BITS&CHIPS

Background

Model-based testing in safety-critical Scaled Agile

30 August 2021

Machiel van der Bijl is the CEO and founder of Axini.

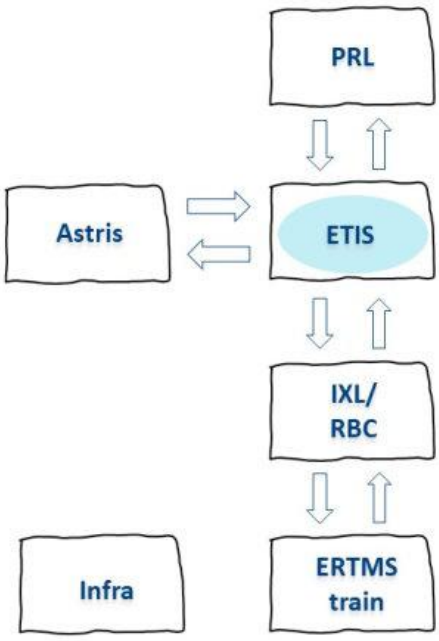
Harm van Beek is an Agile project manager at Prorail, through Cimsolutions.

Prorail is working hard to implement the new European Rail Traffic Management System (ERTMS). Together with Axini and Intraffic, it has set up a Scaled Agile project, applying a model-based testing approach in a safety-critical environment. An experience report.

The new European Rail Traffic Management System (ERTMS) is Prorail's big project for the coming years. With ERTMS, more trains can drive safely on the tracks in Europe. In the long run, this system may even enable self-driving trains. Whereas the current infrastructure conveys messages via signals next to the track, ERTMS allows direct machine communication with trains and engine drivers.

An important component in the machine communication to and from ERTMS trains is ETIS (ERTMS Train Information System). It communicates concurrently and continuously with three different systems: PRL, Astris and CSS. PRL (Procesleiding) is used by the train service controller to manage the trains. Astris enables communication

to and from the rail infrastructure like switches and signals. CSS (Central Safety System) is a new system that communicates directly with the new ERTMS trains.



ETIS and its environment

Safe and Cenelec

Although Prorail has quite some experience with building complex systems like ETIS, it remains very challenging work. One of the big challenges is preventing errors late in the project. These errors can disrupt the planning of a complex system tremendously, but they're very difficult to rule out as it's hard to test communicating systems such as ETIS without their environment.

Another challenge is that Prorail needs to adhere to the Cenelec safety standard (EN 50126/50128/50129). In terms of Cenelec, ETIS is of Safety Integrity Level 1. This means that Prorail needs to follow the rules and regulations prescribed in the standard to build such a system. One of the rules is that the development tools are validated for use.

Last but not least, Prorail employs the Scaled Agile Framework (Safe). This means that at the end of every increment, preferably at the end of every sprint, the team delivers a production-ready system and at the end of every increment, ETIS and its environment are integrated into a working setup and tested. Safe and Cenelec aren't a natural fit; often safety-critical projects follow a more waterfall-like approach.

Cut down on test cost

ICT Group subsidiary Intraffic won the tender to implement ETIS together with Axini. A key part of their approach was to use the Axini Modeling Platform (AMP). The platform as used by Prorail/Intraffic consists of two main components: modeling and no-code test automation.

AMP provides computer-supported formal modeling of specifications in the Axini Modeling Language (AML). In the case of Prorail, this means that paper-based specifications are modeled (a kind of programming) in AML. We used three types of specifications: IRS (Interface Requirements Specification), IDD (Interface Data Definition) and SRS (System Requirements Specification). These build on top of each other.

AMP is capable of automating the entire test process using the information in the AML models. This means that there's no need to manually program test cases including test data. The platform generates these automatically and executes them against ETIS. It thus allows to cut down on test cost while increasing test quality and coverage. This was an important reason for Prorail to choose Intraffic/Axini.

Axini's model-based testing approach

Model-based testing (MBT) is a highly overloaded term. Axini's MBT approach automates the entire testing process: it automatically generates, executes and

evaluates tests. It’s a form of model-based software engineering. However, instead of generating code, it generates test cases.

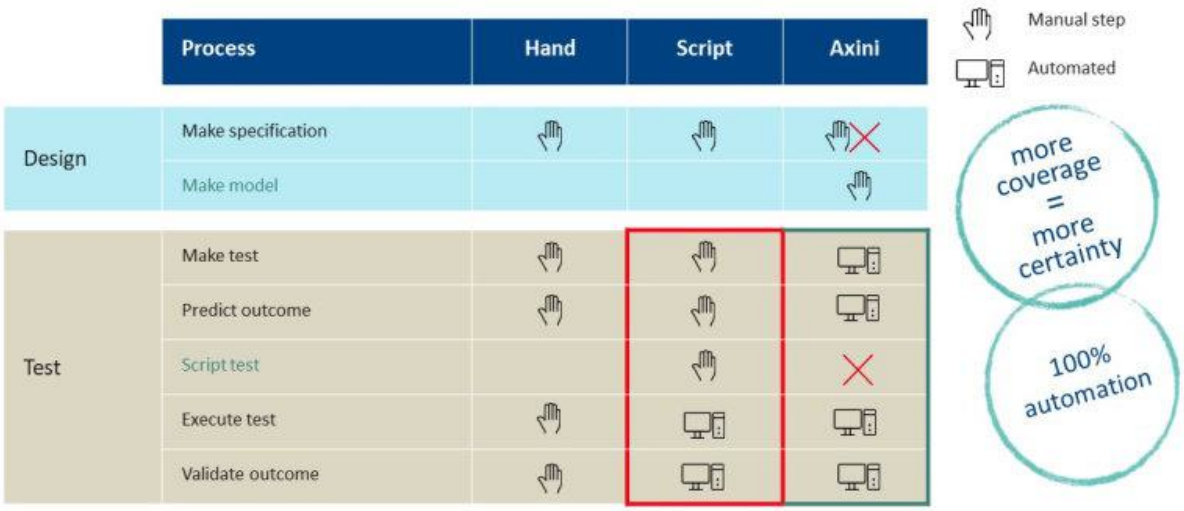


Figure 1: Axini MBT vs. scripting

Figure 1 shows the difference between manual testing, scripting and the Axini approach. For manual testing, we need a specification, based on which we create tests predicting the outcome. We then execute the test and evaluate the outcome. Scripting approaches, like BDD and TDD, automate part of the test execution using programmed tests. Axini’s MBT approach obviates the need to program test cases. Instead, we make a model of the system under test and automate all testing steps: test creation, prediction of the outcome, test execution and evaluation. The model is also used as a specification/design artifact. Some clients generate the entire specification from the model.

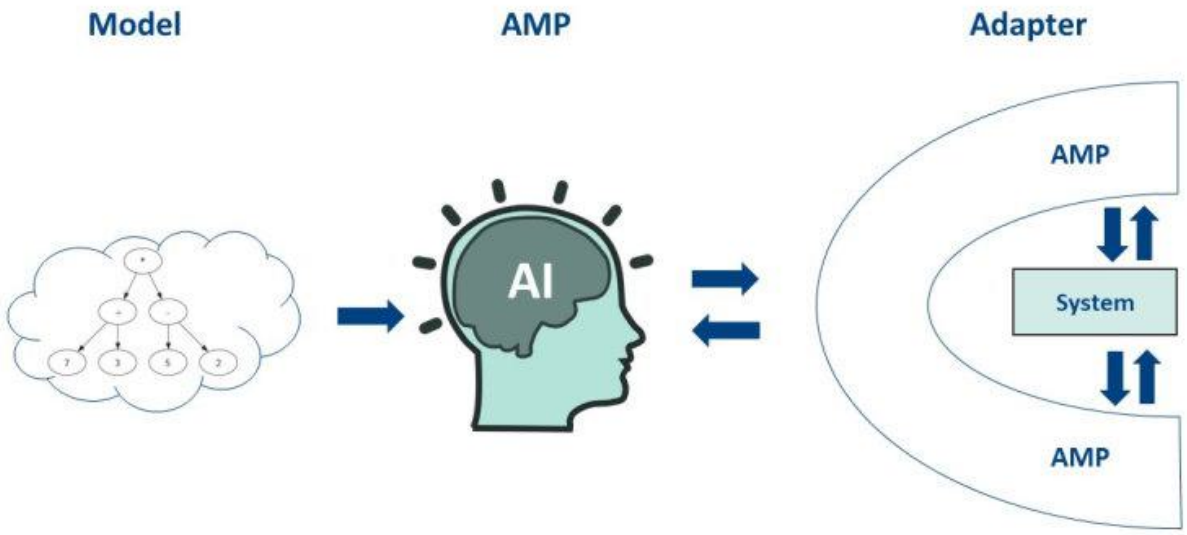


Figure 2: Axini Modeling Platform in action

Figure 2 depicts how the Axini Modeling Platform (AMP) works during testing. The adapter envelops the system under test, allowing AMP to independently send and receive messages over all the interfaces. The model defines the relation between inputs and outputs according to the specification. AMP reads the model and, armed with this information, experiments with the system under test to see if it conforms to the specification. The ability to send and observe messages simultaneously over all the interfaces allows for early testing during the development cycle without the need for simulators or the external system environment.

Ahead of schedule

The ETIS team started modeling directly at the beginning of the project, before programming. This provided immediate feedback to the designers of the specification and improved their output. Every Safe increment consists of several sprints in which the required features are prepared in Jira issues. During the sprints, the features are programmed and modeled in parallel – following the Cenelec requirement that programming and testing are done independently. Unit tests are used to check the

code. Once (part of) a feature is finished, it's immediately tested against the model. The unit tests and the model-based AMP tests are the team's main tests.

The approach is working well. The ETIS project is six months ahead of schedule – 25 percent of the original scope. The team has saved at least 5,000 hours in testing and there have been virtually no integration problems. This is rather unique for Prorail projects of this complexity.

The approach has been integrated into the ETIS team and all team members are trained in AML and AMP. We've found many errors: 'normal' ones but also those that are hard to uncover and could have caused serious integration or even production problems. These errors are detected and fixed immediately during the sprints.

Lessons learned

Having done most of the model-based testing (MBT) at Prorail already, it seemed only logical for Axini to do this work again in the ETIS project. Consequently, the MBT activities had their own budget and targets – this ensures that the activities are independent and can't be overruled by other parties, eg scrum masters or product owners. In Safe projects, however, it's important for all team members to work in the same cadence, following the integration and test cycles. If something changes in the planning, the MBT activities and availability also change. We've learned that model-based testing needs to be integrated into the entire team and MBT budget and resources need to be integrated with the other development activities.

As anticipated, starting modeling before development has a big impact. On the one hand, errors, problems and under-specifications are found early on. On the other hand, information that before was only needed during development is now requested much earlier, at a time when the required people (like designers) tend to be otherwise occupied. We've learned that this needs to be addressed in the organization because if updates don't come quickly in the Safe cadence, modeling is seriously hampered.

The project has also had a big impact on AMP and our MBT approach. ETIS is a relatively big and complex system with complex and big data structures being exchanged with the outside world. It's one of the first systems where AMP is used directly from the get-go, before programming, and where validation feedback was immediately processed in the sprints. While MBT usually focuses on the correctness and robustness of interfaces, for ETIS, it's also used to test system functionality. In fact, next to unit testing, MBT is the only test automation approach being applied. Driven by the project, we've come up with several improvements to the platform and the approach, including support for big and complex messages, user scenarios, Cenelec-validated updates and adapter generation. We've also further improved the robustness and user-friendliness of the tooling.

Shift-left with quality built-in

The ETIS project shows that model-based testing, supported by an MBT platform, speeds up development while delivering high-quality software. Improving the quality early in the process prevents errors and rework, allowing the entire system to be built faster. This is one of the promises of model-based systems engineering, of which MBT is an important part, but it's good to see this pan out in practice, including the numbers to make a business case.

The project is also a good example of, in Safe terms, a shift-left with quality built-in: finding errors early and preventing them from impacting development later in the process. Axini's MBT platform has realized this important business goal for Prorail within the given time and budget constraints.