ITEA Success Story

SAFE

Sustaining automotive safety standards and standardisation

Driving on the road is a way of life – whether for work or for leisure. Being able to get safely from A to B is something we take for granted. And today driving is safer than it was ten years ago, and ten years before that, and in ten years time it will be even safer. This progress can be measured – fewer accidents, fewer injuries, fewer deaths = less cost to society, in both human, financial and environmental terms. So the benefits of safe driving are crystal clear. But to get to that stage, a lot has gone on, and is still going on, behind the scenes and particularly in the software that has become the key ingredient of every modern mode of transport, the road vehicle being no exception.

Functional safety

When the ITEA SAFE project finished in 2014, it had played a vital role in establishing the safety as we increasingly know (and demand) it today in our daily driving. “Essentially, SAFE is part of a long chain of ITEA projects, part of an ongoing story, if you like,” project leader Stefan Voget explains, “to improve the functional safety of electrical and/or electronic systems in production vehicles. What it managed to achieve was the standardisation of a modelling language for use throughout the development cycle, from requirements to the hardware and software phase. In November 2011, the ISO26262 was introduced and at that moment nobody had the knowledge how to use it in their processes, while it was very important to comply with it; for domains where the safety is very critical you either comply with the standard or you are out of the market, or at least severely lagging behind. Our goal was to enable the automotive industry to comply effectively with ISO26262 by providing model-based development processes that integrate functional and safety development based on existing development lifecycle processes.”

Impact

The measure of the success in achieving this goal was underlined at the ITEA-ARTEMIS-IA Co-summit in Berlin in March 2015 when the SAFE project was the recipient of the Award of Excellence in the category 'Standardisation'. This award recognises the high-level technical contribution that a project makes through true international collaboration to generating significant results and promoting the programme and its goals. SAFE was also an integral part of the EAST-EEA success story published in the ITEA magazine in January 2014 (number 17). As Stefan said at the time, "the results of the EAST-EEA project, although it finished a decade ago, act like a reference platform for further development in new projects." The same can be said of SAFE; it may have finished but its impact continues to be felt. And one of the reasons why the impact of the project is still felt today is that not only does the tool enhancement support the users in safety modelling and analysis but it also directly influences how the processes in the automotive market change towards the integrated modelling of both functional and safety aspects.

Eye-catcher

Of course, impact is best measured through implementation. So how have the project results fared? The project partners had already been involved in the standardisation activities of the EAST-ADL and AUTOSAR projects, and then in producing the ISO 26262 – SAFE was another, essential part of the jigsaw. The establishment of ISO 26262, and compliance with it, was crucial to get functional safety to a higher level. However, apart from the standardisation activities, it was the Eclipse-based tool platform activities that created visibility and generated interest in the market. "And since the tools in the SAFE project were developed by both commercial tool vendors and research institutes, these were already integrated in existing bigger toolsets from the beginning on," Voget adds, "fast exploitation was facilitated by delivering new versions of the commercial tools as well as by publishing new features in the research tools."

Exploitation

On the back of its involvement in the SAFE project, Dassault Systèmes, with aerospace industry roots and experience with the energy and railway domains, has developed a Smart, Safe & Connected Car solution that offers customers the 3DExperience platform© (including PLM) to give automotive developers a very specific way to manage the kind of embedded systems that have become a growing challenge in the automotive industry. This new solution is also designed to help customers ensure they are compliant with the ISO26262 and Automotive Open System Architecture (AUTOSAR) safety standards. It contains four modules: an Electronics & Electrical Architecture Definition, Behaviour Modelling and Simulation, Electrical Engineering and Functional Safety Delivery. This last module is designed to give users the ability to track the ISO 26262 safety standard throughout the product design process and took benefit of the SAFE project on Preliminary Risk Assessment, System Safety Concept, Fault Tree Analysis and Failure Modes & Effects Analysis; in this Dassault Systèmes' solution, the proof of the pudding really is in the eating. The solution is currently under negotiation with several automotive customers.

Thanks to the SAFE project, Continental established the ISO26262 compliance in two major domains, namely the safety critical domains of power trains and chassis break systems. These domains represent 40% of Continental's product share and if it they hadn't participated in the SAFE project, Continental would have had an important setback compared to others in the market.

Other examples of successful exploitation of the project's results include Vector Informatik, which implemented FMEA, a model-based qualitative safety analysis method, and added malfunction modelling capabilities in its PREEvision tool, a software application that supports architects, network designers, development engineers and test engineers through the entire development process. Thanks to the SAFE project the integrated modelling of safety aspects is now possible. And pure::systems managed to seamlessly integrate pure::variants into the SAFE platform, thereby enabling the variant management capabilities of pure::variants for contexts with safety related assets. Through tool supported variant management the development process becomes more efficient, faster and more reliable up to 20%.

Ongoing story

"And now, in 2017, three years after the end of the project, we have even got together with one of the former partners, Fortiss, to continue the story by applying the SAFE safety methods to new emerging functionalities," Voget says. "This is the direction that is occurring at the moment – the need for more flexibility to update and upgrade the software in the car. This was not a scenario we had in mind at the time of the project; we are now seeing the element of security playing a more important role. So, it's safety and security. We are facing a new challenge, then, one that has been given an extra dimension, so to speak. However, because the SAFE project has given us such a good basis in terms of safety – we know how to cover the functional safety – we concentrate our efforts on the security challenges that come with growing connectivity – the Cloud, the internet – in the automotive domain." And so the story continues!