Projekt «Entwicklung RTI»

Mit der TA, einem sicherheitsrelevanten (Software-) System innerhalb des Projektumfangs, unterlag das Projekt «Entwicklung RTI» – wie bereits der Bau der GBL – der SN EN 50126. Sowohl die für den Bau anwendbare Version von 1999 [1] als auch die überarbeitete Fassung von 2017 [2] sehen eine Entwicklung nach dem sogenannten V-Modell vor (vgl. Bild 1).

Referenzen

[1] Electrosuisse (Hrsg.): SN EN 50126:1999, Bahnanwendungen – Spezifikation und Nachweis der Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit, Sicherheit (RAMS).

[2] Electrosuisse (Hrsg.): SN EN 50126-1:2017, Bahnanwendungen – Spezifikation und Nachweis von Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (RAMS) – Teil 1: Generischer RAMS Prozess.

[A] Siemens Mobility: RTI ermöglicht Kapazitätserhöhung im Gotthard-Basistunnel. Newsroom-Artikel. Abgerufen von https://www.mobility.siemens.com/ch/de/unternehmen/newsroom/news-archiv/rti-ermoeglicht-kapazitaetserhoehung-im-gotthard-basistunnel.html im November 2022.

[B] SBB AG (Hrsg.): Bericht zur Gebrauchstauglichkeit Tunnelautomatik GBT. 29.11.2021.

Für das Projekt «Entwicklung RTI» sind die Phasen 1 bis 10 [2] – Konzept bis Systemabnahme – von Interesse, wobei die Phasen 6 (Entwicklung) und 7 (Fertigung) durch Lieferanten umgesetzt werden. Grundlage für die Lieferantenaufträge bilden die Systemdefinition (Phase 2), die Anforderungsspezifikation (Phase 4) und die Zuteilung der Anforderungen zu den Teilsystemen (Phase 5). Das Zusammenspiel der beauftragten Entwicklungen wird in der Systemvalidierung (Phase 9) geprüft, die wiederum eine Voraussetzung für die Inbetriebnahme ist. Zu beachten ist, dass einige Lieferanten agile Methoden zur Entwicklung einsetzen, die nur bedingt zu den Vorgaben der Phase 6 passen.

Da es sich beim «Gesamtsystem» – selbst wenn dieses auf die drei Systeme RCS, TA und Iltis beschränkt wird – um ein äusserst umfangreiches und komplexes Gefüge handelt, musste das zu ändernde System durch Abgrenzungen eingeschränkt werden. Folgende Vorgehensweisen ermöglichten eine Reduktion der Komplexität auf ein handhabbares Mass:

– Die Dokumentation der Phasen 1 bis 5 nach EN 50126 umfasst nur Änderungen, die am «System RTI» vorgenommen werden sollen. Unverändertes Bestehendes wird nur aufgenommen, wenn dies für die Verständlichkeit notwendig ist.
– Die Systemfunktionen werden so festgelegt, dass möglichst wenige Funktionen anzupassen sind. Hierfür wird in Kauf genommen, dass einzelne Teilsysteme, bspw. Iltis, zur Betrachtung in mehrere Systemfunktionen aufgeteilt werden.

Ausserdem wurde bereits in der Konzeptphase entschieden, die Änderungen in drei Schritte (Bauphasen) aufzuteilen. Jeder Schritt führt zu einem Release, das validiert und in Betrieb genommen wird. Gleichzeitig wurde angestrebt, die grundlegende Dokumentation der Phasen 1 bis 5 nur einmal und für den Zielzustand – den Zustand nach dem letzten Release – zu erstellen. Die Einführung einer zusätzlichen «Zuteilung» in Phase 5 ermöglichte dies: Hier wurden die Anforderungen aus Phase 4 nicht nur einem Teilsystem, sondern zusätzlich auch einem Release zugewiesen. Wo in Einzelfällen in demselben Kontext unterschiedliche Verhaltensweisen für die verschiedenen Releases notwendig waren, wurde die entsprechende Anforderung zweimal gestellt: Einmal «bis zu» dem Release, ein zweites Mal «ab» dem Release, mit welchem die definitive Verhaltensweise einzuführen war.

Gewonnene Erkenntnisse aus den Releases und insbesondere Rückmeldungen aus dem Feld führten allerdings zu Anpassungen des Zielstandes und damit zu Anpassungen der Dokumentation aus den Phasen 1 bis 5. Diese flossen in verschiedenen Iterationen in die zugehörigen Dokumente ein. Im Grossen und Ganzen gelang es, die Phasen 1 bis 5 a priori für alle Releases zu durchlaufen – die in den fünf Phasen erstellten Dokumente für alle Releases unverändert anzuwenden, erwies sich jedoch als zu ambitioniert.

Hohe Komplexität – nicht nur auf technischer Ebene

Wie bereits erwähnt, bestehen das «System RTI» und sein Kontext aus Teilen bereits bestehender Systeme mit unterschiedlichen Aufgaben und Sicherheitsanforderungen. Darüber hinaus ist dem Projektauftrag Rechnung zu tragen: Die «Gebrauchstauglichkeit» des Systems ist zu verbessern – mit anderen Worten: Das System soll sich für die Bediener:innen logisch, intuitiv und nachvollziehbar verhalten. Durch Anwendung der Methoden «Design for Use» und «MTO» (Mensch, Technik, Organisation) wurde sichergestellt, dass den Bediener:innen und der Gebrauchstauglichkeit ausreichend Rechnung getragen wird. Neben der hohen technischen Komplexität des Systems stellten die Anwendung dieser Methoden und die Verarbeitung deren Ergebnisse besondere Herausforderungen des Projekts dar.

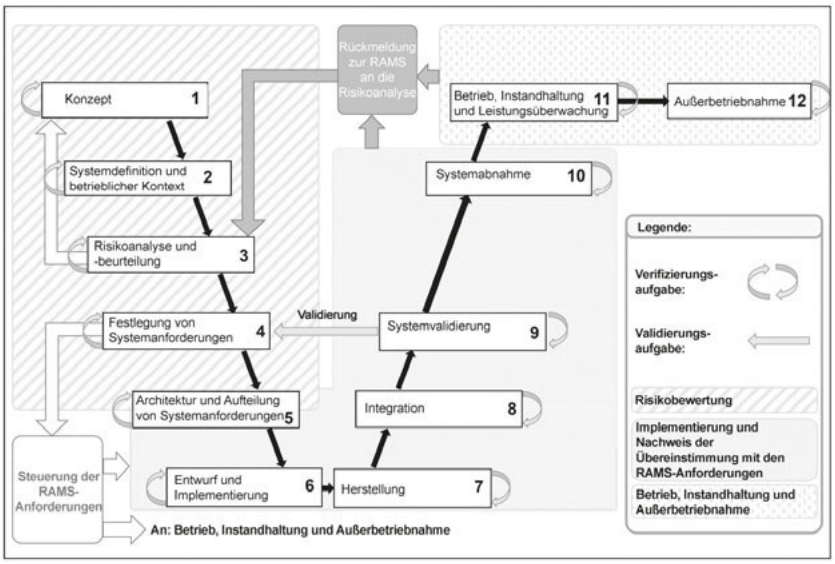

Bild 1: Das V-Modell nach SN EN 50126-1:2017. Quelle: [2], Bild 7, S. 45

Um die gewünschte Verbesserung der Gebrauchstauglichkeit zu erreichen, standen zwei Fragen im Zentrum: Wie wird das System in den unterschiedlichen Betriebssituationen genutzt? Welches Verhalten erwarten die Bediener:innen? Hierzu wurden für RTI eine soziotechnische Simulation unter der Leitung eines User-Experience-Fachexperten sowie Usability-Tests vorgenommen. Nachdem die Bediener:innen darauf hingewiesen worden waren, dass es keine «richtigen» oder «falschen» Verhaltensweisen gibt, wurde eine vierstündige Simulation der normalen Arbeitsabläufe durchgeführt. Zum Einsatz kamen dabei interaktive Prototypen für die zu untersuchenden Kernprozesse sowie Screenshots an den Anzeigen der Umsysteme, sodass eine möglichst realistische Arbeitsumgebung geschaffen wurde. Aus den Rückmeldungen der Bediener:innen auf die Fragen, (1) was gefallen hat, (2) was als Erstes geändert werden sollte und (3) was sonst noch zu erwähnen sei, wurden Massnahmen abgeleitet und ins Projekt aufgenommen. Diese konnten sowohl Anpassungen an Vorschriften und Arbeitsdokumenten als auch der Anzeigen und des Verhaltens des technischen Systems beinhalten. Basierend auf diesen Erkenntnissen wurden ein User-Experience-Konzept und eine «Interaction Map» erstellt, die festlegen, wie sich das System aus Sicht User Experience (UX) verhalten soll. Das UX-Konzept und die Interaction Map sind damit wichtige Dokumente, deren Inhalte aus Sicht SN EN 50126 bereits ab Phase 2 berücksichtigt werden müssen.

Die zentrale Aufgabe der Sicherheitsingenieure bestand in diesem Projekt folglich darin, einerseits die Erkenntnisse hinsichtlich Gebrauchstauglichkeit in die entsprechenden Phasen des RAMS-Prozesses einfliessen zu lassen und andererseits eine Brücke zwischen verschiedenen Ansätzen der Softwareentwicklung – agil und sicherheitsorientiert – zu bilden. Gleichzeitig war die Dokumentation der bereits bestehenden sicherheitsrelevanten Systeme zu beachten, um sicherzustellen, dass mit dem System RTI nicht gegen bestehende Sicherheitsvorgaben oder Anwendungsbedingungen verstossen wird.
Deshalb wurden die Phasen 1 bis 5 in enger Abstimmung mit den Entwicklungsteams der Teilsysteme TA, RCS und Iltis durchlaufen. So konnte gewährleistet werden, dass die erstellte Dokumentation für die folgende Entwicklung und Implementierung zu den bereits bestehenden Systemen und deren Dokumentation passt und ein konsistentes «Gesamtsystem RTI» resultiert.
Geprüft wurde das Ergebnis in diversen Testschichten im Labor, mit Blick auf einzelne Teilsysteme, auf das UX-Konzept bzw. die «Interaction Map» und das Gesamtsystem. Die System- und Abnahmetests wurden für jedes der drei Releases durch einen System-/Sicherheitsingenieur begleitet, sodass unmittelbar ein Vergleich zwischen beobachtetem Systemverhalten und Spezifikation erfolgte.

Befunde aus den Tests wurden mit Fachleuten aus dem Bahnbetrieb, den Entwicklungsteams, UX-Expert:innen und der Projektleitung diskutiert, bewertet und – falls notwendig – behoben. Parallel wurden Schulungen für die Bediener:innen des Systems durchgeführt, um eine reibungslose Integration in den Betrieb zu ermöglichen: Die Inbetriebnahme eines neuen Releases erfolgt innerhalb einer Nacht; sprichwörtlich von heute auf morgen müssen die Fahrdienstleiter:innen und Disponent:innen Bahnverkehr mit einem neuen System den realen Bahnbetrieb sicher abwickeln.

Funktionsnachweis im realen Betrieb
Die erste Prüfung der neuen Funktionalitäten des Systems RTI im kommerziellen Betrieb ergab sich am 17.10.2022 unter Release 2.1: Durch eine Weichenstörung im Spurwechsel Sedrun (GBT) war die Oströhre unpassierbar geworden; für drei nordwärts im Tunnel verkehrende Züge gab es keine (vorwärts gerichtete) Möglichkeit mehr, diesen zu verlassen. In dieser Situation wurde – nach Kenntnisstand der Autoren zum ersten Mal überhaupt – Reversing, also eine Rückwärtsevakuation unter ETCS L2 ohne Personal an der Zugspitze, bei einer Störung im kommerziellen Betrieb angewendet.
Die entsprechend geschulte Fahrdienstleiterin nutzte die neue Funktionalität, um im vorliegenden Störungsfall die Züge rückwärts bis zum Spurwechsel in Faido bzw. aus dem Tunnel hinaus nach Pollegio zu führen, von wo aus sie ihre Fahrt nach Norden durch die Weströhre fortsetzen konnten. Die SBB schätzen, dass die Dauer bis zur Wiederaufnahme des planmässigen kommerziellen Betriebs nach der Störung im Vergleich zur Variante, die Züge mithilfe der Lösch- und Rettungszüge (LRZ) abzuschleppen, um mindestens 1 bis 1½ Stunden reduziert wurde. Damit erfolgte im realen Betrieb ein Funktionsnachweis für das Zusammenspiel der technischen Systeme untereinander und mit den Bedienenden, der als Meilenstein für das Reversing unter ETCS L2 betrachtet werden kann.

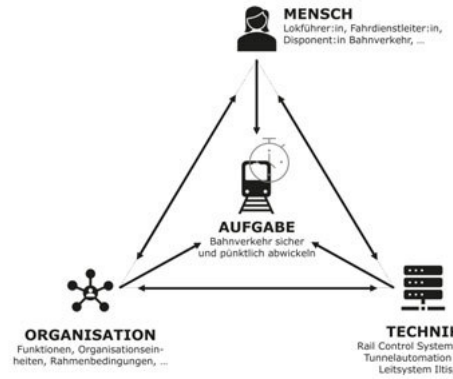

Bild 2: Wechselwirkungen zwischen Mensch, Technik, Organisation und Erfüllung der Aufgabe. Nur wenn allen Bereichen, den jeweiligen Stärken und Schwächen sowie insbesondere der Abstimmung untereinander genügend Beachtung geschenkt wird, können höchste Standards erreicht werden. (Eigene Darstellung)

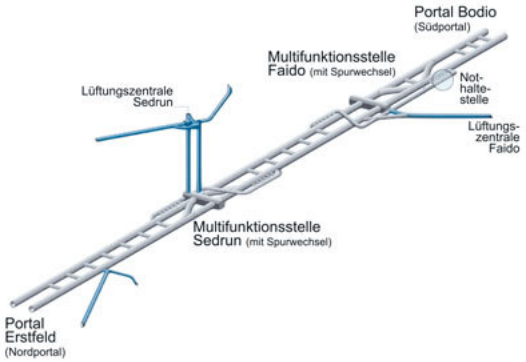

Bild 3: Schematische Übersicht über die Tunnelröhren, Querschläge, Kavernen, Schächte und Stollen des Gotthard-Basistunnels

Mit der Inbetriebnahme von Release 2.2 in der Nacht auf den 7.11.2022 konnte das Projekt «Entwicklung RTI» – bis auf Dokumentationspflichten, welche durch die Sicherheitsingenieure noch zu erfüllen sind – erfolgreich abgeschlossen werden. Alle Auflagen des BAV gelten als erfüllt. Die betrieblichen Einschränkungen wurden aufgehoben, das Projekt «Abschlussarbeiten SA GBT» war erfolgreich, und der Weg für einen (noch) dichteren Fahrplan auf der Gotthard-Basislinie ist frei.

Ausblick: Übertragung auf den Ceneri
Mit dem Projekt «Entwicklung RTI» wurden am GBT nicht nur neue Funktionalitäten, sondern auch eine neue Bedienoberfläche für die Tunnelautomatik eingeführt. Somit sind nun die beiden Basistunnel Gotthard und Ceneri, die von derselben Betriebszentrale aus und teilweise von denselben Personen gesteuert werden, unterschiedlich zu bedienen.
Um diese Divergenz zu beheben, haben die SBB bereits ein Nachfolgeprojekt für den CBT gestartet, mit dem die für den GBT erzielten Fortschritte auf den CBT zu übertragen und punktuell weitere Verbesserungen zu realisieren sind. Auch dieses Projekt wird nach SN EN 50126 durchgeführt und wird einen Beitrag zu mehr Stabilität, kürzeren Störungsdauern und höherer Sicherheit im Bahnbetrieb leisten.

Über die Autoren
Dr. Axel Bomhauer-Beins studierte an der ETH Zürich Elektrotechnik und promovierte ebenfalls dort im Verkehrswesen mit Schwerpunkt Energieoptimierung im Bahnbetrieb. Seither ist er als Ingenieur und Projektleiter im Bereich Verkehrsinfrastrukturen mit Fokus Safety für die AFRY Schweiz AG tätig.

Dr. David Grabowski studierte Physik an der Albert-Ludwigs-Universität Freiburg (D) und promovierte dort. Anschliessend war er in verschiedenen Positionen in der Entwicklung sicherheitsrelevanter Systeme in der Luftfahrt tätig und wechselte 2014 zu den SBB. Dort ist er in verschiedenen Positionen und Projekten als Safety Manager aktiv, so auch für die «Entwicklung RTI».