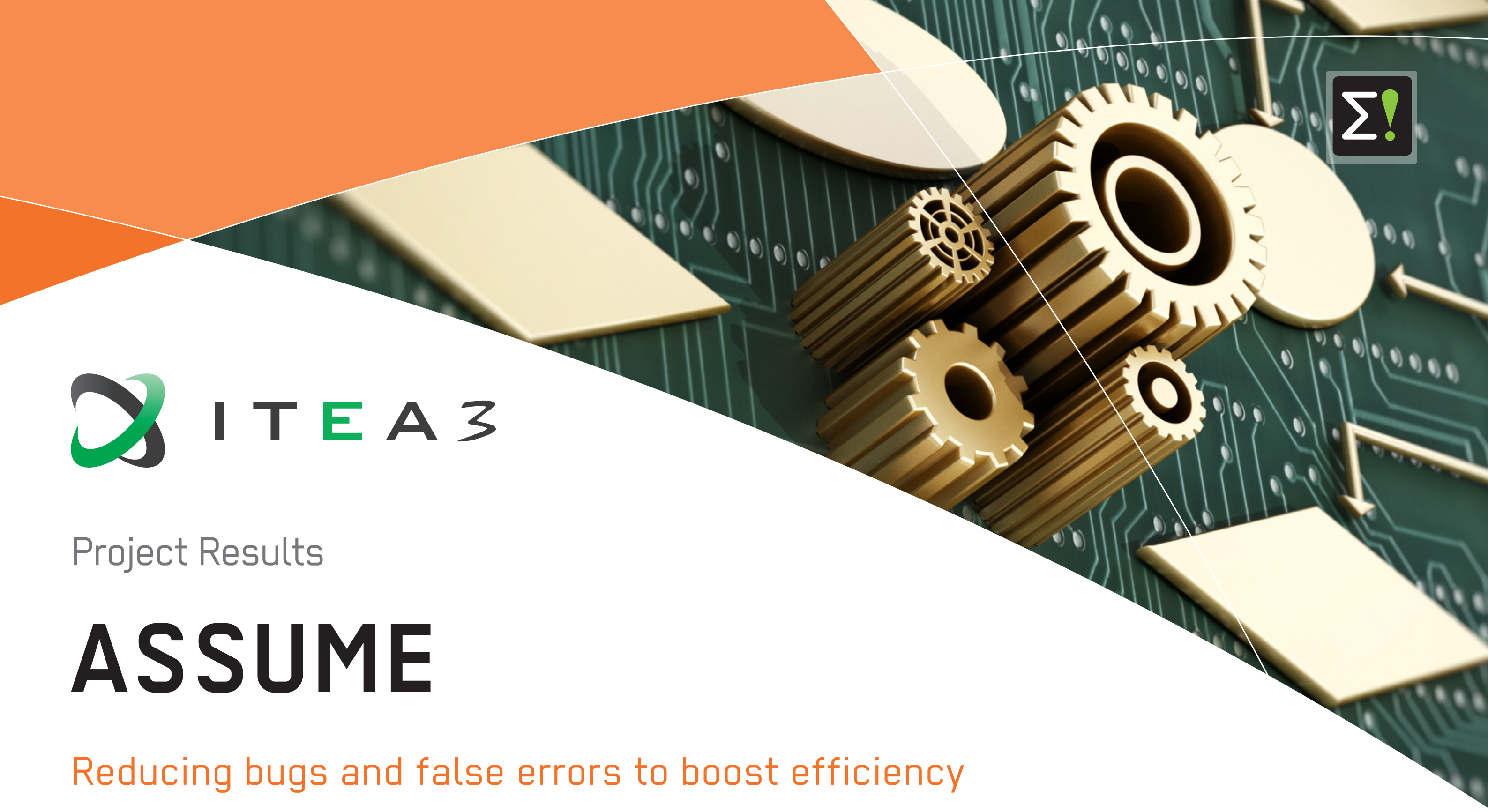


Project Results

ASSUME

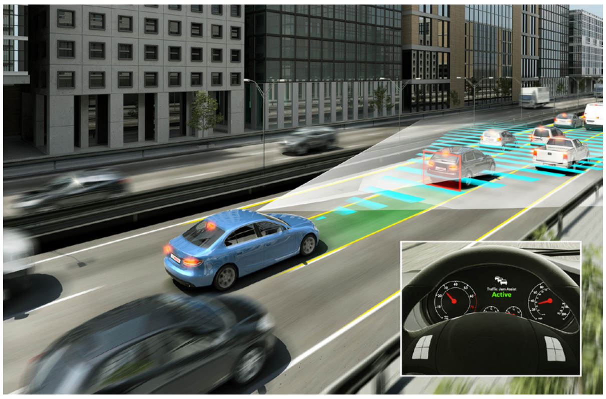
Reducing bugs and false errors to boost efficiency

EXECUTIVE SUMMARY

The ITEA project ASSUME (Affordable Safe & Secure Mobility Evolution) deals with the demands of multi-core technologies in highly automated systems. It assures safety-relevant, performance-critical functionality and is traceable throughout the development process via the efficient verification of large systems.

PROJECT ORIGINS

Future mobility solutions will rely on smart components that continuously monitor the environment and assume more and more responsibility for convenient, safe and reliable operations. The software development challenge is thus to identify and exploit opportunities for concurrency so that reliable and predictable behaviour can be guaranteed. The inherent problem here is that it takes an excessive amount of time for tools to find bugs and false errors. The ASSUME project set out to tackle this issue and thereby boost tool performance and efficiency.



Bosch, Traffic jam assist

The ASSUME consortium – comprising industry players including OEMs and SMEs, tool and service providers and research institutes – set out to provide new tools, standards and methodologies for the efficient construction and synthesis of embedded systems, as well as new algorithms for integration in exploitable tools. The technology focus concerned formal compiler verification, correct real-time implementation for parallel applications and specific attention to hardware modelling. The industrial use cases in the automation and avionics fields, contributed by the industrial partners, provided the foundation for technological innovation.

TECHNOLOGY APPLIED

The project made substantial progress in both improving existing tools and developing new tools, bringing these together in an entire chain so that the benefits of the results achieved by one tool can benefit other tools and their development. These tools (and development leads) included:

- M-XRAY, Metrics for model refactoring support (MES);
- PLAATO, fault tolerance and safety of architectures (TNO);
- SDF³, performance analysis of dataflow models (TU/e);
- RTANA2, timing analysis of real-time system models (OFFIS);
- C-SAPP, analysis of hardware-dependent software (FZI).

Other tools that were improved or developed for static analysis of source code for concurrency errors were Gropius (University of Kiel), Goblint (TU Munich) and Astrée (AbsInt), while KoçSistem and Arçelik developed EmbedSanitizer and Ericsson created the DRDCheck Hybrid tool for race detection at runtime.

A few examples of the new tools developed serve to illustrate some of the specific benefits and key performance indicators, such as the PLAATO Platform Architecture Analysis Tool that focuses on evaluating fault-tolerance and safety of hardware and software architectures. Incorporating an interface with Enterprise Architect and Matlab, it computes a fault tree, failure rates and minimal cut sets on the basis of input (function + hardware description in diagram form). It also provides support for different software failure modes. This tool chain analysis can be integrated in the development chain using model-based systems and safety engineering, as no other tools are currently available that completely support this engineering process. Another new tool is the DRDCheck Hybrid for race detection during runtime in Java. Based on DRDCheck, an open-source dynamic race detector, this tool not only boosts performance by a factor of 10 but also significantly reduces false positives. C-SAPP, meanwhile, contains a metamodel that facilitates the analysis of low-level embedded software and the ability to handle millions of lines of code. False alarms are reduced through knowledge of hardware characteristics and timing constraints, while hardware-related runtime errors are addressed by analysis.

MAKING THE DIFFERENCE

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, the project's goal has been achieved. Thanks to the creation of a tool chain, ASSUME has enabled the use of results between different tools. This level of interoperability has also been boosted by the implementation of Simulink/Stateflow analysis of 60% of the modelling language and the exchange format specification's capture of the results of 75% of the analysis tools. Interoperability and cooperation are ultimately enhanced between different market players.

The list of measurable achievements produced by ASSUME is impressive: an increase of 50% in the performance (run-time) of analysis tools, a 60% reduction of spurious warnings in analysis tools for single core, and an almost 100% reduction of error classes in single core analysis. The reduction of false positives in analysis tools for concurrent software has been significant and the traceability of run-time errors back to the model level has had a success rate of 80% or more. The 40% cut in effort to inspect runtime errors in a typical industrial setting has had a considerable positive knock-on effect in terms of costs.

Project collaboration ensured that the tools (both newly developed and improved) focused on solving the problems of industrial partners, such as Bosch, Daimler, Scania, NXP, Ford Otosan, Arçelik and Airbus. For example, Scania implemented an integration platform for lifecycle traceability based on open standards. The academic partners also developed new ideas and tools in partnership with tool vendors, generating spin-offs and subsequent sales of tools to their industrial partners. Up to 700 developers within the industry partners currently use one or more tools developed in the ASSUME project.

MAJOR PROJECT OUTCOMES

Dissemination

- More than 20 publications (e.g. PLDI 2017, DSD 2018, CAV 2017, NETSYS 2016 best paper, AVOCS 2017 best paper)
- Several presentations/demos at conferences/fair (e.g. WCET 2018, CTI ISO 26262 2017, SAFECOMP 2017, CTI ISO 26262 2017, ERTS 2016, Embedded World 2016, DATE 2016)

Exploitation (so far)

New products (17 in total):

- Avionics real-time tool-flow full integration
- Requirement coverage measurement using SUP
- Model specification and extraction
- High Performance Traceability Solver
- BTC Embedded Tester adapted to MES Quality Co

New services:

- Application of Demonstrator to Series Project
- FZI Open House 2017

New systems:

- Automated Reasoning Support for Large Models

Standardisation

- Static Analysis Exchange Format Draft
- Pushing ASSUME's Static Analysis Exchange format in OASIS/SARIF

Spin-offs

- QPR Technologies
- DataFrame

ITEA is a transnational and industry-driven R&D&I programme in the domain of software innovation. ITEA is a EUREKA Cluster programme, enabling a global and knowledgeable community of large industry, SMEs, start-ups, academia and customer organisations, to collaborate in funded projects that turn innovative ideas into new businesses, jobs, economic growth and benefits for society.

ASSUME
14014

Partners

France

Airbus
École Normale Supérieure (ENS)
Esterel Technologies
Inria
Kalray SA
Safran Aircraft Engines SAS SNECMA
Safran Electronics & Defense Sagem
Sorbonne Université
Thales

Germany

AbsInt Angewandte Informatik GmbH
Assystem Germany GmbH
BTC Embedded Systems AG
Daimler AG
FZI Forschungszentrum Informatik
Karlsruhe Institute of Technology (KIT)
Kiel University
Model Engineering Solutions GmbH
OFFIS
Robert Bosch GmbH
Technical University of Munich

Netherlands

Eindhoven University of Technology
NXP Semiconductors Netherlands BV
Recore Systems BV
TNO
University of Twente
VDL Enabling Transport Solutions
Verum Software Tools BV

Sweden

Arcticus Systems AB
FindOut Technologies AB
KTH (Royal Institute of Technology)
Mälardalen University
Scania

Turkey

Arçelik
Ericsson Ar-Ge
Ford Otosan
Havelsan
KoçSistem
UNIT Information Technologies R&D Ltd.

Project start
September 2015

Project end
December 2018

Project leader
Wolfgang Köpf, Daimler AG

Project email
wolfgang.w.koepf@daimler.com

Project website
http://assume-project.eu/