Formalisierung als Erfolgsfaktor für die ERTMS Level 2-Verifikation

Formalisation as a success factor for ERTMS Level 2 verification

Henrik Roslund | Christoph Bieri | Robert Eschbach

Das Schweizerische Bundesamt für Verkehr (BAV) hat 2023 eine Strategie für einen landesweiten ERTMS-Roll-out (European Rail Traffic Management System, ERTMS) veröffentlicht. Manuelle Prüfungen von ERTMS-Anlagen erweisen sich angesichts der Datenmengen und Komplexität als unverhältnismäßig zeitaufwendig und fehleranfällig. Um den geplanten Roll-out zu bewältigen und Fehlerquellen zu reduzieren, ist eine weitgehende Automatisierung der Planprüfung erforderlich. Dieser Beitrag beschreibt die Erfahrungen, die für ein Digitalisierungsprogramm in diesem Bereich von Bedeutung sind.

1 Die ERTMS-Strategie des BAV

Die ERTMS-Strategie [1] des BAV beinhaltet die konsequente Umsetzung der Führerstandsignalisierung (FSS) auf Basis eines Umsetzungskonzepts, das 2025 von den Infrastrukturbetreibern (ISB) für das gesamte interoperable Schweizer Normalspurnetz vorgelegt werden muss. Die Strategie betrifft Neubauten und Erneuerungen von Bestandsanlagen. Diese müssen ausschließlich mit FSS realisiert werden, während optische Signalisierung nur noch in Ausnahmefällen vorgesehen ist.

Diese Strategie impliziert einen systematischen Roll-out. Um diesen Roll-out zu gewährleisten, umfasst die ERTMS-Strategie des BAV mehrere wichtige strategische Maßnahmen. Ein wesentlicher Fokus liegt auf der Digitalisierung und Industrialisierung der Prozesse der ISB. Für die Prüfprozesse ist die Maßnahme I11 wegweisend: „Die Planungs-, Projektierungs- und Prüfprozesse für die Sicherungsanlagen (…) sind zu vereinfachen und zu beschleunigen, vor allem, indem Industrialisierung und Digitalisierung, insbesondere auch seitens ISB, mit Nachdruck umgesetzt werden."

Diese Maßnahme ist notwendig, da die heutigen Prüfprozesse von FSS-Projekten nicht für ein industrielles Roll-out tauglich sind. Dies wurde bereits vor einigen Jahren erkannt und ein Pilotprojekt für die formale Verifikation in den Jahren 2022 – 2024 durchgeführt. Aufgrund von veränderten Anforderungen und technologischen Entwicklungen wurde dieses nun als Projekt in ein größeres Digitalisierungsprogramm integriert.

2 Aktueller ERTMS Level 2-Umsetzungsstand

In der Schweiz sind mehrere Strecken mit FSS in Betrieb, die sowohl Personen- als auch Güterverkehr ermöglichen und teilweise Teil des ERA TEN-T-Netzwerks (European Rail Agency – Trans European Network) sind. Zu den bedeutendsten gehören die Neubaustrecke (NBS) Mattstetten – Rothrist, der Gotthard-Basistunnel (GBT), Ceneri-Basistunnel (CBT) und der Lötschberg-Basistun-

The Swiss Federal Office of Transport (FOT) has published the strategy for the nationwide rollout of European Rail Traffic Management System (ERTMS) in 2023. Manual verification of ERTMS systems is increasingly proving to be extremely time-consuming and error-prone due to the large volume of data and system complexity. Extensive automation of the verification process is necessary so as to manage the planned rollout and minimise any error sources. This article describes some important experience gained from a digitalisation program in this area.

1 The FOT's ERTMS strategy

The FOT's ERTMS strategy [1] includes the consistent implementation of cab signalling based on an implementation concept that the infrastructure managers (IM) have to submit for the entire interoperable Swiss standard-gauge network in 2025. The strategy applies to both new and renewed infrastructure. In the future, only cab signalling will be implemented, while optical signalling will only be allowed in exceptional cases.

This strategy implies a systematic rollout. The FOT's ERTMS strategy contains several necessary strategic measures in support of this rollout. One key focus involves the digitalisation and industrialisation of the IM processes. Measure I11 points the way to the future for testing processes: "The planning, data preparation and testing processes for the railway signalling systems (...) must be simplified and accelerated, in particular while strenuously pursuing industrialisation and digitalisation, especially by the IMs."

Measure I11 is indispensable since the current verification processes for cab signalling projects are unsuitable for industrialised deployment. This problem was identified several years ago and a pilot project for formal verification was carried out between 2022 and 2024. The project has recently been incorporated into a broader digitalisation program due to evolving requirements and technological progress.

2 The current ERTMS Level 2 implementation status

Several lines with cab signalling are currently being operated in Switzerland for both passenger and freight transport. Some of these lines constitute part of the ERA TEN-T network (European Rail Agency – Trans European network). The most important lines are the Mattstetten – Rothrist railway line (NBS), the Gotthard Base Tunnel (GBT), the Ceneri Base Tunnel (CBT) and the Lötschberg Base Tunnel (LBL) as integral parts

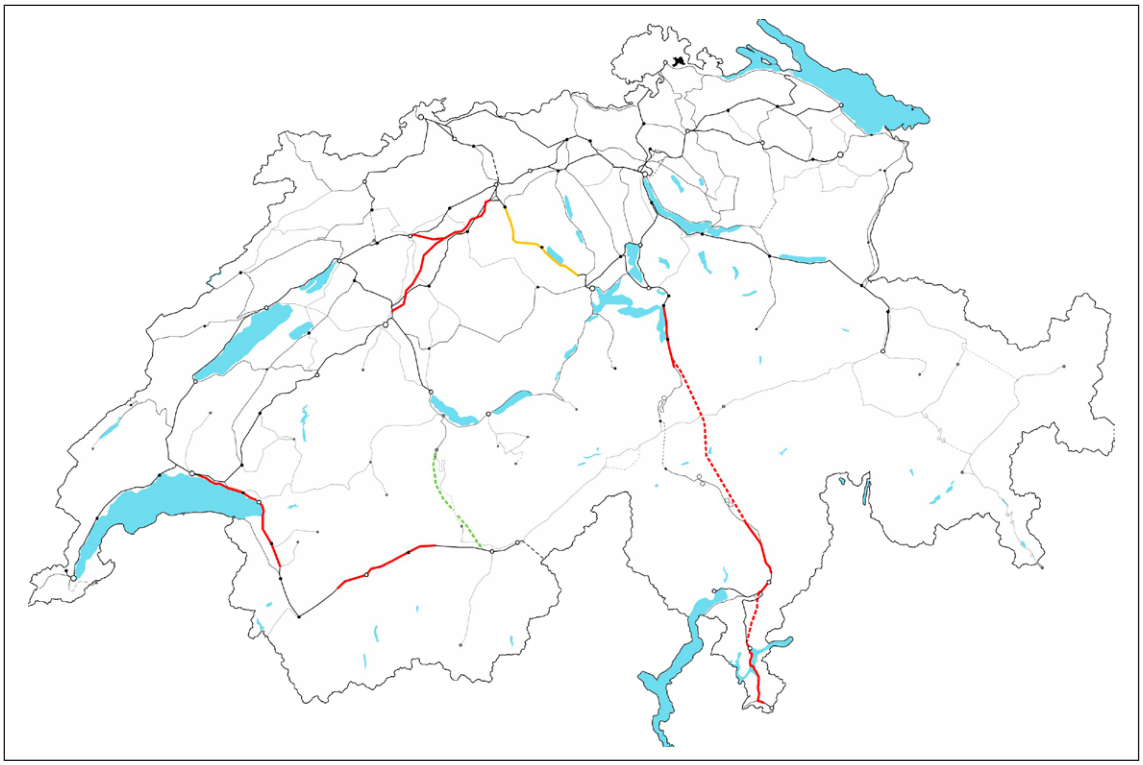

Bild 1: Aktueller ERTMS Level 2-Umsetzungsstand
Fig. 1: The current ERTMS Level 2 implementation status
Quelle / *Source*: SBB

nel (LBL) als integraler Bestandteil des bestehenden ERTMS-Netzwerks, das neun Radio Block Centre (RBC) umfasst (Bild 1).
Mit der fortschreitenden Umsetzung der ERTMS-Strategie des BAV wird der Anteil der mit FSS ausgerüsteten Strecken in den nächsten Jahren weiter anwachsen. Für die nächsten beiden Jahre sind bereits fünf neue Anlagen zur Verifikation angemeldet. Diese laufenden und geplanten Projekte unterstreichen das Engagement der Schweizer Bahnen bei der Modernisierung der Zugsicherung im Rahmen der europäischen Interoperabilitätsbestrebungen.

3 Herausforderungen bei der Planprüfung

Die Prüfung von ERTMS Level 2 (L2)-Plandaten ist mit verschiedenen Aspekten verbunden, die eine effiziente und präzise Bearbeitung erfordern. Aufgrund der aktuellen Projekte von ERTMS L2-Anlagen mit tabellarischen Projektdaten (Bild 2) und komplexen Regeln, die darauf angewendet werden müssen, entsteht eine erhöhte Prüflast. Manuelle Prüfprozesse sind zwar bewährt, auf diese Daten angewendet jedoch unverhältnismäßig zeitaufwendig (viele hundert Stunden) und dennoch fehleranfällig.
Bei manuell erstellten Datentabellen sind die syntaktischen Vorgaben oft nicht eingehalten. Dies kann den Prüfaufwand zusätzlich vervielfachen. Die Herausforderungen sind im Einzelnen:

- Datenmenge: Ein typisches FSS-Projekt umfasst hunderte von Weichen, Marker Boards und Balisen, was zu großen Datenmengen führt. Die Gesamtheit der Unterlagen für eine FSS-Anlage heißt Sicherungsanlagen-Konzept (SA-Konzept) und beinhaltet neben Plänen und projektspezifischen Dokumenten auch die Tabellen mit allen erforderlichen Daten. Diese SA-Konzept-Tabellen (SAK-T) bilden das Gefäß in einem proprietären Format, das mit ca. 800 Syntaxanforderungen [3] spezifiziert wird. Diese Werte (an die 100 000) müssen auf Einhaltung von ca. 260 Projektierungsregeln [2] geprüft werden.
- Datenqualität: Daten, welche manuell oder durch nicht durchgängige Toolketten erstellt werden, resultieren meist in syntak-

of the existing ERTMS network, which contains nine radio block centres (RBC) (fig. 1).
The further implementation of the FOT's ERTMS strategy means that the share of lines equipped with cab signalling will continue to grow over the next few years. Five new installations have already been requested for verification in the next two years. These present and further planned projects emphasise the Swiss railways' commitment to modernising its train control systems as part of its European interoperability efforts.

3 Challenges in the verification process

The verification of ERTMS Level 2 (L2) planning data is associated with multiple aspects that demand efficient and accurate processing. The current approach, using tabulated project data and complex rules, leads to a huge verification workload (fig. 2). Although manual verification methods are well-established, they are incredibly time-consuming, i.e. take hundreds of hours, and are still prone to errors.
The syntactic specifications are frequently not adhered to during the manual creation of data tables, thereby significantly increasing the verification effort. The identified challenges:

- data volume: a typical cab signalling project contains hundreds of switches, marker boards and balises, which leads to large volumes of data. The entirety of the planning and data preparation documents for a cab signalling system is called a signalling concept ("SA-Konzept" in German). In addition to the plans and project-specific documents, this also includes tables containing all the necessary data. These signalling concept tables (SAK-T) constitute a container in a proprietary format that follows approximately 800 syntax rules [3]. The values in these tables (approximately 100,000) must be verified for compliance with around 260 planning rules [2].

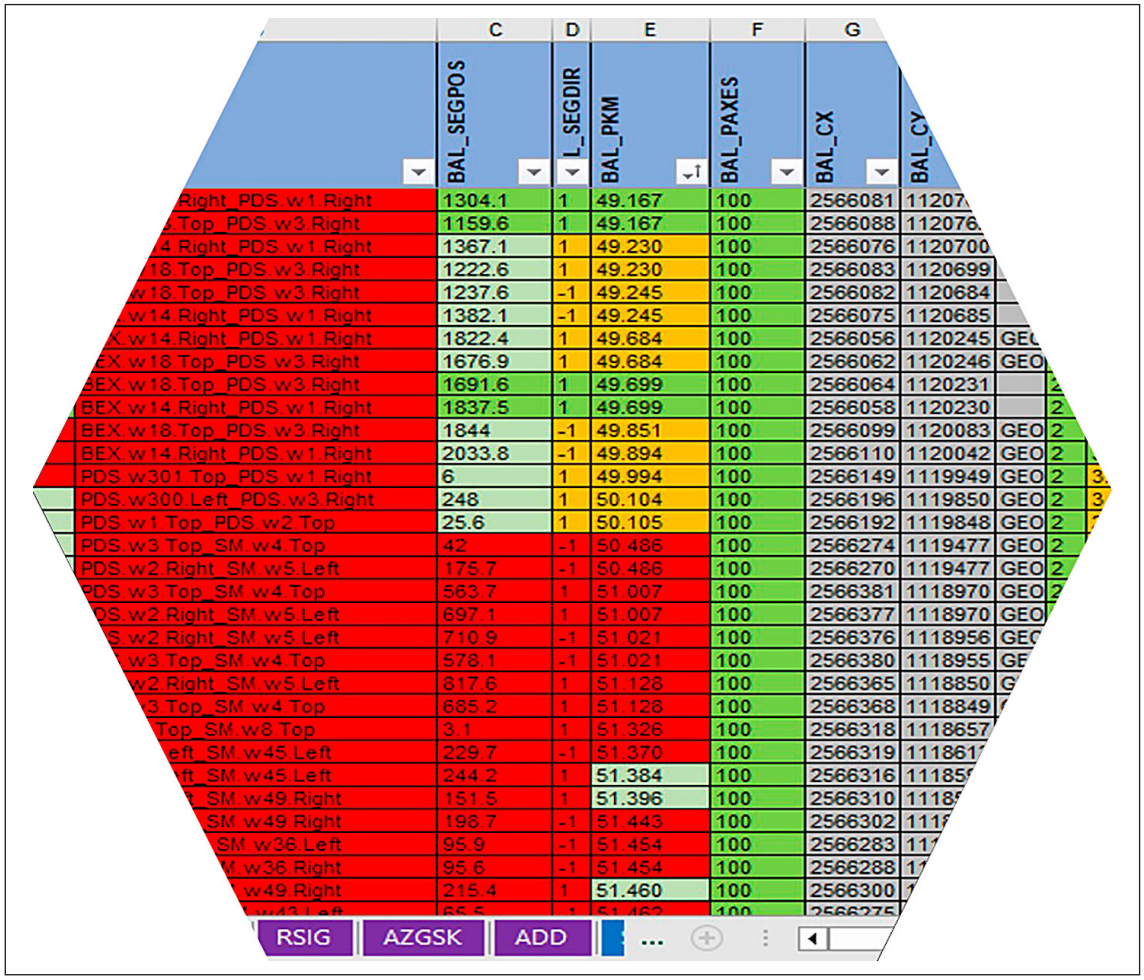

Bild 2: Herausforderungen bei der Planprüfung
Fig. 2: Challenges in plan checking
Quelle / *Source*: SBB

tisch nicht korrekten Daten und verhindern dadurch die automatisierte Weiterverarbeitung im Verlauf des Prozesses.

- Kombination verschiedener Versionen: In einem System, das sich in Entwicklung befindet, ändern sich die Projektierungsregeln und andere Anforderungen laufend. Eine FSS-Anlage deckt einen großflächigen Einsatzbereich ab, der mehrere Stellwerkperimeter beinhalten kann und jeweils in einem einzigen Projektierungsdatensatz (SAK-T) abgebildet ist. Bei einer späteren Anpassung der Anlage haben sich die Projektierungsregeln möglicherweise bereits geändert. Der Bestandsschutz besagt, dass nur angepasste Elemente nach den neuesten Vorgaben umgesetzt werden müssen. So entsteht eine Anlage, die nicht einheitlich nach einer einzigen Version der Projektierungsregeln realisiert ist. Eine manuelle Prüfung kann mit diesem Umstand pragmatisch umgehen. Für eine automatisierte Prüfung erfordert das eine präzise Definition, wie der Bestandsschutz gehandhabt werden soll. Alle Tools der ganzen Prozesskette müssen damit umgehen können, wenn nicht bei jeder kleinen Änderung die ganze Anlage aktualisiert werden soll.
- Datenmodell: Ein Datenmodell bildet das Rückgrat für eine effiziente und zuverlässige Verarbeitung von Anlagendaten. Es muss in der Lage sein, die komplexen Zusammenhänge und Abhängigkeiten innerhalb einer Anlage präzise abzubilden. Sowohl Vorgaben als auch die Anlage selbst unterliegen einer stetigen Entwicklung. Das Datenmodell muss flexibel genug sein, um diese Änderungen zu verarbeiten, ohne die Konsistenz und Integrität der Daten zu gefährden. Eine sorgfältige Planung und Strukturierung des Datenmodells sind daher unerlässlich und eine wichtige Grundlagenarbeit.

- data quality: data created manually or using non-continuous tool chains often results in syntactically incorrect data and thus prevents any further automated processing.
- the combination of different versions: the planning rules and other rules in a system under development often change. A cab signalling system covers a significant area, which can include several interlocking perimeters, and is specified in a single planning data set (SAK-T). If the project is subsequently adapted, the planning rules may also change. Grandfathering rights mean that only the newly adapted elements have to be implemented according to the latest rules. This results in a project that has not been uniformly realised on the basis of a single version of the planning rules. Manual verification is able to deal with this situation on a pragmatic basis. However, automated verification requires precise rules on how to deal with any grandfathering rights. All the tools throughout the process chain must be able to deal with this, otherwise the overall project will need to be updated as a whole every time a small change is made.
- the data model: a data model constitutes the backbone for the efficient and reliable processing of the project data. It must be able to map the complex relationships and dependencies within a project accurately. Both the specifications and the project itself are subject to constant development. The data model must be flexible enough to process these changes without jeopardising the consistency and integrity of the data. The careful planning and structuring of the data model are therefore essential.

Gemäß einer strategischen Entscheidung soll railML künftig als Standard-Datenformat verwendet werden. Dies ist eine Chance, dass alle Werkzeuge darauf abgestimmt werden und dadurch eine international gemeinsam verständliche Sprache gefunden wird.

- Release-Management: Mit der Freigabe von neuen Vorgaben muss das ganze System über den ganzen Projektierungs- und Prüfprozess auf diese neuen Vorgaben angepasst werden. Das heißt beispielsweise: Die Werkzeuge müssen SAK-T nach den neuesten Syntaxvorgaben erstellen können und die Prüfwerkzeuge müssen gegen die neuesten Projektierungsregeln prüfen können. Erst dann kann ein neues Release der Vorgaben in Anwendung kommen.

Vor dem Hintergrund dieser Herausforderungen werden manuelle Prüfungen sehr lang und teuer. Dies wirkt sich negativ auf den Projektablauf und Folgeprojekte aus. Zudem entstehen durch wiederholte Prüfungen und notwendige Korrekturen zusätzliche Kosten und administrative Mehraufwände. Eine frühzeitige teilautomatisierte Prüfung trägt dazu bei, den Prozess zu optimieren und die Planungsqualität zu erhöhen.

4 Vorgehen einer Automatisierung mit Formalisierung

Um die automatisierte Planprüfung zu ermöglichen, müssen Syntaxanforderungen [3] und Projektierungsregeln [2] auf Vollständigkeit und Konsistenz geprüft und ggf. angepasst werden. Dabei ist auch implizites, bislang nur mündlich überliefertes Wissen systematisch zu erfassen. Dieses aufwendige Requirements Engineering bildet die Grundlage für eine formale Datenvalidierung auf Basis mathematischer Datenmodelle und maschinenlesbarer Regeln.

Die Syntaxanforderungen [3] beschreiben die syntaktischen Vorgaben an die Elemente der Gleisnetztopologie. Hierbei wird das vom ERTMS-Systemführer Schweiz vorgegebene, proprietäre Datenformat SAK-T verwendet. Eindeutige und syntaktisch korrekte Bezeichnungen von Elementen bilden die Basis für ein mathematisches Datenmodell, welches die Grundlage für die Planprüfung gegen Projektierungsregeln darstellt. Die Überprüfung dieser Anforderungen stellt somit einen elementaren Bestandteil der Planprüfung dar. Erst nach erfolgter Syntaxprüfung und Korrektur ist eine Planprüfung gegen die Projektierungsregeln möglich.

Die Projektierungsregeln [2] beschreiben semantische Vorgaben an Länge von bzw. Grenzen zwischen Abschnitten, Distanzen zwischen bzw. Positionierung von Elementen auf der Gleistopologie, verfügbare Fahrwege, diverse Schutzfunktionen und weitere Eigenschaften dieser Elemente. Eine automatisierte formale Prüfung gegen diese Regeln hat viele Vorteile, kann aber nur erreicht werden, wenn

- Plandaten und Regeln eine eindeutige formale Semantik zugeordnet wird,
- Datenmodell und Regeln mit einem geeigneten Format formal spezifiziert werden,
- Datenmodell und Regeln von ausgewählten formalen Analysewerkzeugen automatisiert eingelesen und verarbeitet werden und
- der Umgang mit Bestandsschutz und Kombinationen von verschiedenen Versionen präzise geklärt ist.

Zur Auswahl geeigneter Methoden und Werkzeuge wurden die Anforderungen aus [2] und [3] auf Konsistenz, Vollständigkeit und Präzision geprüft und die technischen Möglichkeiten zur Umsetzung der oben aufgeführten Punkte bewertet. Dabei dienten Qualitätskriterien wie Funktionalität, Testbarkeit, Analysierbarkeit

It has been strategically decided that railML will be used as the standard data format in the future. This is an opportunity for all the tools to be harmonised and for a standard international language to be found.

- release management: as soon as new versions of the specifications or rules are released, the entire tool environment must be adapted to comply to these new specifications and rules throughout the entire planning and testing process. For example, this means that the planning tool must be able to create SAK-T according to the latest syntax specifications and the test tools must be able to undertake verification in compliance with the latest planning rules. The prerequisite is therefore that the new release of the specifications or rules be used.

These challenges have led to manual verification becoming time-consuming and expensive. This harms the project process as well as any subsequent projects. Additionally, any repeat verifications and necessary corrections result in increased costs and administrative overheads. Partially automated verification at an early stage helps to optimise the process and increase the planning quality.

4 Automatisation with formalisation

The syntax [3] and planning rules [2] have to be checked for completeness and consistency and adjusted where necessary so as to enable automated verification. Implicit knowledge that has previously only been shared on a verbal basis now also needs to be systematically collected. This extensive requirements engineering forms the basis for the formal data validation based on mathematical data models and machine-readable rules.

The syntax rules [3] describe the syntactic specifications for the elements of the track network's topology. The proprietary SAK-T data format specified by the Swiss ERTMS system leader is used here. Unambiguous and syntactically correct designations of elements form the basis for a mathematical data model, which in turn constitutes the foundation for verifying compliance with the planning rules. Verifying these rules therefore constitutes a fundamental part of the plan verification. Verification against the planning rules is only possible once the syntax has been checked and corrected.

The planning rules [2] describe the semantic specifications for the length of or boundaries between the sections, the distances between or positioning of elements on the track topology, the available routes, various protective functions and any other properties of these elements. Automated formal verification against these rules has many advantages, but can only be achieved if

- the data and rules have been assigned precise, formal semantics,
- the data model and rules have been formally specified in a suitable format,
- the data model and rules are automatically read and processed by selected formal analysis tools and
- the handling of grandfathering rights and combinations of different versions has been precisely clarified.

The requirements from [2] and [3] have been checked for consistency, completeness and precision and the technical feasibility of implementing the above points has been evaluated for the selection of the suitable methods and tools. Quality criteria such as functionality, testability, analysability and reliability [4] have served as the basis for the decision-making. The automated veri-

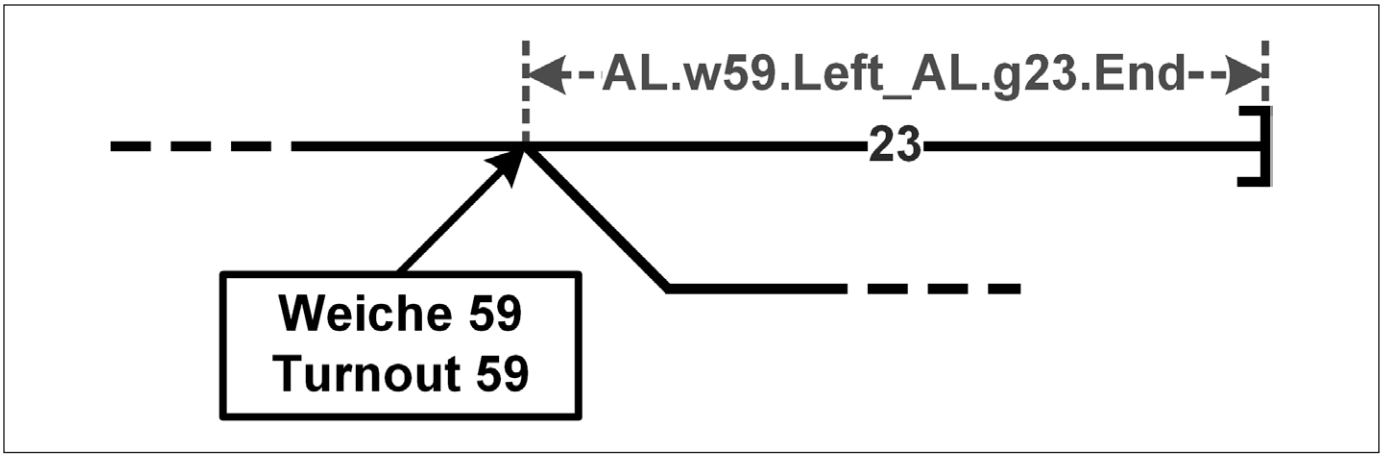

Bild 3: Vorgehen einer Automatisierung mit Formalisierung; Syntaxbeispiel
Fig. 3: The automation with formalisation procedure; a syntax example

Quelle / *Source*: Henrik Roslund

und Zuverlässigkeit [4] als Entscheidungsgrundlage. Die automatisierte Prüfung der Syntaxanforderungen erfordert andere Vorgehensweisen, Techniken und Werkzeuge als die automatisierte Überprüfung von Projektierungsregeln. Neben der Prüfung, ob die Syntaxanforderungen korrekt umgesetzt sind, müssen syntaktisch korrekt zusammengesetzte Spezifikationsanteile oft präzise in kleinere Bestandteile zerlegt werden können. Welche Bestandteile das sind, ergibt sich sowohl aus den Syntaxanforderungen selbst als auch aus den Projektierungsanforderungen, die in ihren semantischen Vorgaben auf bestimmte Bestandteile Bezug nehmen.

Beispielsweise muss ein Segment der Gleistopologie die Verbindung zweier Referenzpunkte darstellen: Vom ersten Punkt in Altdorf (AL) bei Weiche 59 (w59) über den linken Weichenschenkel (Left) zum zweiten Punkt in Altdorf (AL) am Ende des Gleises 23 (g23.End) ergibt das Segment mit dem Namen: AL.w59.Left_AL.g23.End. Um die Konsistenz mit der bestehenden Gleisnetztopologie prüfen zu können, muss dieses Segment wieder in seine einzelnen Teile zerlegt werden (Bild 3).

Die Syntaxanforderungen bilden die Grundlage für eine formale Syntax der Plandaten und darauf aufbauend eine formale Semantik, also eine eindeutige Zuordnung von syntaktisch korrekten Datenbeschreibungen zu konkreten Daten, die in der formalen Datenvalidierung analysiert werden können. Neben der reinen Prüfung der Syntaxanforderungen und der korrekten Zerlegung in kleinere Bestandteile ist ein weiterer Aspekt von zentraler Bedeutung: Plandaten müssen in andere Datenformate übersetzt werden können. Für die formale Datenvalidierung sind sowohl die von Analysewerkzeugen unterstützten Datenformate als auch Formate wie SQL für relationale Datenbanken und railML zentral. Für die Prüfung von Syntaxanforderungen werden Techniken aus dem Bereich der formalen Sprachen und des Compilerbaus verwendet, die die oben genannten Herausforderungen am besten adressieren. In diesem Bereich dienen Grammatiken zur formalen Beschreibung der Anforderungen. Für die Überprüfung der durch die Grammatik formalisierten Anforderungen wird ein sogenannter Parser eingesetzt, der automatisiert die Einhaltung der Grammatikregeln überprüft und Möglichkeiten der Zerlegung und Übersetzung bietet. Der Parser wird dabei automatisiert aus den Grammatiken generiert, muss also nicht fehleranfällig und zeitaufwendig programmiert werden. Die Qualitätssicherung erfolgte gemäß den Vorgaben der EN 50128:2011 für unterstützende Werkzeuge und Sprachen, unter anderem über automatisierte Tests, die in einem speziellen Testframework durchgeführt werden.

fication of syntax rules requires different approaches, techniques and tools than the automated verification of planning rules. In addition to verifying whether the syntax rules have been correctly implemented, any syntactically correct specification components also often need to be broken down precisely into smaller parts. The specific components are determined by both the syntax rules themselves and the planning rules, which refer to specific components in their semantic specifications.

For example, a segment of the track topology must represent the connection between two reference points: the area from the first point in Altdorf (AL) at turnout 59 (w59) via the left leg of the turnout (Left) to the second point in Altdorf (AL) at the end of track 23 (g23.End) results in a segment entitled AL.w59.Left_AL.g23.End. This segment must be broken down into its individual components again so as to verify the consistency with the existing track network's topology (fig. 3).

The syntax rules provide the foundation for a formal planning data syntax and, building on this, formal semantics, i.e. the unique assignment of syntactically correct data descriptions to specific data that can be analysed in the formal data validation. In addition to simply verifying the syntax rules and the correct decomposition into smaller components, yet another aspect is also of central importance: it is necessary to be able to translate the planning data into other data formats. Both the data formats supported by analysis tools and formats such as SQL for relational databases and railML are central to formal data validation. Techniques from the field of formal languages and compiler construction are used to verify the syntax rules, as they best address the aforementioned challenges. Grammars are used in this area to describe the rules formally. A so-called parser is used to verify the rules formalised by the grammar, which automatically checks the compliance with the grammar rules and offers options for decomposition and translation. The parser is generated automatically from the grammars and therefore does not have to be programmed in an error-prone and time-consuming manner. Quality assurance has been carried out in accordance with the requirements of EN 50128:2011 for supporting tools and languages, including automated tests conducted within a special test framework.

The planning rules must be formalised at an appropriate level of abstraction. Modelling based on set theory was chosen here, which naturally corresponds to the level of abstraction for the rules from [2]. Techniques from the fields of constraint solving and model checking have primarily been used to verify the rules

Die Projektierungsregeln müssen auf einer geeigneten Abstraktionsebene formalisiert werden. Hierbei wurde eine mengentheoretische Modellierung gewählt, die dem Abstraktionsgrad der Regeln aus [2] natürlich entspricht. Zur Überprüfung der Regeln gegen die formalen Plandaten wurden hauptsächlich Techniken aus den Bereichen Constraint Solving und Model Checking verwendet. Hierbei sind terminierende Prüfabläufe, die zu eindeutigen Prüfergebnissen führen, eine zentrale Anforderung. Ein hoher Grad an Nicht-Determinismus bei der Auswahl konkreter Prüfschritte und viele Abhängigkeiten zwischen einzelnen Prüfschritten verlangen eine angemessene und korrekte Umsetzung der formalen Prüfung. Die formale Datenvalidierung wurde hierzu mit formalen Constraints und einem Constraint Solver durchgeführt, die Ergebnisse mit einem Model Checker formal verifiziert und damit abgesichert. Neben automatisierten Prüfschritten werden auch manuelle, von Prüfexperten durchzuführende Prüfschritte berücksichtigt. Die Koexistenz von automatisierten und manuellen Prüfschritten stellt eine weitere Herausforderung an die Prüfabläufe dar.

5 Erkenntnisse

Um den aktuell steigenden Prüfaufwand bewältigen zu können und gleichzeitig die Vorbereitungen für den bevorstehenden Roll-out voranzutreiben, ist ein zweistufiges Vorgehen erforderlich:

5.1 Stufe 1: Weiterentwicklung der bestehenden Tools und Prozesse

Die heutigen Methoden und Tools sind nicht für einen industrialisierten Roll-out tauglich und werden diesen Grad an Reife auch nicht erreichen. Dennoch müssen die heute verwendeten Tools weiterentwickelt werden, um sicherzustellen, dass das kommende Prüfvolumen gestemmt werden kann. Diese Weiterentwicklung muss in stetem Abwägen von Kosten und Nutzen geschehen, da diese Werkzeuge eine beschränkte Lebenszeit haben und dennoch verlässlich angewandt werden müssen. Hier fließen auch die Resultate aus den früheren Automatisierungsbestrebungen ein und unterstützen so direkt den bestehenden Prüfprozess. Der Nutzen solcher Investitionen darf jedoch nicht nur in der Produktivität der Prüfung gesehen werden: Auch Erkenntnisse für die nächste Toolgeneration sind wertvoll. Fehlentwicklungen sind auf dieser Stufe viel günstiger zu korrigieren als danach.
Diese bestehenden Werkzeuge müssen so lange ihren Dienst leisten, bis eine neue Generation eines umfänglichen Verifikationstools produktiv angewandt werden kann.

5.2 Stufe 2: Fokus auf umfassende Digitalisierung mit möglichst vollautomatischer Verifikation

Gleichzeitig läuft die Konzeptphase für die Gesamtarchitektur der Tool-Kette von der Planung über die Prüfung bis hin zur Inbetriebnahme. Das Verifikationstool muss sich in die angestrebte Architektur einbetten, um die Datendurchgängigkeit sicherzustellen.
Bei diesem zweistufigen Vorgehen ist es besonders wichtig, dass nicht das Eine zulasten des Anderen begünstigt wird, und auch die Migration vom Alten zum Neuen muss früh genug und ganz konkret geplant werden.
Die Erfahrungen aus den ersten Automatisierungsbestrebungen haben viele Erkenntnisse gebracht, beispielsweise:

- Obwohl die unabhängige Verifikation ein guter Ansatzpunkt ist, um ein System in digitalisierter Ausprägung entwickeln zu können, bestehen Abhängigkeiten, die eine isolierte Entwicklung verhindern können. In unserem Fall ist während der Entwicklung die Entscheidung gefallen, dass die Plandaten im railML-

against the formal planning data. Scheduled verification processes that lead to unambiguous verification results are a key requirement. A high degree of non-determinism in the selection of specific verification steps and the many dependencies between the individual verification steps require the appropriate and correct implementation of formal verification. The formal data validation has been performed using formal constraints and a constraint solver and the results formally verified and validated using a model checker. In addition to the automated verification steps, manual verification steps performed by verification experts have also been taken into account. The coexistence of automated and manual verification steps represents a further challenge to the verification processes.

5 Findings

A two-stage approach is required to cope with the currently increasing testing effort and at the same with the preparations for the upcoming rollout:

5.1 Stage 1: Further development of the existing tools and processes

The current methods and tools are not suitable for large-scale deployment and will not attain this level of maturity. Nonetheless, the tools in use today must be further developed to handle the upcoming test volume. This development should be continuously balanced against the costs and benefits, as these tools have a limited lifespan and need to be dependable. Previous automation efforts have also informed this process, supporting the existing testing framework. However, the value of such investments extends beyond merely increasing verification productivity; insights for future tool generations are also important. The early identification of errors is much more advantageous than addressing them later.
These existing tools must continue to perform their functions until a new generation of comprehensive verification tools can be utilised productively.

5.2 Stage 2: Focus on comprehensive digitalisation with fully automated verification wherever possible

At the same time, the concept phase for the overall architecture of the tool chain is underway: from planning and testing through to commissioning. The verification tool must be integrated into the desired architecture so as to ensure data consistency.
This two-stage approach means it is particularly important that one is not favoured at the expense of the other and the migration from the old to the new must also be planned early enough and very concretely.
The experience gained from the first automation endeavours has provided many insights, for example:

- even though independent verification is a good starting point for developing a system in digital form, some dependencies can hinder isolated development. In our case, it was decided during development that the planning data must be available in railML format, which fundamentally differs from the proprietary format of the SAK-T and makes the developed syntax verification obsolete in future.
- a syntactically correct database is a prerequisite for starting test automation. The generating software must ensure data quality.
- the dynamic environment with changing planning rules and lively processes is a fact. All the tools must be able to deal with this.

Format vorliegen müssen, was sich grundlegend vom proprietären Format der SAK-T unterscheidet und die entwickelte Syntaxprüfung künftig hinfällig macht.
- Eine syntaktisch korrekte Datenbasis ist eine Voraussetzung, um eine Prüfungsautomatisierung zu starten. Die Datenqualität muss zwingend durch die generierende Software sichergestellt werden.
- Das dynamische Umfeld mit sich wandelnden Projektierungsregeln und lebendigen Prozessen ist Fakt. Jegliche Tools müssen damit umgehen können.
- Der Einsatz formaler Methoden und Parser-Technologien zur Automatisierung von ETCS L2-Planprüfungen bietet großes Potenzial zur Effizienz- und Qualitätssteigerung.

Um die ambitionierten Ziele der BAV-Strategie [1] zu erreichen, müssen jedoch noch technische und organisatorische Herausforderungen gemeistert werden:
Technische Schwerpunkte sind dabei die Standardisierung von Datenformaten, insbesondere durch die Nutzung von railML, sowie die Performanz-Optimierung der Werkzeuge und eine anwenderfreundliche Integration in die Planungsprozesse. Zudem gilt es, die Beschaffungsstrategie für Prüfwerkzeuge und -dienstleistungen zu optimieren.
Der organisatorische Schwerpunkt liegt auf der iterativen Entwicklung: Da die Industrialisierung in einem komplexen System wie bei Eisenbahn-Sicherungsanlagen viele gegenseitige Abhängigkeiten aufweist, kann nicht sequenziell vorgegangen werden. So würde eine komplette Überarbeitung der Projektierungsregeln nicht zu sinnvollen Ergebnissen führen, ohne dass parallel auch deren Formalisierung und die Spezifikation des Datenformats weitergetrieben wird. Idealerweise wird dieses iterative Vorgehen koordiniert anhand einer einfachen Topologie mit wenigen Objekten angegangen und nach und nach an komplexere Themen herangeführt.

6 Fazit

Die konsequente Migration auf FSS erfordert eine umfassende Digitalisierung und Industrialisierung der Prüfprozesse. Während erste Fortschritte durch Pilotprojekte erzielt wurden, steht die Prüforganisation vor Herausforderungen wie der großen Prüflast und der Qualität der Plandaten. Um den bevorstehenden Roll-out erfolgreich zu gestalten, sind innovative Ansätze zur Automatisierung und Standardisierung notwendig. Die Integration eines durchgängigen Datenmodells und die iterative Entwicklung mit allen beteiligten Entwicklungsteams werden entscheidend sein, um die ambitionierten Ziele der ERTMS-Strategie zu erreichen. ■

- the application of formal methods and parser technologies to automate ETCS L2 verifications presents significant potential for enhancing efficiency and quality.

However, technical and organisational challenges still need to be overcome in order to achieve the ambitious goals of the FOT strategy[1]:
The focus here is on the standardisation of data formats, particularly through railML, as well as enhancing the performance of the tools and ensuring user-friendly integration into the planning processes. It is also crucial to optimise the procurement strategy for testing tools and services.
The organisational focus is on iterative development: given that industrialisation in a complex system such as railway safety systems has many interdependencies, it is not possible to proceed sequentially. For example, a complete revision of the planning rules would not lead to any meaningful results without their formalisation and the specification of the data format being driven forward in parallel. Ideally, this iterative approach should be coordinated using a simple topology with a small number of objects and gradually introduced to more complex topics.

6 Conclusion

The persistent implementation of cab signalling requires the comprehensive digitalisation and industrialisation of the testing processes. While initial progress has been made through pilot projects, the verification organisation faces challenges such as a high workload and the insufficient formal quality of the planning data. Innovative approaches to automation and standardisation are necessary in order to make the upcoming rollout a success. The integration of a consistent data model and iterative development with all the involved development teams will be crucial to achieving the ambitious goals of the Swiss ERTMS strategy. ■

LITERATUR | LITERATURE
[1] BAV (Hrsg.): ERTMS-Strategie BAV, Stand 2023, BAV-421.14-1/28/11/17/19: https://www.bav.admin.ch/bav/de/home/verkehrsmittel/eisenbahn/fachinformationen/zugbeeinflussung.html, vom 10.06.2025 15:43
[2] SBB AG (Hrsg.): Projektierungsregeln ETCS Level 2 KGB, Dokument #102, Version V 6.0, Datum: 21.08.2023, Dokumenten-ID: 97602070, Polarion Revision (1114115) vom 21.08.2023 13:38
[3] SBB AG (Hrsg.): Vorgaben an Sicherungsanlagenkonzepte ETCS Level 2, Anhang A3 zum Dokument #108, Version 4.1, Datum 24.02.2022, Dokumenten-ID: 101669103, Polarion Revision (740049) vom 02.02.2022 16:33
[4] Norm ISO/IEC 25010:2023 Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – Product quality model

AUTOREN | AUTHORS

Henrik Roslund
Seniorberater ERTMS Level 2, MIRSE / *Senior consultant ERTMS Level 2, MIRSE*
TÜV SÜD Schweiz AG
Anschrift / *Address*: Aargauerstraße 250, CH-8048 Zürich
E-Mail: henrik.roslund@tuvsud.com

Christoph Bieri
Leiter für die sicherheitsorientierte Verifikation von ERTMS Level 2 Projekten / *Manager for the safety-oriented verification of ERTMS Level 2 projects*
SBB Infrastruktur
Anschrift / *Address*: Hilfikerstraße 3, CH-3000 Bern 65
E-Mail: christoph.bieri@sbb.ch

Dr. Robert Eschbach
Berater ERTMS Level 2, Experte für Formale Methoden / *Consultant ERTMS Level 2, Formal Methods Expert*
M2C ExpertControl GmbH
Anschrift / *Address*: Industriestraße 12, D-82194 Gröbenzell
E-Mail: robert.eschbach@m2cec.com