ASSUME

Reducing bugs and false errors to boost efficiency

Mobility is one of today's key societal challenges and is impacted by a huge array of factors, including global warming, restrictions in the energy supply, an ageing population and security concerns. Fortunately, autonomous systems can play an important role in tackling all of these issues due to the possibilities for increased safety, reduced fuel consumption and emissions and social inclusion for the elderly or disabled.

Success story

An inherent problem, however, is the excessive amount of time taken by tools to find bugs and false errors in autonomous systems. For instance, tools using abstract interpretation to prove the absence of runtime defects typically cease to be useful above 200-300,000 lines of code (depending on the programming features and complexity), while model checking techniques are currently limited to much smaller code sizes. This is the challenge that a consortium of 38 partners set out to meet from September 2015 to December 2018 within the ITEA project ASSUME (Affordable Safe & Secure Mobility Evolution).

The challenge of public perception

By bringing together a mix of OEMs, SMEs, tool/service providers and research institutes from five countries (France, Germany, Turkey, Sweden and the Netherlands), ASSUME aimed to boost tool performance and efficiency in the mobility domain. A major step for the development of autonomous systems is the shift from assistance systems to automated (hands-off) systems which are completely responsible for their own decisions. Public perception is moving towards higher expectations regarding the safety of highly autonomous systems; as a result, greater trust is needed if automated driving is to become both applicable and acceptable. With hands-off systems, a failure rate clearly below that of a human actor is the minimum expectation. Future mobility solutions will therefore rely on smart components that continuously monitor the environment and assume an increasing amount of responsibility for convenient, safe and reliable operations.

In a nutshell, ASSUME's main goal was to enable the affordable, standard-compliant development and verification of highly automated, safety-relevant and performance-critical mobility systems. A strong focus on development methods for concurrent systems and static verification techniques allows for the cost-effective proof of the absence of problems, even in a multi-core environment. The major field of innovation for the project's industrial partners (end-users) was model-based parallel software engineering for multi- and many-core processors. By improving their existing tools and developing new ones, ASSUME ultimately enabled the effective use of formal verification and synthesis technology along the design flow.

Improved connections between companies

German partners have seen successes in terms of technical output, commercial results and ongoing

Project start
September 2015

Project end
December 2018

Project leader
Dumitru Potop Butucaru
INRIA

More information
itea4.org/project/assume.html

collaboration. Bosch, for example, worked with several ASSUME partners to develop new methods and tools for the sequential verification of very large embedded software. Through several Bosch use-cases, these lead to a threefold decrease in the time taken for verification, a reduction of the memory footprint by a factor of three and a reduction of the number of false warnings by a factor of up to ten. The methods developed in ASSUME are now routinely used for large software products with more than two million lines of code. Furthermore, the methods and tools are being applied in several other business units of Bosch, which can now use formal methods efficiently in real projects.

ASSUME has also improved connections between companies: during the project, BTC ES, MES, Daimler and OFFIS set up a collaborative toolchain for model-based, requirement-driven development which integrates the industrial tools of BTC ES and MES with an OFFIS research prototype. In an industrial use-case provided by Daimler, it has been shown that this can reduce the effort for safety verification while improving requirement traceability. From OFFIS' perspective, ASSUME demonstrated both opportunities and shortcomings for the application of formal methods in industrial settings and also had a positive impact on their overall funding status. In addition to support for several PhD positions, they were able to acquire extra projects (including ARAMiS II and PANORAMA) and improved their standing in the scientific community with various peer-reviewed publications.

The methods developed in ASSUME are now routinely used for large software products with more than two million lines of code

As for other highlights from German partners, FZI Research Center for Information Technology has extended their portfolio towards safety-critical software and their follow-up activities have financed several new staff members. Various research projects building on the discussions and outcomes of ASSUME have been initiated, particularly with the German automotive industry but also with tooling providers and national academic partners. Likewise, EXPLEO has extended its software code quality assessment and model quality assessment while continuous customer projects in both fields have resulted in a growth of two to three highly-qualified employees. Bosch aims to keep this ball rolling with new, publicly-funded projects with former ASSUME partners and has generated greater awareness of the project's results through a joint paper on sound abstract interpretation published at the SAE World Congress.

Enabling knowledge transfers

The main activities of the Swedish consortium, which was led by KTH, were focused on allowing seamless traceability and impact analysis of functional and safety properties for Scania's development environments alongside SME FindOut. The collaborations initiated in the project are still running at several levels. A KTH senior researcher for instance, has been working part-time as an external consultant for Scania's R&D team on technologies initially developed within ASSUME – a great example of sustainable cooperation focused on knowledge transfers from academia to industry. KTH also recruited a software developer, who has been following up his activities as a PhD student in their research unit. Thanks to his involvement in ASSUME, this software developer is now a co-chair of the governing board of the OSLC Open Project, an international standardisation effort related to the software integration technologies promoted by KTH and Scania in ASSUME.

KTH's goal of pragmatic technical collaborations with Swedish industry has clearly been fulfilled as activities initiated within the project resulted in a significant increase in Scania's internal efforts based on ASSUME technologies, a momentum which is still ongoing. These developments have also been felt among the smaller companies, as FindOut was able to hire two consultants for three years to develop a suite of visualisations for electrical systems, message passing structures and software structures which has now been integrated into tools for system architects at Scania. Overall, these successes have allowed project partner KTH to remain visible at an international level regarding sustainable standardisation efforts for technologies in their research agendas.

New connections for academia

In addition to collaboration between industry and academia, cross-academic links also had a crucial role to play in ASSUME. In France, Sorbonne Université and École Normale Supérieure collaborated on novel techniques to allow for the

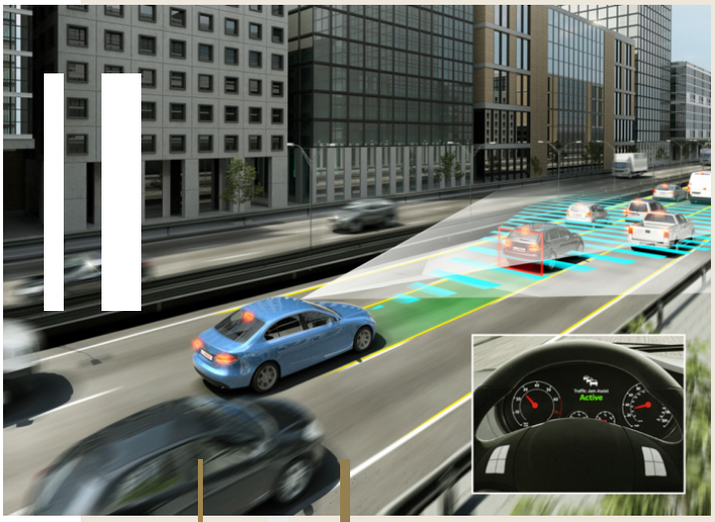
static analysis and verification of parallel software running on multicore processors. Most notably, they developed new models and abstractions that account for the weak consistency memories of multicore systems (including Total and Partial Store Ordering models), the detection of deadlocks and the real-time scheduling policies used in multicore embedded software systems (including dynamic priorities and the priority ceiling protocol). This produced both theoretical results (accompanied with formal proofs) and proof-of-concept implementations.

For Sorbonne Université, ASSUME's impact is predominantly internal as project-related publications have consolidated the institution's reputation as an expert in the formal analysis of concurrent software. The project also led to one PhD defence, with the student subsequently hired at a company which develops static analysis tools. In regard to the intersection of academia and industry, Sorbonne Université and École Normale Supérieure's results were integrated by AbsInt into their Astrée industrial analysis tool (enhancing its scope, efficiency, and precision) and their partnerships with Airbus and AbsInt were strengthened. As a result, AbsInt was able to develop the first ever sound static analysis for embedded automotive software targeting the novel multicore AUTOSAR standard.

Benefits across Europe

Similar outcomes were seen at other partners across the Netherlands and Turkey, such as the Dutch research institute TNO. The ASSUME project afforded them the opportunity to advance their knowledge on functional safety and the systematic analysis of automotive applications in vehicle automation in order to ensure their reliability and functional safety. In turn, this allowed them to sharpen their market propositions in subsequent projects, train colleagues on these topics and attract new projects. More tangibly, they were able to develop an analysis tool based on a combination of Matlab and Enterprise Architect, which was then expanded and superseded by new efforts from a number of colleagues.

At Eindhoven University of Technology (TU/e), the project's most significant outcome was the sparking of an investigation into the use of max-plus automata to significantly enhance the scalability of performance verification of embedded stream processing systems. Following the end of ASSUME, this was extended to cyber-physical systems and manufacturing systems. In addition, ASSUME made TU/e aware of both the importance and the costs of fault-resistance, especially in the context of FPGA-based designs in the automotive domain and for space-critical operations. The advanced analysis techniques developed in the project have been consolidated into the publicly-available SDF3 (SDF For Free) toolset and the open-source tool LSAT and have been used in collaboration with ASSUME and other partners.



As one final success story from ASSUME, Turkish partner KoçSistem used the project to develop or improve various tools, including AlloyInEcore (for specifying metamodels with their static semantics to facilitate formal, automated reasoning on models) and Tarski (providing generic frameworks for automated traceability analysis). In addition to opening up a commercial revenue stream with Ford Otosan, ASSUME has led them to start a new, local R&D project based on automotive manufacturing processes and receive funding for two additional ITEA projects, XIVT and PANORAMA.

Ensuring a smooth transition

All in all, ASSUME has brought enormous technological benefits to the field of autonomous systems for mobility through the design of a Static Analysis Platform (SAP) that allows for more efficient development of safety-critical, concurrent software for different domains, as well as high-quality, fault-free code for future software systems. Thanks to the creation of a tool chain, ASSUME has enabled the use of results between different tools including:

- a 50% increase in the (run-time) performance of analysis tools
- a 60% reduction of spurious warnings in analysis tools for single cores
- an almost 100% reduction of error classes in single core analysis
- an 80% or more success rate of traceability of run-time errors back to the model level
- a 40% cut in efforts to inspect runtime errors in a typical industrial setting

Greater efficiency means lower costs for organisations in this domain, as well as the opportunity for new collaborations and increased market access via increased interoperability between different players and technologies. Around 700 developers currently use one or more tools developed in the ASSUME project and this number is set to grow, helping society as a whole to make a smooth transition to mobility which is sustainable, affordable and inclusive for all.