

Tool Support for Validation of Formal System Models: Interactive Visualization and Requirements Traceability

Eduard Kamburjan

Department of Computer Science
Technische Universität Darmstadt, Germany
kamburjan@cs.tu-darmstadt.de

Jonas Stromberg

Department of Computer Science
Technische Universität Darmstadt, Germany
jonas.stromberg@stud.tu-darmstadt.de

Development processes in various engineering disciplines are incorporating formal models to ensure safety properties of critical systems. The use of these formal models requires to reason about their adequacy, i.e., to validate that a model mirrors the structure of the system sufficiently that properties established for the model indeed carry over to the real system. Model validation itself is non-formal, as adequacy is not a formal (i.e., mathematical) property. Instead it must be carried out by the modeler to justify the modeling to the certification agency or other stakeholders. In this paper we argue that model validation can be seen as a special form of requirements engineering, and that interactive visualization and concepts from requirements traceability can help to advance tool support for formal modeling by lowering the cognitive burden needed for validation. We present the VisualisierbaR tool, which supports the formal modeling of railway operations and describe how it uses interactive visualization and requirements traceability concepts to validate a formal model.

1 Introduction

The importance of formal methods for safety-critical systems has long been recognized in many engineering disciplines and is demanded or recommended by certification authorities in, e.g., railway engineering [6] and avionic [31] industries. Recently, with the increasing integration of computational parts into devices, digital twins [30] and co-simulation [14] are used to develop new products and prototype changes. One important class of formal methods in this area is formal system modeling.

Under formal system modeling we understand the development of a formal system model of a real system or of a design of a planned system (short: target system) that mirrors the structure and behavior of the target system sufficiently to prototype [18] and/or evaluate changes¹ [14]. Digital twins are a variant of this, which are integrated into the target system. Nonetheless, digital twins are based on a subsystem whose structure they must mirror as close as possible and face the same challenges for validation. Formal system modeling requires model validation to ensure that properties established for the formal model hold for the target system: While verification ensures that the model *behaves correctly*, validation ensures that the *correct thing* was modeled. Model validation itself is not formal (in the sense that it is not a mathematical property), it is an informal process to argue for the adequacy of the model and bridges between the intention of the developer and the realized model. Validation is required to convince safety assessors, such as certification agencies, that formal proofs have value in the certification process and other stakeholders that the prototypes developed in this model save development time for the target system.

Our main observation in modeling projects with industry partners is that certain stages of formal modeling can be seen as a specific form of requirements engineering.

¹We contrast formal system modeling with Model-Driven-Development approaches, where the model becomes the final system through refinement.

- *Requirements elicitation is model scoping.* Both these processes turn the *implicit* knowledge and assumptions of the user about the domain into an *explicit* representation. More importantly, they also decide on the aspects of the domain that are not needed for a specific model/project.
- *Requirements traceability is model validation.* Both tasks relate parts of the formal system model to the target system, which are the two main artifacts from requirements engineering view. Instead of tracing a requirement to the point where it is realized, one traces an aspect to the point where it is modeled. In reverse, instead of tracing backwards what requirement a part of the implementation is realizing, one traces what aspect a model-part realizes.

However, formal modeling poses challenges that prevent the straightforward adaptation of, e.g., Software Engineering practices. The boundary between modeling and programming is not clear [5], but concerning validating programs and formal system models of the described kind the main difference is that model validation of formal system models requires to validate a *white-box* model (in contrast to a black-box model when testing a program) and, in particular, raises the following points:

Cognitive Burden. Significant cognitive burden is required to judge formal system models, as formal modeling languages are not adopted by all industries and there is little training material available. Even in industries which use formal modeling, keeping the cognitive burden low is a desired aspect of adopters of formal methods in industry [26] and the cognitive burden of validation is higher than when designing, e.g., use cases and user stories.

Validating Structure. It is conceptually different to validate the *structure* of a white-box model, than to validate the *behavior* of a black-box model [1]. As formal modeling aims to mirror the structure precisely enough that changes in the model have the same causal effect as their counterpart in the target system, merely describing (by, e.g., test cases) the input/output does not suffice. This thwarts the application of behavior-centric approaches such as Behavior-Driven Development (BDD) [27].

Another experience we make in our work with domain experts is that merely *visualizing* a formal system model is not enough when using it to prototype new ideas [18]. Interaction with the visualization allows even quicker feedback cycles with the domain experts, as it allows them to test a specific situation for validation with little overhead to induce it into the model. This ties in with the above point of lowering the cognitive burden to simplify validation.

These observations raise the question how, and what, techniques for requirements traceability and interactive visualization can be applied to formal modeling. In particular, we are interested in integrating such techniques into an IDE that helps not only with model verification, but also with model validation.

We illustrate with the VisualisierbaR tool for formal modeling of railway operations how requirements traceability can be integrated into a formal methods toolkit and describe future research directions for formal modeling languages and toolkits.

Our main contribution is to develop tool support for model validation by integrating requirements traceability and interactive visualization into an IDE, as well as a tool and a case study illustrating this idea. This work is structured as follows: Sec. 2 describes model validation in railway operations, Sec. 3 gives an overview over a formal model in this domain, Sec. 4 describes the implementation of the VisualisierbaR tool, Sec. 5 describes the validation features, Sec. 6 gives two case studies from automatic train operations and rule prototyping and Sec. 7 concludes with related and future work.

2 Validation of Railway Operation Models

We describe our approach using the VisualisierbaR tool developed for the FormbaR model [19] for German railway operations. This section describes the specification of railway operations and the chal-

lenges of validating in this domain, while the approach itself is easily generalized to other domains.

2.1 Specification of Railway Operations

Railway operations for German railways are not described by a single document, but by (1) legal regulations, the “*Eisenbahn-Bau- und Betriebsordnung*” (*Law for Operating and Building Railways*) [10], (2) public rulebooks managed by Deutsche Bahn (DB), in particular Ril. 408 [7] and 819 [8], (3) internal rulebooks for operations, (4) requirements specification for technical elements, (5) training documentation and (6) internal announcements. FormbaR only considers the operations of DB, but other railway companies are also bound to the same legal regulations (and to Ril. 408 when using DB infrastructure), in addition to their own internal rulebooks.

In this environment, procedures are not described algorithmically in one place, but are described in a distributed manner. This makes it hard to pinpoint the exact point where the procedure is defined. E.g., the procedure to depart a train is partially described by Ril. 408 [7], partially by the requirements of the specific station interlocking in a station, partially by internal announcements and possibly by local exemptions (“*Lokale Zusätze*”). Implicitly, building regulations are also referenced, as certain minimal distances are assumed to hold.

These procedures are subject to constant change and completely new procedures for automatic train operations (ATO) and ETCS level 3 are in development. When scoping FormbaR, it was decided not to model certain rules, because they are not relevant to train operations itself but, e.g., specify interactions with the passengers [19].

2.2 Validating Railway Operation Models

Validation of models of new procedures requires to track each part of the model to the document that specifies it — legal regulations, rulebooks and technical documents are requirements and model validation entails documenting that the requirements are met. This is especially critical if these models are planned to be used for certification.

However, contrary to engineering projects, the form of the requirements is already fixed in a form that is optimized towards other uses – rulebooks are a form, which is difficult to process and which may not be changed during development. In terms of characteristics for software requirements [15], they are neither unambiguous, nor complete or modifiable². Furthermore, while there is a public specification in DOORS format available for the new European Train Control System (ETCS) modes of operations, the other rulebooks are written in plain natural language structured by sections and paragraphs. The use of technical documents that were not intended to be used as requirements for formal system models is not specific to railway engineering but is common in other fields, as formal models are mostly developed after the target system is finished. Similarly using the requirements of the original system can be problematic, as the formal model then expresses what the system is *supposed to do*, in contrast to what it really *does*. Nonetheless this can be of use, e.g., to analyze the design before implementation.

Not the complete model is directly related to requirements: some parts model basic infrastructure. E.g., FormbaR contains code for the physical behavior of the train, which is not explicit in any rulebook. For validation it is important to carefully distinguish between basic infrastructure and other model parts, since an error in the basic infrastructure is a mistake of the modeler, while an error in the other parts may hint towards a problem with the target system.

²Arguably, they are also neither consistent nor structured by importance.

2.3 Validating FormbaR

We use three techniques to validate FormbaR: simulation, interactive visualization and traceability.

Simulation. Simulation runs the model on predefined infrastructures and scenarios and checks that the behavior is the one expected by the domain expert, e.g., that after a fault on the infrastructure the train has the expected delay. This roughly corresponds to acceptance testing for software, but does not scale for bigger scenarios, e.g., because propagation of faults is not easily specifiable or predictable. Visualization scales better, as it is easier for a human to assess the visualized situation than to assess (or specify) the expected behavior as a trace.

Interactive Visualization Simulation is only able to detect errors in simple scenarios. A visualization tool shows the state of the whole infrastructure, e.g., the position of the train or the state of the signals. Interactive visualization is not merely a representation of the behavior of the system. The user interacts with the model via the visualization and introduces faults or gives orders to the train.

Interaction extends the use of visualization for validation. First, it is easier for the domain expert to assess the adequacy of the model if larger parts of the model can be inspected easily. Second, by interacting with the model he can explore the behavior of the model for questions arising during the validation. E.g., to check whether a certain combination of faults has been modeled correctly, when the interactions of faults is scattered in the model.

Requirements Traceability Simulation and interactive visualization treat the model as a black box and merely ensure that the behavior of the model corresponds to the expectations of the domain expert in a number of situations. To ensure that the *internal structure* of the model mirrors the internal structure of the domain we annotate the model and the visualization with links to the text files containing the specification.

Requirement links trace a requirement either forward (answering “*where is this requirement realized?*”) or backward (answering “*what requirement does this code realize?*”). Similarly, annotations are two-directional. A section of a rulebook links to the code in the model that implements it (i.e., is a forward trace link) and the code links to the rulebook it implements (i.e., is a backwards trace link). Links between model and specification are not enough, as the code may still implement a procedure that is described in several places. Visualization allows us to output messages that also contain links to the specification, to connect these representation without explicitly invoking the model. These links serve two purposes: First, they enable us to track in the visualization whether the procedure is executed correctly (i.e., according to specification). Second, they ensure that the visualization, which is an additional abstraction layer/artifact (additionally to rulebooks and formal model) is integrated into the validation of the formal model.

3 ABS and the FormbaR Model

In this section we give a short overview over the Abstract Behavioral Specification (ABS) language [16] and the FormbaR [19] model of railway operations. For brevity’s sake, we only introduce ABS and FormbaR as far as needed to explain VisualisierbaR; an introduction to ABS can be found in [16], an extended description of FormbaR in [19].

3.1 Abstract Behavioral Specification

ABS is a modeling language, developed for the modeling, simulation and analysis of distributed systems. ABS models are executable, yet it is not a programming language in this context: its foremost use is to mirror the structure of the target system, not its computational results. Its conceptual closeness to programming languages, however, allows us to demonstrate the use of requirements traces more succinctly. Most constructs of ABS are standard and its syntax is based on Java, with additional statements for concurrency. We introduce the data, communication and time models of ABS.

Data and Communication Model. ABS models data and behavior in two sublanguages. Data, and operations on the data, is modeled in a functional sublanguage based on abstract data types (ADTs). As an example, the following defines an ADT modeling the state of a (logical) signal:

```
data State = GO | HALT | SLOW | INVALID;
```

Behavior and communication is modeled in an object-oriented language on top of the functional sublanguage. The object model uses classes and interfaces and is based on Java, but all fields are object-private. Additionally, traits may be used to add methods to a class. The following class models a Zs10 auxiliary signal (end of speed limitation).

```
1 [Concept:"Zs10"] class Zs10(Edge track, String name) {
2   uses NoSig adds NoBack adds Nameable;
3   List<Trans> trigFront(Train t, Edge e){
4     Information info = NoInfo;
5     if( e == track )
6       info = AreaEnd(-1, False, null);
7     return list[Pass(info)];
8   }
9 }
```

The class Zs10 has two fields (track and name) and uses three traits (NoSig, NoBack, Nameable). It has one additional method, that transmits AreaEnd if the train passes the Zs10 auxiliary signal from the direction where it is visible. The types Trans for transmissions and Information for transmitted information are ADTs.

Simulation, Time and Model API. FormbaR uses Timed ABS [4], which extends ABS with explicit operations on time. The statement **await** duration(x,y) suspends the current process for at least x to y simulation time steps. At runtime, the shortest possible time is chosen. In FormbaR, a simulation time step corresponds to one second.

ABS can be compiled into, among other languages, Erlang and then be executed. The compiled executable contains a runtime environment in Erlang, that implements the above concurrency model and keeps track of the symbolic time — the global symbolic clock is only advanced if every object is waiting for time to pass. The clock is then advanced by the minimal time that unlocks some object.

3.2 The FormbaR model of Railway Operations

The FormbaR model is centered around the notion of *points of information flow*, which are the basic infrastructure of the formal model and are not specified by the rulebooks.

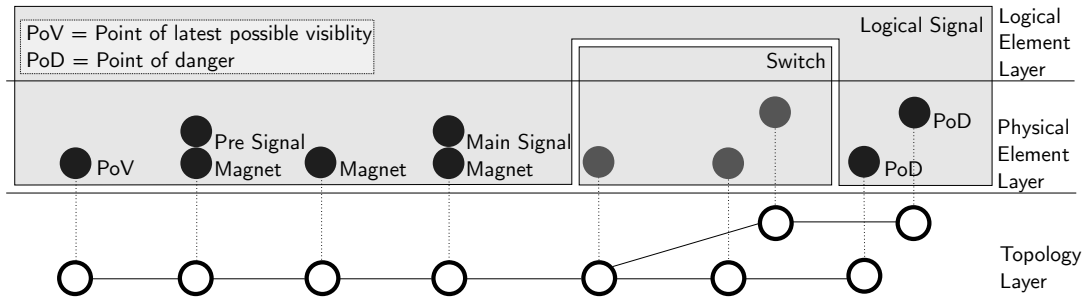


Figure 1: The lower three layers of a station entry, with a logical entry signal and a switch. (From [19])

Definition 1. A Point of Information Flow (*PIF*) is an object at a fixed position on a track, where one of the following applies:

- It is an infrastructure element transmitting information to trains (e.g., balises)
- It is in some critical distance to an infrastructure element (e.g., the point where the presignal is seen at the latest)
- It is an infrastructure element, which receives information from trains

PIFs allow one to discretize the infrastructure from an *operational* perspective, as the physical behavior of the train can be interpolated between two PIFs. FormbaR is also able to handle state changes of trains between two PIFs, e.g., because of orders or if the train comes to a halt before a signal. However, for the most time during simulation, the train behaviors must only be adjusted at PIFs and simulation is thus less time-consuming.

3.3 Infrastructure

The infrastructure model is based on a graph, where the nodes form the base for a four-layer model of the infrastructure. At each node of the graph, PIFs may exist and the edge has the length of the track in between two nodes.

This topological graph forms layer 1 and contains all information about physical distances. Layer 2 is a set of physical elements assigned to a node, e.g., presignals, main signals, etc. Furthermore, layer 2 is the view of the train driver on the infrastructure, who has to react to these elements. Layer 3 consists of *logical elements*. A logical element is a set of physical elements, which share state or interface to the interlocking system. This layer is the view of the train dispatcher on the infrastructure, as it is not possible to, e.g., change the state of the main signal without changing the state of the presignal. A physical element may be assigned to multiple logical elements (e.g., a presignal may belong to multiple logical signals) or none (e.g., a buffer stop).

Fig. 1 shows the entry to a train station. The black elements constitute one logical signal, the entry signal of the station: The point of visibility, where the presignal is seen at the latest, the presignal itself, the main signal, three magnets of the automatic train protection system PZB and two point of danger which are covered by the signal (e.g., axle counters). VisualisierbaR has basic CAD features to create and manipulate infrastructure.

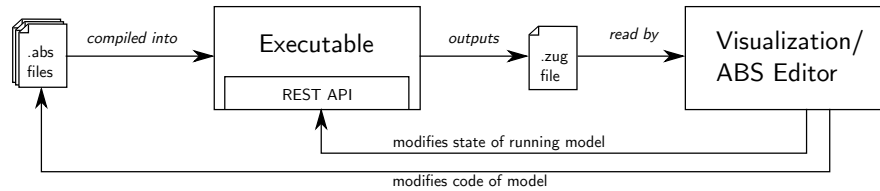


Figure 2: Overview over the components in the implementation

3.4 Communication of Stations and Trains

Stations manage a set of logical elements and communicate only with their logical elements and adjacent stations. Trains only communicate with the lowest layer of the infrastructure, the graph. The nodes relay all the transmissions from the physical elements on them to the train. Trains and stations communicate directly only via orders and only in case of faults, not during normal operations.

4 Implementation and Interaction

In the following sections we describe *VisualisierbaR*, an IDE that implements the principles of the previous section and illustrates prototyping of railway operation procedures. The interface has three components: an ABS IDE for the model, a PDF viewer for the rulebooks and a visualization. *VisualisierbaR* is designed for a multi-monitor working place, due to the space requirements of the visualization of the simulation. First, we describe the architecture of the implementation and the possibilities to interact with the model in *VisualisierbaR*.

4.1 Implementation

To start the simulation, the following workflow is implemented: The ABS compiler first generates Erlang code and then compiles Erlang to an executable file. The executable outputs a `.zug` file. This file contains a list of all *FormbaR* events that are needed for the visualization and acts as the interface between visualization and the model. It also allows to replay an execution without having the ABS code. The format is a list of events, e.g., the following is a main signal with the internal Erlang identity `TrackElements.HauptSignalImpl:<0.581.0>` changing its state to “Go”(Fahrt) at 459/8s.

```
CH;TrackElements.HauptSignalImpl:<0.581.0>;FAHRT;459/8
```

Additionally, the executable contains a web server running a RESTful API [32] to query the object state, call methods from the outside and to limit the clock. By limiting the clock, it is possible to start the executable, read (and visualize) the output up to a certain time step and then interact with the model by calling methods via the RESTful API. Afterwards, one may resume the execution for some fixed time span by increasing the limit of the clock. *VisualisierbaR* requires that the ABS project consisting from `*.abs` files and a scenario are selected. It automatically compiles the model and starts the executable. We use two kinds of interactions from *VisualisierbaR*, which are illustrated by the two cycles in Fig. 2.

4.2 Interaction with Running Model

Interaction with the running model is the inner cycle in Fig. 2. As described, the web server allows us to interact with an already running model by invoking exposed methods. In the visualization, each physical

element displays the interactions. An interaction is a method which is exposed by an `[HTTPCallable]` annotation in the interface of the class.

The RESTful API is used to read the list of exposed methods and allows to easily add methods as new interactions (at compile time). When the simulation is halted, these methods may be called to change the current state and alter the following steps in the simulation. In principle, the model must not be halted for the interactions, however `FormbaR` does not adjust simulation and wall time, to interact on a precise point in time, one thus needs to simulate up to this point, interact, and continue simulation. These interactions are available for trains and physical elements, which may however propagate the interaction to their currently responsible train station, resp. logical element.

4.3 Interaction with ABS Code

Interaction with the ABS code is the outer cycle in Fig. 2. `VisualisierbaR` contains an IDE for ABS, which allows to run the simulation, visualize it and then directly modify the ABS model. This allows visual *debugging* of railway operations, where certain situations can be modeled as the infrastructure and then directly checked whether the new (or modified) procedure behaves as intended. After modifying the code, the model is recompiled and re-executed.

To support this interaction, it is necessary to provide a way to link the visualization with two parts of the ABS code: First, the infrastructure that is currently active and second, the part of the procedure that is executed. This connection falls under contextualization, which does not only provide the context of rulebooks for the ABS model, but also the context of the ABS model for the visualization. When modifying the infrastructure, the complete initialization block of the scenario is generated anew.

5 Using VisualisierbaR for Validation

In this section we describe the use of `VisualisierbaR` for validation. First, we describe the visualization.

5.1 Visualization

Modes. `VisualisierbaR` can be started in three modes. If `VisualisierbaR` is started in *Visualize/Edit* mode, then the code of the ABS model and the visualization of the simulation are shown. The scenario can be edited, the simulation can be rerun and the contextual documents can be displayed. If `VisualisierbaR` is started in *Interactive* mode, then the visualization of the simulation is shown. The simulation, however, is not run yet. Instead the visualization offers the opportunity to either interact with the halted simulation (e.g., to inject faults by breaking signals or to give orders to a train) or decide to continue for a certain time frame. The ABS model and contextual documents can be displayed, but the scenario can not be edited. In these two modes, the root directory of the ABS model and the chosen scenario have to be selected. Finally, the *Replay* mode allows to visualize `.zug` files without ABS model.

A detail of the visualization of railway operations is shown in Fig. 3. This window offers, beyond visualization itself, the ability to interact with the model and can be used as an editor, that offers standard computer aided design (CAD) features: adding, editing, copying and deleting nodes, edges and physical elements. It is also possible to manage logical elements. If the ABS model is changed, the model is recompiled and the visualization shows the rerun scenario.

Window A.2 shows the details of a train or element, if one is selected. For physical elements, properties such as position and its logical element are displayed. For trains, additionally to the properties,

the $v-t$ and other graphs are shown. In interactive mode, A.2 also contains the possible interactions with the selected element or train. Optionally, a window with the list of FormbaR-events can be opened. There are 3 possibilities to advance the simulation:

- by manually selecting a point in time or event,
- by traversing the list of events automatically at a fixed rate events/second,
- by traversing the list of events automatically at a fixed speed. In this case the position of trains between two nodes is interpolated.

In any case it is possible to go back in time and review a part of the simulation. It is however only possible to interact with the current (i.e., newest) state.

Interaction is realized through a RESTful API [32] embedded in the ABS executable that allows to call methods from the outside and to limit the clock. The executable outputs *.zug files, which are read by the visualization. Reading these files allows one to replay an execution without needing the ABS code, which simplifies sharing.

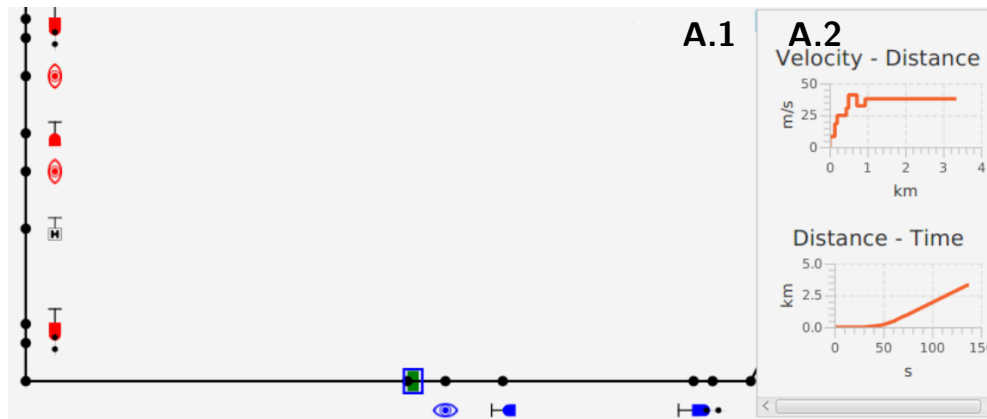


Figure 3: Window A: Visualization. The green train is about to enter the station on the bottom right, the entry signal shows “Go”. Window A.2 shows the $v-t$ diagram and other information about the train.

5.2 Requirements Traces

The links between the components are illustrated in Fig. 4:

Documents to ABS By selecting a part of the rulebook that is linked from the code, the linking code, i.e. the annotated element, can be highlighted.

ABS to Visualization Objects are highlighted in the visualization, if their object creation site (their **new** expression) is selected in the ABS editor.

Visualization to Documents The visualization allows us to show explaining text for the simulation. These messages may contain the annotations to the rulebooks.

Visualization to ABS The object creation sites of elements selected in the visualization are highlighted in the editor.

ABS to Documents The ABS code allows us to directly link to the rulebooks from the code via annotations. The relevant part of the rulebook is then highlighted.

The first two links implement forward tracing, the others implement backward tracing. The links between ABS and documents support n - m relations – if a part of the document is modeled in several points of the code, a window allows to select one. The following sections illustrate the trace links in more detail.



Figure 4: Structure of trace links in VisualisierbaR.

Visualization. The visualization provides context in two ways: (1) when selecting an element, window A highlights the statement responsible for the creation of this element. This link is used to trace an element in the visualization to a point in the model. (2) Additionally, special MSG-events in the *.zug files are supported: These events are shown as pop-ups and visualize non-visible state changes (e.g., message exchange between train and station). An MSG-event may contain annotations to link to contextual documents. This link traces a point in the execution of a model to a rulebook/requirement.

ABS Model. The ABS model is shown in window B in Fig. 5. ABS is a modeling language with a Java-style syntax and is presented similar to mainstream programming languages in the IDE.

In window B a file browser shows the different code files (B.1), while the main part (B.2) allows one to view and manipulate a single ABS file. B.2 offers standard IDE features like syntax highlighting or jumping to definitions.

Specific to VisualisierbaR are two features that provide contextualization:

- I In the scenario setup in file Run.abs, each created element can be clicked on and is then highlighted in the visualization (window A). This link is used to trace a part of the model to the visualization.
- II Each class and method can be annotated with [Document:Y], where Y is a rulebook identifier (e.g., “Ril. 408.0615”) the name of a concept or a keyword, (e.g., “Main Signal”). A click on such annotations highlights the document part in the document window (window C) marked with this identifier (in case of [Document:Y] or a window that lists all document parts responsible for the keyword (in case of [Concept:X]). This link is used to trace a part of the model to the rulebook/requirement. If a concept is linked to multiple parts of the rulebooks, the user can select one of them. The mapping between annotated concept and rulebook sections are manually managed in a .csv file that allows n - m relations and is a variant of a requirement matrix between code and rulebooks.

The IDE offers a way to modify the code and recompile. After recompilation, window B.2 is split into two panes, where the left shows the current code and the right the code of the model before compilation to simplify tracking of changes.

Documents. Window C is a PDF viewer which highlights parts of the document if referenced from the other components. It provides context in two ways. When a part of the document is clicked on and this part of the document is referenced from the model, a list of all annotation referring to it is shown. This list then highlights the annotation in window B.2. This link is used to trace a requirement to the model.

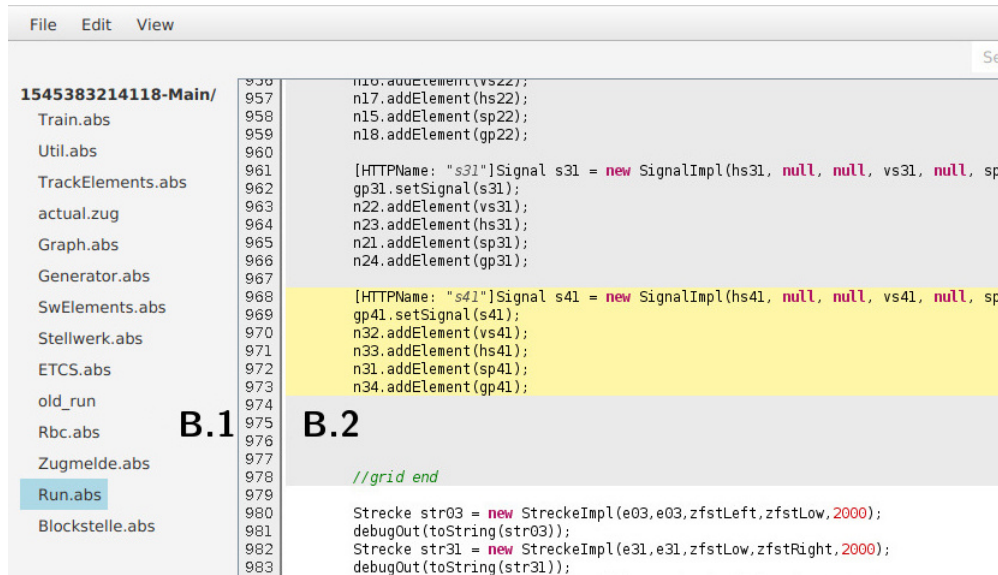


Figure 5: Excerpt of Window B: ABS editor. The different backgrounds visualize infrastructure selected in window A.

Fig. 6 shows the PDF viewer. The bars on the left mark the referenced parts of the documents. The window on the right is displayed when a part of the document is clicked on and lists all references in the ABS code to it. A list of all references can be shown in the ABS editor.

6 Validation Case Studies for ATO and Prototyping

We give two examples how VisualisierbaR can be used in the workflow of rulebook authors. The first example is from the on-going development of new procedures for autonomous train operations [33], where VisualisierbaR was applied to check that the new rules correctly interact with the old rules for non-autonomous train operations. The second example models the change of a rule. Following real world changes [29], we model the effects on delays, depending on whether the first train after a fault has occurred drives on sight or not.

6.1 Validating ATO Procedures

We give an example where VisualisierbaR is used in the current development of a system to handle faults during autonomous train operations (ATO) with grade of autonomy (GoA) 4 [33] to analyze how the additional checks needed for ATO interact with the operational rules. In this case, the requirements are the developed procedures for ATO GoA 4 and their correct interactions with the original rules.

The investigated scenario was an obstacle in front of a signal, where the autonomous train adheres to the rules specific to GoA 4 (detecting the obstacle and waiting for it to disappear) as well as to the rules for general operations (responding to the signal). The model has to realize both rulebooks.

The decisions necessary for ATO are annotated with links to the ATO documentation and the already existing model for general operations with links to the rulebooks. To connect the model with the visualization, we added messages and used the following scenario: A train is driving towards a signal and an

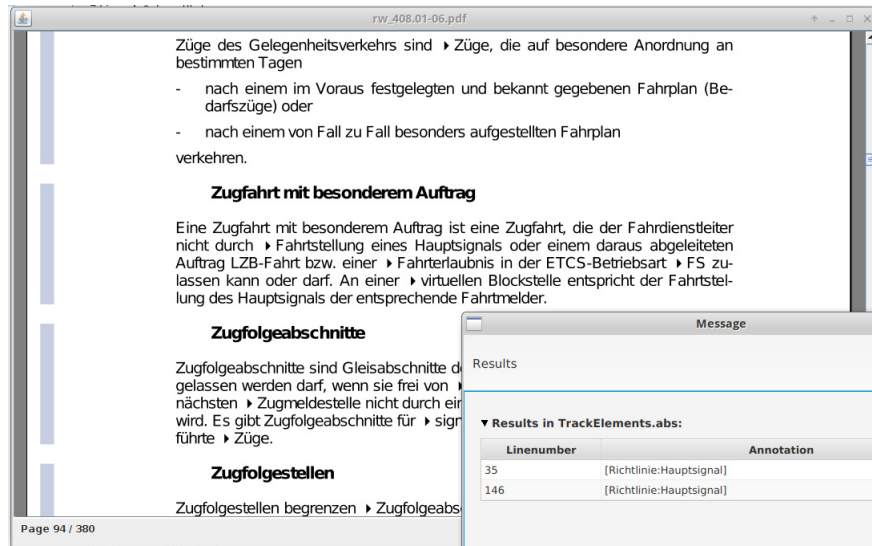


Figure 6: Window C: PDF viewer

obstacle, e.g., a cow, is directly before the signal. The signal signals “Halt”. ATO GoA 4 adds the rule that a train halts before any detected obstacle.

Trace links are able to enhance validation through simulation by tracing certain execution steps back to the original procedures. Simulating the scenario shows that the train detects the cow and halts until the cow leaves the track, even if the signal switches to “Go”. Similarly, if the cow leaves and the signal is still signaling “Halt”, the train waits. At each point, the simulation displays the decisions of the ATO algorithms, e.g., if the obstacle is not detected anymore it is displayed why the system decided to halt.

This allows us to check that rules for ATO GoA 4 do not override rules for normal train driving or otherwise interfere with them. From a development process view, the simulation itself is a behavioral test that links its output with the requirements and the annotations are links for requirements traces.

6.2 Prototyping Rule Changes

To reason about the effects of a proposed rule change, *Visualisierbar* was first used to model a variant of the infrastructure in the west branch of the Frankfurt City Tunnel. This branch has a length of 4.7km and is the main part of the Rhein-Main S-Bahn – eight lines pass through it, with intervals below five minutes. Its high usage makes it representative of how rules affect operations in networks with high occupancy rate and short distances between signals. We only model one direction (from Hauptbahnhof to Südbahnhof) without the branch-off point Schlachthof, which is sufficient for the analyzed rule change.

On the infrastructure two trains with a 5 minutes interval are simulated, both with a maximal velocity of 60km/h. We model the following scenario: the main signal on the track between Ostendstraße and Lokalbahn³ has a fault that is local to this signal (e.g., a broken bulb). To sustain operations, the train dispatcher gives an order to depart (equivalent to a ZsI auxiliary signal) nonetheless.

Old rule. The train dispatcher must not order to drive on sight, thus the first train can still drive the full 60km/h. In this case the second train, which departs at $t = 300s$, arrives in the final station at $t = 1027s$.

³This block was chosen because it has the shortest sight distance and requires the slowest speeds when driving on sight.

New rule. Now, the train must first drive on sight, which is walking speed in tunnels (6 km/h). In this case the second train (which is not effected by this and may drive 60km/h) arrives at the final station at $t = 1487s$.

The delay, over 7 minutes⁴ is specific to this infrastructure and time table, yet gives an estimate which helps the developers to assess the impact of a rule change. Another example to examine rule changes with FormbaR is discussed in [19]. VisualisierbaR is an improvement over the previous ad-hoc visualization, as it allows to assess the relevant information faster by showing the $v-t$ graph.

This application of VisualisierbaR was presented to the rulebook authors of DB Netz responsible for this rule, who deemed the visualization and the trace links as helpful.

7 Conclusion and Future Research

We presented VisualisierbaR and have shown how it can be integrated into the processes for developing railway operation procedures. It illustrates how model validation can be supported by integrating requirement traces and how these traces increase the usefulness of tests and visualization. It extends our previous work on modeling these procedures by giving an interface that does not require the user to learn ABS to use the model, but gives him the possibility for deeper manipulation with ABS if necessary. VisualisierbaR extends the use cases of formal tools in railway engineering from support for implementation and planning [9, 13] to the development of new procedures by using an ABS model to prototype ATO procedures. Beyond railway engineering, we addressed the challenge to use technical documents as requirements for validation, which are not designed to be used as requirements and are not modifiable by the modeler.

VisualisierbaR is available under formbar.raillab.de/visbar with limited annotations, as most rulebooks and the rules for the above ATO case study are not public. A video demonstrating the usage of VisualisierbaR is available under <https://figshare.com/s/71f1c2e7252bfd032f57>.

It is often observed that formal models offer a benefit for the designer, even without analyzing formal properties, as it forces to clarify all ambiguities. Thus, formal modeling languages must not only be easy to analyze, but also easy to validate and easy to integrate into existing development processes. Yet, validation of formal system models and its place in development processes remains a challenging domain. For future work, we are not only interested in the integration of validation of formal models into a development process, but the development process of formal models and digital twins itself. In particular, we are interested in the following:

- Requirement trace generation for formal modeling.
- Integration of conceptual modeling [28] into formal model validation by connecting requirements and formal model with a domain ontology⁵.

The overarching questions are (1) how to design formal modeling languages (and IDEs for them) which are not only easily usable and analyzable, but also easy to validate and (2) how to use traceability in verified formal models for certification. We propose that automatic generation of traces would not only vastly simplify validation, but also be a step towards a wider acceptance of formal proofs for certification.

⁴This is longer than the delay caused purely by waiting (3 minutes) for the first train to arrive, but still realistic. The additional 4 minutes are caused by a non-optimal train dispatching in our model. However, the duties of the train dispatcher to document the situation and give written orders in case of faults accounts for this.

⁵Conceptual modeling faces similar problems with validation, but is more abstract in the information it captures and relies more on implicit knowledge, than specifications, designs or a concrete existing system.

Related Work Luteberget et al. [24] use traces to link errors raised during verification to the responsible part of the model and the original document. These traces roughly resemble the annotations in messages generated by VisualisierbaR during simulation, but are not used to validate the model itself. Ferrari et al. [11] investigated the requirements of railway engineering projects from a natural language processing perspective. Concerning the connection of conceptual and formal modeling, Kharlamov et al. [21] propose to use ontologies to develop digital twins, but not for validation.

Fischer and Dghaym [12] use acceptance tests to validate a formal model of Hybrid ETCS L3 segments. Contrary to requirement traces and interactive visualization their approach requires *fully formalized* test cases of observable behavior of the model. This approach is not only subsumed by simulation – as discussed, it also does not lower the cognitive burden of validation, as these test cases are a *formal behavioral model themselves*.

Integration of multiple aspects is common for programming languages in mainstream IDEs, but development environments based on formal methods focus mostly only on the formal model and its verification, e.g., by an interface to the proof system. E.g., the B-OVADO [13] tool for the PERF [3] approach, offers a toolbox for data validation tasks that integrates B as a language to specify data. The Sphinx tool [25], which integrates verification and modeling tools for model-based engineering of hybrid systems, is the only approach that uses formal methods for coordinating multiple components for development. It also provides a way to connect to documentation in a special UML profile and is specific to differential dynamic logic. Interaction [22] and visualization [23] for validation of B-models was investigated by Ladenberger et al. (Interactive) visualization of formal models is also supported for Circus [2] and PVS [34] models.

Future Work Beyond further research in the connection to requirements engineering sketched above, we plan (1) to enable statistical analyses, such as expected lost units [20] after a rule change, in a representative network and (2) to integrate our verification approach [17] to use it for certifications. We also plan to investigate how, analogous to Domain Specific Languages, Domain Specific IDEs, can be used to integrate formal methods into other domains.

Acknowledgments This work is supported by the FormbaR project, part of AG Signalling/DB RailLab. We thank Heike Villioth-Ebert, Armin Krieger, Matthias Kopitzki and Bilal Üyümez for their feedback.

References

- [1] Yaman Barlas (1996): *Formal Aspects of Model Validity and Validation in System Dynamics*. *System Dynamics Review - SYST DYNAM REV* 12, doi:10.1002/(SICI)1099-1727(199623)12:3<183::AID-SDR103>3.0.CO;2-4.
- [2] S. L. M. Barrocas & Marcel Oliveira (2012): *JCircus 2.0: an Extension of an Automatic Translator from Circus to Java*. In Peter H. Welch, Frederick R. M. Barnes, Kevin Chalmers, Jan Bækgaard Pedersen & Adam T. Sampson, editors: *34th Communicating Process Architectures, CPA 2012, organised under the auspices of WoTUG*, Open Channel Publishing Ltd., pp. 15–36. Available at http://wotug.org/paperdb/show_paper.php?f=1&num=662.
- [3] Nazim Benaïssa, David Bonvoisin, Abderrahmane Feliachi & Julien Ordioni (2016): *The PERF Approach for Formal Verification*. In Thierry Lecomte, Ralf Pinger & Alexander Romanovsky, editors: *RSSRail 2016 proc.*, Springer International Publishing, Cham, pp. 203–214, doi:10.1007/978-3-319-33951-1_15.

- [4] Joakim Bjørk, Frank S. de Boer, Einar Broch Johnsen, Rudolf Schlatte & Silvia Lizeth Tapia Tarifa (2013): *User-defined schedulers for real-time concurrent objects*. *ISSE* 9(1), pp. 29–43, doi:10.1007/s11334-012-0184-5.
- [5] Manfred Broy, Klaus Havelund, Rahul Kumar & Bernhard Steffen (2018): *Towards a Unified View of Modeling and Programming (Track Introduction)*. In Tiziana Margaria & Bernhard Steffen, editors: *ISoLA*, Springer, pp. 3–21, doi:10.1007/978-3-030-03418-4_1.
- [6] CENELEC (2011): *DIN EN 50128:2011, Railway applications – Communication, Signalling and Processing Signals*.
- [7] DB Netz AG, Frankfurt, Germany (2017): *Richtlinie 408, Fahrdienstvorschrift*.
- [8] DB Netz AG, Frankfurt, Germany (2017): *Richtlinie 819, LST-Anlagen planen*.
- [9] Stefan Dillmann & Reiner Hähnle (2019): *Automated Planning of ETCS Tracks*. In: *RSSRail, LNCS 11495*, Springer, pp. 79–90, doi:10.1007/978-3-030-18744-6_5.
- [10] Eisenbahnbundesamt (Federal Railway Authority) (2017): *Eisenbahn-Bau- und Betriebsordnung*. April 2017: <https://www.gesetze-im-internet.de/ebo/index.html>.
- [11] Alessio Ferrari, Gloria Gori, Benedetta Rosadini, Iacopo Trotta, Stefano Bacherini, Alessandro Fantechi & Stefania Gnesi (2018): *Detecting requirements defects with NLP patterns: an industrial experience in the railway domain*. *Empirical Software Engineering* 23(6), pp. 3684–3733, doi:10.1007/s10664-018-9596-7.
- [12] Tomas Fischer & Dana Dghaym (2019): *Formal Model Validation Through Acceptance Tests*. In: *RSSRail 2019, LNCS 11495*, Springer, pp. 159–169, doi:10.1007/978-3-030-18744-6_10.
- [13] Manel Fredj, Sven Leger, Abderrahmane Feliachi & Julien Ordioni (2017): *OVADO - Enhancing Data Validation for Safety-Critical Railway Systems*. In Alessandro Fantechi, Thierry Lecomte & Alexander B. Romanovsky, editors: *RSSRail 2017 proc., LNCS 10598*, Springer, pp. 87–98, doi:10.1007/978-3-319-68499-4_6.
- [14] Cláudio Gomes, Casper Thule, David Broman, Peter Gorm Larsen & Hans Vangheluwe (2018): *Co-Simulation: A Survey*. *ACM Comput. Surv.* 51(3), pp. 49:1–49:33, doi:10.1145/3179993.
- [15] IEEE (1998): *IEEE Guide for Software Requirements Specifications. IEEE Std 830-1998*.
- [16] Einar Broch Johnsen, Reiner Hähnle, Jan Schäfer, Rudolf Schlatte & Martin Steffen (2010): *ABS: A Core Language for Abstract Behavioral Specification*. In: *FMCO, LNCS 6957*, Springer, doi:10.1007/978-3-642-25271-6_8.
- [17] Eduard Kamburjan & Reiner Hähnle (2017): *Deductive Verification of Railway Operations*. In: *RSSRail 2017, LNCS 10598*, Springer, pp. 131–147, doi:10.1007/978-3-319-68499-4_9.
- [18] Eduard Kamburjan & Reiner Hähnle (2018): *Prototyping Formal System Models with Active Objects*. In: *Interaction and Concurrency Experience, EPTCS 279*, Open Publishing Association, pp. 52–67, doi:10.4204/EPTCS.279.7.
- [19] Eduard Kamburjan, Reiner Hähnle & Sebastian Schön (2018): *Formal modeling and analysis of railway operations with active objects*. *Science of Computer Programming* 166, pp. 167 – 193, doi:10.1016/j.scico.2018.07.001.
- [20] Florian Rudolf Kämmerer (2017): *Entwicklung eines Kennzahlensystems für Effektivität des Bahnbetriebs bei Abweichungen vom Regelbetrieb*. Master’s thesis, Technische Universität Darmstadt.
- [21] E. Kharlamov, F. Martin-Recuerda, B. Perry, D. Cameron, R. Fjellheim & A. Waaler (2018): *Towards Semantically Enhanced Digital Twins*. In: *2018 IEEE International Conference on Big Data*, pp. 4189–4193, doi:10.1109/BigData.2018.8622503.
- [22] Lukas Ladenberger (2017): *Rapid Creation of Interactive Formal Prototypes for Validating Safety-Critical Systems*. Ph.D. thesis, University of Düsseldorf, Germany.
- [23] Lukas Ladenberger, Jens Bendisposto & Michael Leuschel (2009): *Visualising Event-B Models with B-Motion Studio*. In María Alpuente, Byron Cook & Christophe Joubert, editors: *Formal Methods for In-*

- dustrial Critical Systems*, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 202–204, doi:10.1007/978-3-642-04570-7_17.
- [24] Bjørnar Luteberget, John J. Camilleri, Christian Johansen & Gerardo Schneider (2017): *Participatory Verification of Railway Infrastructure by Representing Regulations in RailCNL*. In Alessandro Cimatti & Marjan Sirjani, editors: *Software Engineering and Formal Methods - 15th International Conference, SEFM 2017, Trento, Italy, September 4-8, 2017, Proceedings, LNCS 10469*, Springer, pp. 87–103, doi:10.1007/978-3-319-66197-1_6.
- [25] Stefan Mitsch, Grant Olney Passmore & André Platzer (2014): *Collaborative Verification-Driven Engineering of Hybrid Systems*. *Mathematics in Computer Science* 8(1), pp. 71–97, doi:10.1007/s11786-014-0176-y.
- [26] Chris Newcombe (2014): *Why Amazon Chose TLA +*. In Yamine Ait Ameer & Klaus-Dieter Schewe, editors: *Abstract State Machines, Alloy, B, TLA, VDM, and Z*, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 25–39, doi:10.1007/978-3-662-43652-3_3.
- [27] Dan North (2006): *Introducing BDD*. [Http://dannorth.net/introducing-bdd/](http://dannorth.net/introducing-bdd/).
- [28] Antoni Olivé (2007): *Conceptual Modeling of Information Systems*. Springer-Verlag, Berlin, Heidelberg.
- [29] Jrn Pachl (2018): *Das Ersatzsignal – ein deutscher Sonderweg? Deine Bahn* 3. In German.
- [30] Roland Rosen, Georg von Wichert, George Lo & Kurt D. Bettenhausen (2015): *About The Importance of Autonomy and Digital Twins for the Future of Manufacturing*. *IFAC-PapersOnLine* 48(3), pp. 567 – 572, doi:10.1016/j.ifacol.2015.06.141.
- [31] RTCA Inc, EUROCAE (2012): *DO-178C*.
- [32] Rudolf Schlatte, Einar Broch Johnsen, Jacopo Mauro, Silvia Lizeth Tapia Tarifa & Ingrid Chieh Yu (2018): *Release the Beasts: When Formal Methods Meet Real World Data*, pp. 107–121. Springer International Publishing, Cham, doi:10.1007/978-3-319-90089-6_8.
- [33] Bilal Üyümez (2018): *Modellierung des Steuerungsprozesses der Rückfallebenen als Grundlage für die Automatisierung*. *Eisenbahntechnische Rundschau*. In German.
- [34] Nathaniel Watson, Steve Reeves & Paolo Masci (2018): *Integrating User Design and Formal Models within PVSio-Web*. In Paolo Masci, Rosemary Monahan & Virgile Prevosto, editors: *Proceedings 4th Workshop on Formal Integrated Development Environment, F-IDE@FLoC 2018, Oxford, England, 14 July 2018., EPTCS 284*, pp. 95–104, doi:10.4204/EPTCS.284.8.