360.revista de alta velocidad
número 5 - junio - 2018. Pág 93 - 103

Test and Certification of Railway automation and digitalization approaches (Rail 4.0)

Meyer zu Hörste, Michael
Asbach, Lennart
Hardi, Hungar
Lemmer, Karsten

German Aerospace Centre (Deutsches Zentrum für- Luft- und Raumfahrt – DLR)[1]

Abstract

The current industry mega-trend of digitalization –sometimes called "Rail 4.0", too - will lead to a major change in railway automation. The automation of railway operations will increase significantly in the coming years and will help to meet the challenges of the railways. Which of the approaches discussed currently will come into operation is depending on technical, operational and legal requirements. Many projects in Germany and Europe are currently dealing with the automation of railway operations. Therefore pilot projects can be expected in the near future. Improved concepts for railway operation e.g. the level 3 of the European Train Control System (ETCS) using moving block, on-board integrity supervision or virtual train sets will result in even higher requirements to the accuracy and reliability of the localization. Hence some major issues are still to be solved. It is among others: Precise and reliable localization, e.g. based on sensor data fusion based on Global Navigation Satellite Systems (GNSS), reliable communication technologies robust against obsolescence, obstacle detection systems fulfilling civil and criminal law as well as cost requirements and cyber security. The contribution will focus on the last aspect: Tests need to be developed to ensure the safe and reliable behaviour of automated trains under normal and disturbed conditions. In current practice, highly automated, mechanically evaluated tests need strictly formal test cases which are unambiguously defined. If these preconditions are not met, the automation effort is high, so that it is often better to only aim for a partial solution. To get test cases of high quality, the choice of tools used for test defining them is crucial: The tools must restrict the engineer to prevent unclear definitions being introduced. They must enable the domain expert to write test cases which can readily be translated for use in the test bench.

Keywords: Train Control, Testing, Conformity, ERTMS, ETCS, ATO

1 *Meyer zu Hörste, Michael. Institute of Transportation Systems. Email: Michael.MeyerzuHoerste@dlr.de. (Corresponding author)*
Asbach, Lennart. Institute of Transportation Systems. Email: Lennart.Asbach@dlr.de
Hardi Hungar. Institute of Transportation Systems. Email: Hardi.Hungar@dlr.de
Lemmer, Karsten. Transport and Energy. Email: Karsten.Lemmer@dlr.de

1. Introduction

Today functional testing becomes more and more important, as complex train control systems (e.g. ETCS) offer a lot of functionalities but specifications, written in natural language. The tests are necessary to reach real interoperability but also offer a chance to reduce the field tests. DLRs research aims to reduce time and costs of test runs and increase the scope of the tests to make the final European admission as easy as possible.

Main focus of the research is testing for ETCS and the standardized interfaces for field components and interlocking (e.g. Eulynx, DB NeuPro). In the field of ETCS especially the onboard (OBU) and radio-block centre communication is focused. Due to the increasing demand for ATO this gets more and more into the focus of DLRs research as well.

With its laboratory RailSiTe. DLR is researching tomorrows testing methods in the railway domain. The paper will show the current approach of conformity testing in a test bench for the entire system. It includes interfaces for OBU, RBC, Interlocking and field elements to allow a comprehensive test execution and evaluation. By now the test bench is able to connect to almost every RBC in the world using internet protocols and special tools for GSM-R adaption.

The goal of the research work on OBU testing is attained when the following scenario is reality: All ERTMS tracks are virtually rebuild in a test bench. All European operational scenarios have been created and formalized. Assuming this, there cannot be any requirement in the system specification, which is not tested in one of the operational scenarios. If there is any, it can be removed from the specification, because it is obviously not needed. By testing every new onboard system on the entire European network virtually, in all operational situations, interoperability is proven and inherits conformity.

Todays testing process of conformity tests and interoperability tests offers high potential for implementation. A first step has been made by formalizing some selected tracks in the European network. By creating an RBC-Proxy, DLRs laboratory is able to behave exactly like certain RBCs, which allows testing of tracks without a real RBC connection. This is important to accelerate the process massively.

The expected result is the reduction of field and manual parts of the laboratory tests to a minimum. At least on the functional layer the field tests can be replaced by laboratory tests more or less easily. This contribution shows first ideas to reuse existing tests for testing ATO systems.

Right now there are already many ATO systems, or at least driverless systems, available and in service. The real challenge will be the implementation of those systems on main-line tracks. Having a look to the current train control systems, on the functional level there is only a very small gap between driver-operated and automatic trains.

The track-train communication is safe and ready for automatic train operation. Thus we can assume that the ATO for main line tracks will be an add-on module for train control systems (red box in figure 1). This includes track-side and on-board systems. This contribution shall focus on the testing of the on-board part, the driver-replacement.

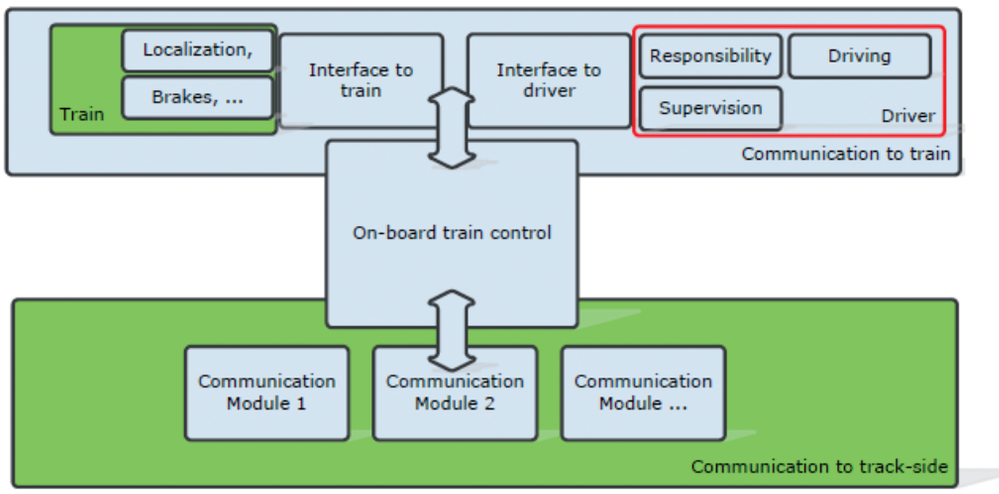

Figure 1: Overview of current setup of on-board train control

Figure 1 shows a basic setup of today s on-board train control. The communication to the track-side is available by many technologies, in case of ETCS one of the communication modules could be the GSM-R channel. The train interface is also already connected to the train control system. Information and commands are exchanged, e.g. braking, doors, pantograph or localization information. In most cases the driver has to control the traction lever according to the information of the train control system. From a technical perspective the main task of the driver is supervision and responsibility for the train. The first part of this contribution will focus the influence of ATO systems to the current testing methodologies.

2. Testing on-board ATO modules

2.1 Changes in testing due to ATO

In the current implementations the on-board conformity tests are running 100% automatically. Since the driver machine interface (DMI) has to be part of the test, because of the current law, it is controlled by a robot. The train interface is controlled by the laboratory. In case of ATO functions of the system-under-test these laboratory modules (robot and train interface) can be replaced by the ATO module. At least if the ATO module is tested together with the on-board train control (in case of ETCS this is called European Vital Computer, EVC) the test could be performed in the same manner but with less effort on the laboratory side. The interesting question is what additional descriptions in the test specification are necessary to ensure the proper testing of the ATO module. Since we assume a black-box test for the ATO module, the first inspection has to be done on the interfaces of the module. Today there are many ideas for these interfaces; one could be the reuse of the interface between the DMI and the EVC, in case of ETCS. As long as there is a radio connection available between the track-side and the onboard, all necessary information will be provided. For example a new movement authority is transmitted to the train control system and the ATO simply has to follow this information. Today it is shown with permitted speed and many more values on the DMI. I.e. for all information, which is available via the current DMI, the functional test specification of ETCS

can be reused. Of course, the evaluation methods have to be adapted, because now not only the train control behaviour has to checked but also the ATO behaviour (train interface unit, driver machine interface etc.). If there are any additional inputs for the ATO-module, maybe cameras

to replace the drivers eyes or diagnostic systems to ensure the proper function of the train, they have to be included by adding new test cases in the test specification. Since this should be relatively easy for all pure digital -interfaces, like diagnostic information of the train, it will be more complex for kind of analogue information like the camera image. If, maybe due to legal restrictions, there is a certain reaction required based on the output of image recognition, this will lead to very complex tests. The challenge is the number of possible inputs. It gets even worse, if state-of-the-art methods like machine learning are used for the image recognition. In the current authorization process the certification of a machine learning systems seems to be impossible. Current research approaches are trying to solve certification issues for machine learning algorithms by using watch-dogs, which assure that the machine cannot leave certain boundaries. But right now there is no efficient methodology found.

Even if there is no approach with artificial intelligence and self-learning algorithms the certification and testing of obstacle detection systems will be challenging. Spot checks are possible, but their results are questionable. The number of possible inputs is simply too high (32*10^12 possibilities for a full HD image with 24bits colour depth), to ensure a proper test coverage. Two solutions are conceivable at the moment. Maybe the easiest approach is to ensure no obstacles by fencing the track completely. If a safe fencing is not productive, another possibility would be the acquisition of real data from real train journeys for testing obstacle detection. I.e. a proper way would be to equip all current trains with cameras and use this material (ideally commented) for testing the obstacle detection systems. By this approach, at least a very real test can be assured and the result is more resilient. This procedure can be used for different sensors and is not limited to video based sensors. The following section will exclude the testing of video based obstacle detection and will focus on functional interfaces.

2.2 Solution Approach

Components and systems for railway applications, especially for safe applications, need to be tested comprehensively before taken into operation. These tests have different aims: they can be used to show that a system fulfils the relevant specification, the foreseen operational profile or safety requirements. All these tests need to be described to be performed in the field or to be formalized to be executed in a lab. Both need a formal definition and description to prove the correctness of the results.

The approach used for the conformity tests for ETCS can be extended for operational and safety lab tests, operational field tests and fits very well for testing ATO-systems, too. It may, as demonstrated in the section on interface conformity for digital track side systems, even applied to partial standardisations. The principle method of the generation of the test sequences can be used for the different types of tests. The optimization criteria as well as the rules for the parameterization differ for the different kinds of tests. If the same approach for the formalisation and parameterization is used, the lab environment can be used for any type of test, with, however, some adaptations to be made to achieve sufficient flexibility.

Test case generation and the test sequence construction profit substantially from the application of formal approaches. This field features a variety of languages, methods and tools. Present-day solutions cover only part of the needs of practice, but show potential to be much more useful if applied in a carefully designed process employing adequate formalisations.

3. Test Generation

3.1 Conformity Test Sequences

The group of eight suppliers of train control systems called UNISIG (Union of European

Signalling Companies) have specified the ETCS by writing the SRS (System Requirements Specification SRS [1]) and produce and deliver ETCS components for different railway undertakings and infrastructure manager like Deutsche Bahn AG (German Railways) in Europe. Before these may come into operation, their conformity with the SRS and their interoperability has to be proven with lab tests as stated in previous section.

The issue 3.1.0 of the conformity test was specified by the Subset-076 Working Group (CEDEX, DLR, INECO, MULTITEL, RINA). This specification includes the Hardware-in-the-loop tests of the ERTMS/ETCS on-board equipment [1], the method of their creation [2] and the method of test [3]. The specification of the reference lab architecture [4] completes the set of specifications.

Some of the UNISIG companies are implementing products or just finalising them. Some test trips (field tests) have been performed successfully on the German pilot line Jueterborg-HalleLeipzig. Currently the last steps of implementation of the tests are performed and the latest version will be published very soon. The test target has been defined, generic test cases have been specified and the method for the generation of the final test sequences has been developed and realised. For the better understanding of the following sections these steps will be discussed shortly in the following.

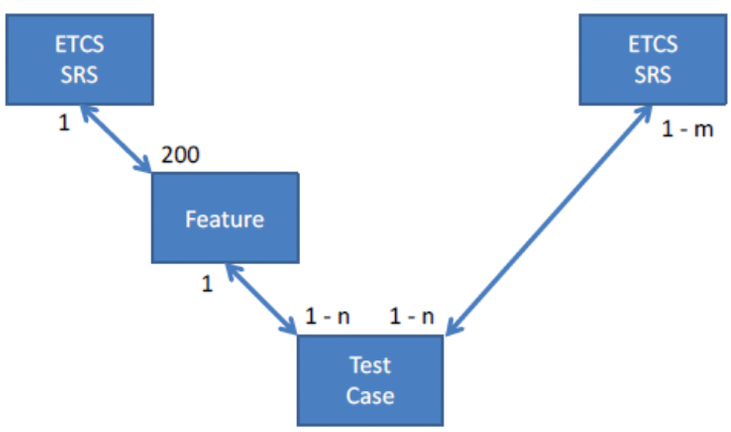

Figure 2: Relation between SRS and Test Sequence

The defined target of test sequences is to test each requirement of the SRS at least once. Firstly, to organise and reduce the amount of requirements of the SRS, more than 200 features have been identified. After this, the required positive and negative test cases have been created for each feature. Totally more than 1700 test cases have been generated. Equivalent test cases for different ETCS modes or levels have been merged to reach a first optimisation and reduction of number of test cases. This means that test cases which are applicable for different mode-level combinations are described as only one test case, if the feature was not dedicated to a specific mode-level combination. Important is the testing of the feature itself. Just for clarification, each ETCS mode is an operational state of the on board equipment and the ETCS level is an overall degree of the usable functionality of ETCS. For the execution of the tests the test cases are concatenated to 775 test sequences, which all start at the powering on of the on-board equipment and end with the no power mode. The test subsequences are concatenated due to their start- and end-conditions to reach a consistent sequence of system states. The test sequences have been optimised to reach the lowest degree of redundancy of testing. Parts of a test are only executed twice or more if they are needed to reach a state which has not been tested yet. Up to the test sequences the specification is completely generic. At this stage the

variables and parameters are filled with values, though some remain to be set dynamically during execution of the sequence. So the test sequences could be understood as operational test trips. The relation from the SRS up to the test sequence is shown in Fig. 2.

Finally the fundamental structure of the test sequence should be clarified. Each test sequence simulates a test trip by stimulating the on-board equipment via the black-box-interfaces. In addition, the SRS-conformant reactions of the on-board equipment are defined in each test sequence. The reactions and the stimulating events are bound to the interface where they should be observed and evaluated or raised. Essentially the test sequences consist of the stimuli and the expected reactions of the on-board equipment. In the test sequence one stimulus or reaction is represented by a test step. Fig. 3 shows the structure of a test sequence.

The 775 test sequences contain up to several hundred test steps and their execution in realtime in the labs need up to several hours. A time rafting testing is not possible due to the fact that the real time behaviour of the ETCS component is tested. As mentioned above the test sequences are implemented in the reference labs. Some of the test sequences have been executed successfully, but the stated problems of duration and unstable inputs on the user interface by the human being show that automation is needed. As soon as an input is missed or incorrect the complete test sequence must be repeated.

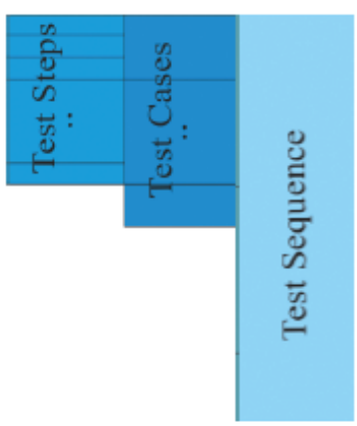

Figure 3: Symbolic structure of a test sequence for conformity testing

The tests defined by this method are documented in the ETCS subset 076. These are used to proof the conformity of the constituent European Vital Computer (EVC) which is the core of the on-board unit.

3.2 Operational Test Sequences

The conformity test sequences which have been discussed in the previous section fulfil the purpose to show that an application is realising the specification sufficiently complete. They do not claim to be operationally reasonable. Thus, a railway undertaking tendering ERTMS/ETCS systems need to check whether these fulfil their operational requirements. These tests are a separate set of test sequences at the moment. They need to be defined by a similar methodical approach as shown above, but they have need to fulfil more requirements: The test sequences must represent the most typical or important scenarios of the operation of the railway. They need to show the fulfilment of the European requirements as well as the national add-ons.

The approach is to use the same test cases for the operational test sequences as well. Some specific test steps and test cases are added to represent operational aspects which are not

represented in the technical tests. The method for the generation of the test sequences is used, too. So the test cases consist out of technical and operational test steps. The test cases are concatenated to a realistic test sequence. This operational test sequence is formalised and filled with parameters according to the same rules as the technical test sequences.

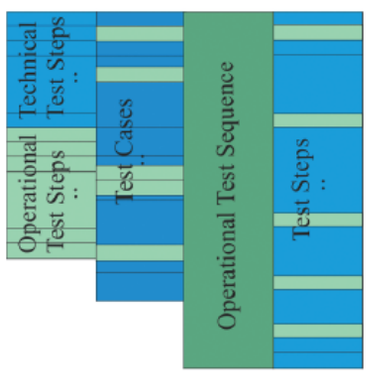

Figure 4: Structure of a test sequence for operational testing

The main difference is that the definition of the test sequences is not optimized to fulfil the specification requirements using the shortest possible sequences. The optimisation criteria are here to find as much relevant or important regular or disturbed operational scenarios to be tested.

The parameterization of the test sequences is done according to the operational environment. Average or standard parameters are typically used for this purpose. Extreme or rare parameters are to be avoided.

The main advantage is here, that the basic database of the test cases as well as the testing environment can be used for both as well as the execution environment in the lab.

3.3 Perspective: ATO Test Sequences

No matter, if the implementation of the ATO is done by integrating new features in the onboard train control or adding a module replacing the driver, both approaches can be tested on functional level by the approaches described above. Due to the experience with the ETCS test specification, the conformity approach is recommended. In contradiction to the current implementation of the conformity tests a closer relationship to the real operation is useful to avoid too artificial scenarios in the lab tests. This is even more important if a field test shall be executed with the same scenarios.

Looking a little bit into the details this means that for example the correct driving behaviour (acceleration/deceleration) of the ATO module can be tested similar to the current implementation of the tests for the braking curve behaviour of the ETCS EVC. The laboratory would stimulate the driving action by sending a movement authority (or whatever signals necessary) and the virtual position of the traction lever can be evaluated by the laboratory. This methodology can be transferred to all functional interfaces of an ATO-module or an integrated ATO system easily, as long as there is digital information available. Beside the already available methodology there is another advantage of this lab-testing approach: Assuming the number of tests will increase massively to reach a certification for an ATO module, the high efficiency of laboratory tests will reduce the effort to a productive level.

During a migration phase there will be a lot of data available from the non-automatic operated

trains. These data can be easily reused for testing the ATO systems. I.e. huge number of tests can be defined by using the real data and the trust in the systems can be maximized and a comprehensive testing for ATO on functional interfaces can be assured easily.

4. Interface Conformity of digitalized track-side equipment

4.1 Digitalization of track-side equipment

The general approach of constructing executable test sequences from generic test cases is equally well suited for the conformity test of track-side equipment as it is for testing on-board components. What is different with track-side equipment is the lesser degree of standardisation: Interfaces and even functional architectures may differ, depending on the manufacturer. To improve compatibility, an approach currently employed by the German Railways is to incrementally specify the interface behaviour of equipment components. I.e., only some of the interfaces of an interlocking system are specified (and shall be tested), while others remain to be considered somewhen in the future. The reason is that it is easier to specify and implement a standard version of the focus interface, and not having to come up with a formalisation and re-implementation of the full system.

The downside is that this approach faces an inherent difficulty when it comes to testing. To drive the focus interface (and observe the correct interpretation of messages received over it), it is usually necessary to have access to (all the) other interfaces. Specification is easier by far--one can “internalize” the uncontrolled interfaces by subsuming everything in internal behaviour of an automaton.

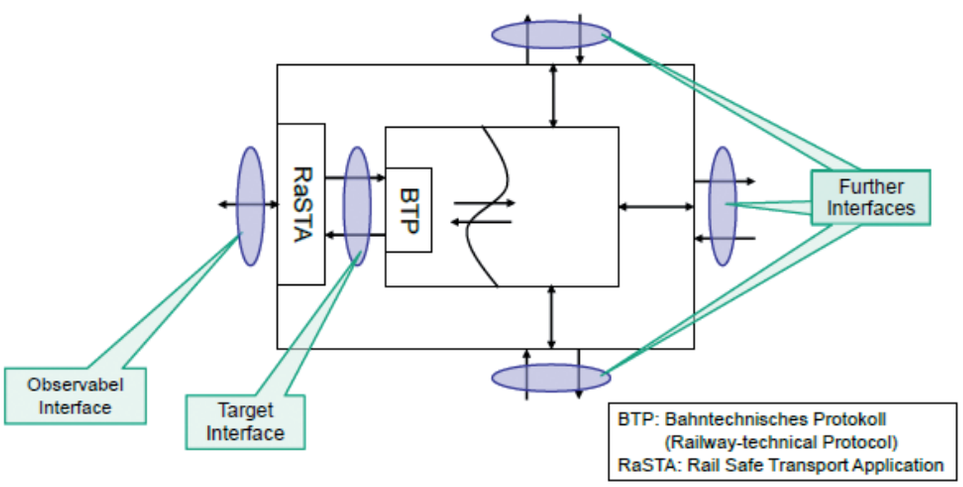

Figure 5: Schema of a system with four interfaces, of which one is to be specified

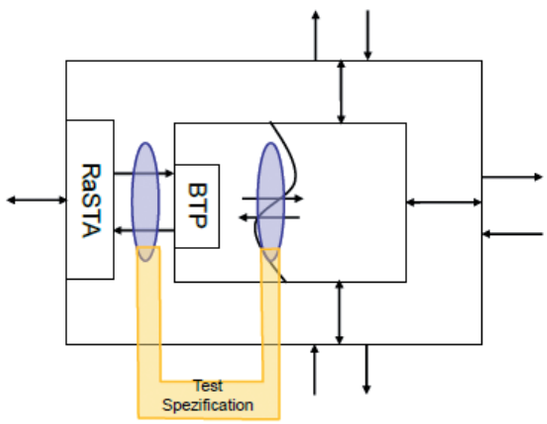

Figure 6:
Schema of a system with additional virtual internal interface as the specification view on the specific interface to be tested

Fig. 5 shows a schematic view of a system where the interface in focus is on the left, and is shown with some detail. The specification addresses the functional level of the Rail Technical Protocol (RTP) and abstract from the concrete implementation of communication through the Rail Safe Transport Application (RaSTA) which utilizes an Ethernet connection. Fig. 6 gives the specification view, where the additional virtual internal interface is added. Telegrams on the focus interface are related to messages and observations on this virtual internal one. Technically, these messages and observations are just actions of UML state machines which make up the specification. They reflect actions happening on the other (masked) interfaces, but are not formally related to them.

This works for the specification, but for testing it can of course not be done in terms of the internal specification interface but needs the real behaviour on the masked interfaces. I.e., test cases and operation have to take the view of Fig. 5, while their derivation must refer to Fig. 6. The problem is acerbated by the unavailability of a precise relation between internal and masked interfaces. In current practice, such a relation does not even exist: There are considerable differences between the masked interfaces (whose standardisation is yet to be initiated) in the different manufacturers' implementations of the devices as already mentioned above.

4.2 Solution Approach

Differences between the solutions of different manufacturers call for integrating them into the test process in some way. Our solution relies on the assumed ability of the manufacturers of bridging the gap between (virtual) internal messages and commands and externals. The envisaged test architecture is depicted in Fig. 7.

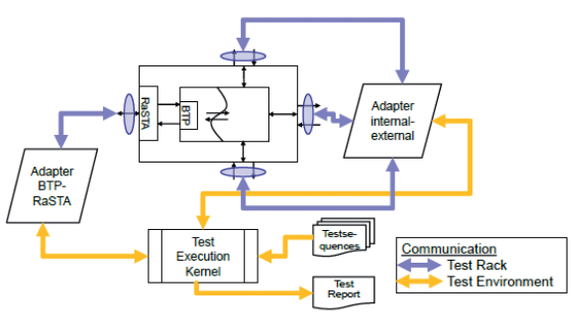

Figure 7: Components of the test architecture.

The test rack adds two components to the test object:

- Adapter internal-external: The manufacturer shall provide a module which translates between internal and masked interfaces. For its realization, interface drivers, simulators, or existing test interfaces accessing internals of the device may be used. Even a test engineer performing manual steps may be integrated via a suitable interface component.
- Adapter RaSTA-RTP: This module must be provided by the test laboratory.

The test rack serves to provide the test object with an interface which is on the same level of abstraction as the specification. The remaining components of the test architecture are rather standard:

- Test Execution Kernel: The kernel controls the test execution, i.e., it initializes the test objects, starts test sequences (including parameter completion in advanced scenarios), protocols the results, performs corrective actions (breaks and restarts if necessary) and generally monitors the execution. The kernel will be partially automatized.
- Test Sequences: A data base with test sequences sharing the characteristics with those of the on-board tests.
- Test Report: A data base for detailed result data and accumulated reports.

5. Validation

To be able to make qualified assertions of standard conformance, several arguments have to spelled out. On the one hand, the correctness and completeness, resp. sufficient coverage, of the test cases with respect to with respect to the specification has to be checked. This involves techniques and methods form the domain of model based testing. Currently, manually derived test suites are evaluated for their suitability. In future enhancements of the overall approach, also test case generation from the specification models is intended to be considered.

Adapter design and validation will have to cope with the common problems of crossing abstraction levels (namely atomicity and timing issues as well as value concretizations). For the internal-external adapter a monitoring concept which observes its operation dynamically is envisioned. The user interface of interlocking systems provides many information about internal states and thus qualifies as an adequate point of observation.

6. The Role of Formal Methods

Formal methods are used increasingly in the testing process of rail equipment, albeit slowly. They make their entry in one of two ways.

The first is via a formalisation of specification. This has a benefit in itself, as ambiguities, omissions and inconsistencies are reduced when a specification is formulated in a more or less rigorous notation. Examples from practice are the specifications of track-side equipment mentioned in the previous section. While currently limited to single interfaces, it is intended to specify the functional behaviour of, e.g., interlocking systems completely. Another example is the development of formalising the ERTMS/ETCS SUBSET 026 in the project openETCS.

Besides the effect of improving the quality, a formalised specification is of course a necessary basis for many further process enhancements. With respect to testing, formalised requirements permit at the very least a systematic derivation and coverage analysis of test cases, and in favourable scenarios even the automation of test case generation. For the latter, commercial tools are already available (rttester, rhapsodyATG, etc.), though these tools are not yet widely used in the rail domain.

The second way formal methods enter the testing process is in the automation of test construction. The elaborations in the preceding sections illustrate the highly nontrivial task of constructing a test set. In arranging test cases for the ETCS OBU, the Chinese postman algorithm has been used to find a first solution, which led to a stable test suite only after extensive work on parameter instantiation and calibration. Getting the timing, position and velocity parameters right proved to be rather difficult.

The construction of test sequences for track-side equipment is less difficult with respect to real-valued parameters, but on the other hand has to solve issues with testing generic systems which are to be instantiated to control a particular local arrangement of track elements. Testing is done on one or few sample layouts. To allow a flexible arrangement in test sequences, test cases should be formulated in a parametric style, permitting their instantiation depending on the needs of other test cases.

In both cases, formal languages for parametric test case specification are used, and algorithms for optimizing the arrangement into sequences are applied. These formal based solutions are still to be improved upon, as the currently available techniques have a limited scope and achieve non-optimal results.

7. Conclusion

The approach used for the conformity tests and operational tests for ETCS is proven in use and can therefore be extended for testing ATO functionalities and interfaces, too. As long as the interfaces are functional and digital the methodology can be reused easily. It may, like for interface conformity, even applied to partial standardisations. The principle method of the generation of the test sequences can be used for the different types of tests. The optimization criteria as well as the rules for the parameterization differ for the different kinds of tests. If the same approach for the formalisation and parameterization is used, the lab environment can be used for any type of test, with, however, some adaptations to be made to achieve sufficient flexibility.

Test case generation as well as test sequence construction profit substantially from the application of formal approaches. This field features a variety of languages, methods and tools. Present-day solutions cover only part of the needs of practice, but show potential to be much more useful if embedded applied in a carefully designed process employing adequate formalisations.

Future approaches for digitalisation of rail traffic management systems, train control systems or interlocking focus on a stronger modularisation and standardisation. Therefor the same approach should be applied to ensure conformity and interoperability of the modules of such digitalized components. By applying this proven-in-use approach the cost and time required for the tests can be reduced up to the final goal of zero field test .

8. References

- [1] ERTMS -- Test Sequences, SUBSET-076-6-3, Version: 3.0.0, 1/06/2016
- [2] ERTMS -- System Requirements Specification. SUBSET-026, Version 3.4.0, 15/06/2016
- [3] ERTMS -- Test Sequence Generation: Methodology and Rules. SUBSET-076-4-1, Version 1.0.2, 1/07/2016
- [4] ERTMS -- Methodology of testing. SUBSET-076-3, Version 2.3.1, 1/07/2016
- [5] ERTMS -- Functional requirements for an on-board reference test facility, Version:3.0.0, 15/06/2016