CASE

Agile working methods in a safety-environment

Companies that develop software which must function in a safety environment need to comply with the European CENELEC standard. The CENELEC standards stipulate which processes you need to follow when you develop safety-relevant software. These standards are based on the V-model: build first, test later. This working method is a proven and robust approach to safety-critical projects, but it leaves little room for flexibility. This is why ProRail chose the SafeScrum approach, combined with Model-Based Testing by InTraffic and Axini. This approach allows updates to be implemented at an early stage, while working in compliance with safety standards. The method results in higher quality and lower costs.

ProRail will adjust the present train security system in order to comply with the European standard ERMTS: European Rail Traffic Management System – a comprehensive and complex assignment. ProRail awarded the project of developing ETIS, the ERTMS Train Information System, to InTraffic. This system transmits information from trains to PRL (Process Control) and vice versa. The development of ETIS is an important part of the much larger PEIL-project, which stands for ProRail ERTMS ICT Logistics.

Harm van Beek is project leader ERTMS Train Control at ProRail and manages the development of the ETIS-project. Harm describes the importance of quality assurance and safety: "Quality assurance is of the utmost importance for the railroads. The various software systems have to operate in a safe manner, but the interfaces between the various systems must also be developed in accordance with the most stringent safety requirements. After all, the entire chain has to function safely."

INTRAFFIC
mastering mobility

SafeScrum is a certified method for developing software in compliance with the highest security standards.

ERIK VELDHUIS,
SAFETY MANAGER ETIS PROJECT AT INTRAFFIC

SafeScrum: best of both worlds

InTraffic appointed Erik Veldhuis to the ETIS-project to supervise quality assurance and safety management. "We have our own quality system and of course we have to comply with the CENELEC-standard as required by the EU", says Erik. "The latter involves a challenge, because the EU safety standards are based on the V-model: you start by making a complete design of the system to be developed, then you write the code and subsequently you test the code. This approach differs from the Scrum method which we prefer to use at InTraffic. Scrum is an iterative working method that allows you to continuously elaborate on what you have developed. You work in sprints of several weeks – in our case three – while you directly test the software you developed during each sprint.

InTraffic chose to work with SafeScrum in order to meet the stringent safety requirements while at the same time maintaining flexibility within the development environment. Erik: "An implicit feature of the SafeScrum method is that you constantly view the software you design from a security perspective. The following routine question is directed at all team members during each daily stand-up: have you noticed 'hazards' that may lead to potential risks or accidents? A hazard is a condition of the system that could possibly lead to an accident. We keep a 'hazard log' in which we record the causes and effects of each risk, how we could remove the risk and which mitigating measures can be conceived when there is no software-based solution." SafeScrum was developed by experts and has been evaluated positively by external Independent Safety Assessors. "It is a truly certified method for developing software in compliance with the highest security standards", Erik explains.

Model-Based Testing

InTraffic uses Axini tooling to test the software. Axini founder Machiel van der Bijl describes the process underlying the tool: "One of the tools we supply is Model-Based Testing (MBT). This method follows the approach of model-based software development. You use the model and its formal language to make unambiguous statements about what has to happen according to the specification, and you relate this to the requirements. The model-based testing process consists of a number of fully automated tests that verify whether all requirements have been met. This is how you close the loop." The unique feature of the Axini-solution is that you don't need to write and script the test cases by hand. Instead, they are generated automatically in such a way that even the most unlikely scenarios are tested. A CENELEC SIL1 system requires the MBT tooling to be validated to allow it to be used for developing software that has to comply with the strictest safety requirements.
Machiel: "You have to describe what the tool does and show that the tool is suitable for developing software that is applied in safety-related projects. One of the requirements is traceability: not only do you have to show that the tests are functioning properly, but you also have to demonstrate the relationship with the requirements stated in the specification. The great thing about our model-based tool is that test scripts are generated automatically on the basis of the requirements. This means that all required tests will have been performed at the end of a sprint."

Faster feedback

This method fits in with the principles applied by ProRail for the ETIS-project, says Harm. "We want faster feedback on software that has been developed. This also means that there is less work at hand, because it reduces the number of test results. For instance, at any given moment you will only have up to 30 test results instead of 300. We want to create a predictable situation when we get closer to delivery dates, in order to ensure steady progress in the PEIL-project. In complex integrations you can't wait with developing the interface until the software is ready; the integration has to be an integral part of the development process. This is only possible when all involved Scrum teams follow the same style and rate of progress, with system demos

→

to happen in a timely cadence. Finally, we want to make the software available when it is needed. If we develop an integration between ETIS and PRL now, it can't be taken into production straight away because ETIS and ERTMS are not going live yet. SafeScrum satisfies the conditions imposed by each of these principles."

SafeScrum & SAFe

In order to meet the conditions of the last two principles, the overarching PEIL project works in accordance with the SAFe methodology. You pronounce the word SAFe in the usual way, but the A and F are written in capitals. Harm: "SAFe stands for Scaled Agile Framework, a realisation method that is applied in large implementations and which ensures continuous alignment of work that is performed by multiple Scrum teams. We employ this method within the larger PEIL-project to make sure that all project teams are well aligned in terms of their style and rate of progress." Harm is aware of the fact that the terminology can cause confusion. "These are two different working methods, but they complement each other perfectly", he says.

Many projects have proven that agile working methods – short cycles with fast feedback and smaller working units – result in software of higher quality at lower costs.

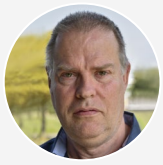
HARM VAN BEEK,
PROJECT LEADER ERTMS TRAIN CONTROL AT PRORAIL

Focus on quality results in cost reduction

SafeScrum allows you to combine Scrum with working safely, and this offers a number of benefits according to Harm van Beek, Erik Veldhuis and Machiel van der Bijl. Harm: "Many projects have proven that agile working methods – short cycles with fast feedback and smaller working units – result in software of higher quality at lower costs. The safety world has held onto the waterfall model for a long time because of the lack of a good alternative for guaranteeing safety. However, the test results of the waterfall model and retrospective testing always require a lot of rework. The later you find an error, the more expensive it is to correct it because it often affects other parts of the software. Which means that in addition to fixing one single error, you also need to correct all consequential errors. SafeScrum allows you to find your errors at a much earlier stage and thus correct them much earlier, usually already during the next sprint. This working method results in a substantial cost reduction, because the focus is on quality. Quality improvement always results in reduced costs, while the reverse does not always hold true. So it is much better to use quality as your guiding principle instead of costs. And this is precisely what we are doing with SafeScrum."

Contact

Harm van Beek
Project leader ERTMS train control at Prorail
E harm.vanbeek@prorail.nl



Erik Veldhuis
Safety manager ETIS project at InTraffic
E erik.veldhuis@intraffic.nl

Machiel van der Bijl
Founder of Axini B.V.
E vdbijl@axini.com