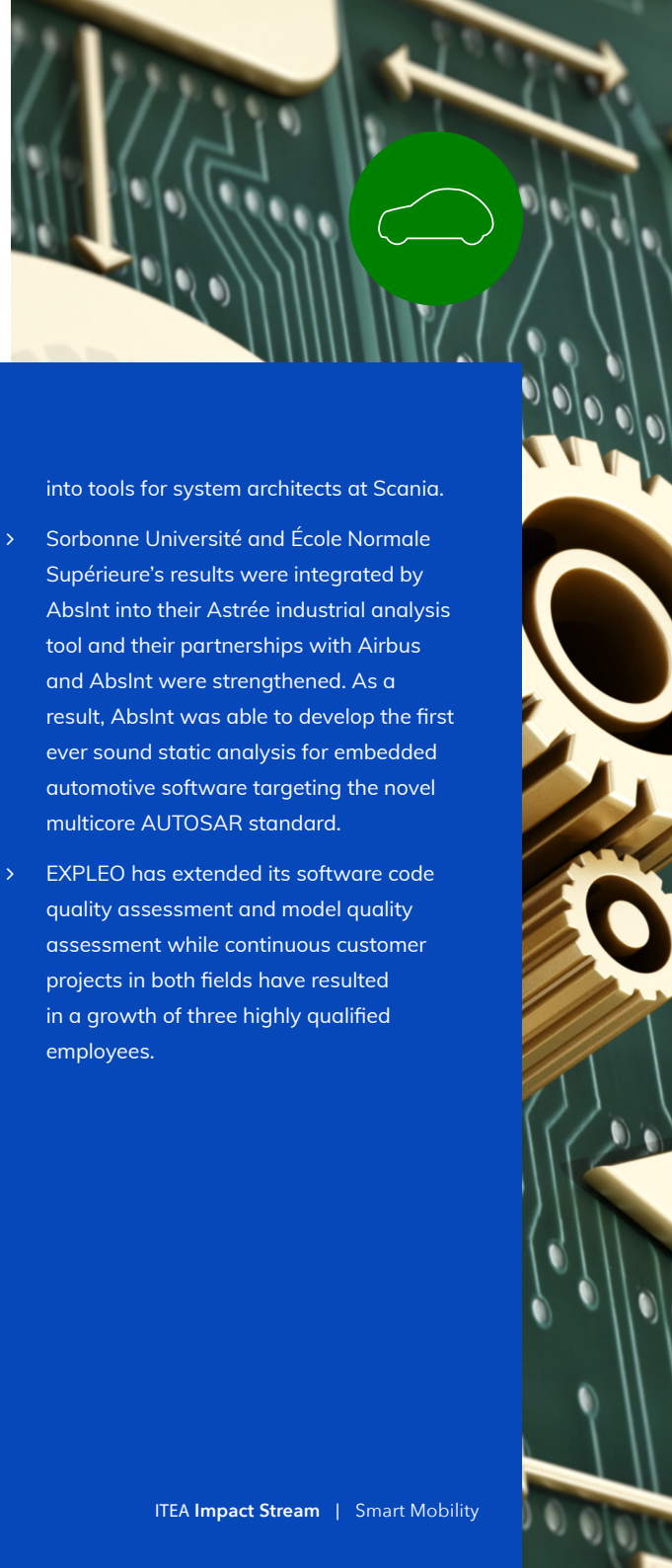
ASSUME

Reducing bugs and false errors to boost efficiency

Published October 2021

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.

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 the ASSUME consortium of 38 partners from 5 countries set out to meet from September 2015 to December 2018.



Impact highlights

- 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
- In Bosch, 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.
- 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.
- Sorbonne Université and École Normale Supérieure's results were integrated by AbsInt into their Astrée industrial analysis tool 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.
- 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 three highly qualified employees.

Project results

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.

Exploitation

The ASSUME partners have seen successes in terms of technical output, commercial results and ongoing 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.
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.

The main activities of the Swedish consortium 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 knowledge transfers from academia to industry. Cross-academic links also had a crucial role to play in ASSUME. For example, Sorbonne Université and École Normale Supérieure developed new models and abstractions that account for the weak consistency memories of multicore systems, the detection of deadlocks and the real-time scheduling policies used in multicore embedded software systems. This produced both theoretical results and proof-of-concept implementations.

ASSUME made TU/e aware of both the importance and the costs of fault-resistance, especially in the automotive domain and for space-critical operations. The developed advanced analysis techniques 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.
Thanks to newly developed or improved tools, ASSUME enabled KoçSistem to open up a commercial revenue stream with Ford Otosan, and start a new, local R&D project based on automotive manufacturing processes and two additional ITEA projects, XIVT and PANORAMA.

Around 700 developers currently use one or more tools developed in ASSUME 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.

ASSUME

14014

PROJECT LEADER

Dumitru Potop Butucaru, INRIA

PROJECT START

September 2015

PROJECT END

December 2018

PROJECT WEBSITE

https://itea4.org/project/assume.html

PARTNERS

France
- Airbus Operations ●
- École Normale Supérieure (ENS) ◉
- Esterel Technologies ⊙
- INRIA ○
- Kalray ⊙
- Safran Aircraft Engines SAS SNECMA ●
- Safran Electronics & Defense Sagem ⊙
- Sorbonne Université ◉
- Thales ●

Germany
- AbsInt Angewandte Informatik ⊙
- BTC Embedded Systems ⊙
- Daimler ●
- Expleo Germany ●
- FZI Forschungszentrum Informatik ○
- Karlsruhe Institute of Technology ⊙
- Kiel University ◉
- Model Engineering Solutions ⊙
- OFFIS ○
- Robert Bosch ●
- Technische Universität München ◉

The Netherlands
- Eindhoven University of Technology ◉
- NXP Semiconductors Netherlands ●
- Recore Systems ⊙
- TNO ○
- University of Twente ◉
- VDL Enabling Transport Solutions ●
- Verum Software Tools ⊙

Sweden
- Arcticus Systems ⊙
- FindOut Technologies ⊙
- KTH (Royal Institute of Technology) ◉
- Mälardalen University ◉
- Scania ●

Turkey
- Arcelik ●
- Ericsson ●
- Ford Otosan ●
- Havelsan ●
- KoçSistem ●
- UNIT Information Technologies R&D ⊙

● (Large) Industry ○ Research institute ⊙ SME ◉ University ● Government