Project Results

Meeting the challenge of verifying embedded software

Static-analysis techniques overcome limitations of process-based quality assurance

The ES_PASS project set out to overcome the limitations of current quality-assurance which is exclusively focused on complying with a qualified process. It has extended the use of static-analysis technologies for product-based assurance into the industrial processes for developing safety-critical systems. The project adapted and enhanced static-analysis tools and services, and demonstrated their use in key domains such as aerospace, automotive and rail transportation.

Traditional software quality-assurance processes based on compliance with a qualified process are now reaching their limits. Current verification-and-validation methods, mainly based on testing, are difficult to scale up at acceptable costs for future large and complex systems. A new and complementary approach is required that focuses on the product rather than the process.

Static-analysis techniques are the most promising approach to support the required shift from process-based to product-based assurance at European level. Static analysis represents a strong opportunity for Europe to guide and take the lead in this evolution, as European academic research in static-analysis techniques has an unequalled level of excellence. However, development methodologies and services must be adapted to support deployment of these techniques.

OVERCOMING LIMITATIONS OF CURRENT TOOLS

Most current verification and testing tools rely on techniques introduced in the 1980s or early 1990s. While they offer mature technology, they are no longer powerful enough to take up the challenge of validation and verification of today's complex embedded software.

Static-analysis techniques have now matured and offer a formal means to enhance the overall quality of software while reducing verification-and-validation costs, and remaining compatible with the usual skills and practices of industry. Moreover, they have already been implemented in tools, and the market is now ready for the adoption of such techniques.

Development of safety-critical products in a range of key European domains – such as aeronautics, automotive, space and railways – can undoubtedly benefit from such an approach in terms of cost effectiveness and reduced time to market. Static analysis also offers strong advantages for non-safety critical applications, where a software failure may have strong impacts on assets or the environment.

Static analysis was first used by Airbus to verify embedded flight software, and recently in Space transportation; it is now recommended for automotive and railways control software.

ES_PASS
(ITEA 2 ~ 06042)

Partners
AbsInt
Airbus
CEA/LIST
Daimler
EADS Astrium
EADS Innovation Works
ENS
Esterel Technologies
FéRIA (IRIT and ONERA)
Fraunhofer FIRST
GTD
IFB
PSA
Continental
Saareland University
Technical University Munich
Thales Avionics
Thales Transport
UPM

Countries involved
France
Germany
Spain

Project start
May 2007

Project end
November 2009

Contact
Project leader :
Maurice Heitz, CS Systèmes d'Information
Email :
maurice.heitz@c-s.fr

Project website :
www.es-pass.org

Project Results

MAXIMISING THE BENEFITS OF STATIC ANALYSIS

ES_PASS set out to promote the use of static-analysis tools to verify properties in code produced by software developments. At the same time, it supported the adaptation of current engineering practices to maximise the benefits of static-analysis techniques.

Key project results include

- Enhanced static-analysis tools and development methods;
- Improved engineering processes integrating static-analysis techniques;
- Dissemination of static-analysis technology in European and global industry; and
- The build up of a European static-analysis community

The project extended static-analysis techniques and integrated them into tool suites such as Absint A^3 and Esterel SCADE suite to ease access and use. Moreover it showed that static-analysis techniques represent a promising solution to major new issues that have arisen with new automated software development methodologies:

- introduction of commercial off-the-shelf (COTS) components and
- use of automatically generated software,

since static-analysis techniques only require the final code – the product – and no other development artefact.

PUSHING THE SPREAD OF THE TECHNOLOGY

ES_PASS is now serving as a driving force for this market. Its results address a fast-growing market in test automation. It is set to become a key driver as the project focused on the most dynamic category of verification tools.

The active static-analysis community that has resulted from the ITEA project will push the spread of the technology in Europe. The project has also extended the static-analysis tools of European editors – enabling them to gain a competitive advantage over US competitors. It has also helped develop new competences in static-analysis technology and supported its use, which will create associated new jobs.

Most importantly, the project is bringing added value and competitive advantage to the European software industry as whole in terms of quality assurance, testing and safety.

Major project outcomes

DISSEMINATION

- 53 publications
- Three technical workshops at European level
- Three presentations at conferences – annual ITEA Symposium

EXPLOITATION

- Industrialisation of one academic tool: ASTREE integration into Absint A^3
- Two new products: Absint A^3 and CEA Frama C
- Enhancements to existing static analysis products, including Fluctuat, Caveat, Absint suite and SCADE suite
- Application within engineering processes intended for internal use by end-users

PATENTS

- One patent application in preparation

STANDARDISATION

Contributions for static analysis techniques applicability and standards evolution:

- Aeronautics: DO-178B applied; DO-178C in progress
- Automotive: no standards yet; ISO 26262 in progress
- Space: ECSS-E-40 applied; new version in progress
- Railways: CENELEC EN 50128 applied; new version in progress

ITEA 2 Office
High Tech Campus 69 - 3
5656 AG Eindhoven
The Netherlands
Tel : +31 88 003 6136
Fax : +31 88 003 6130
Email : info@itea2.org
Web : www.itea2.org

ITEA 2 – Information Technology for European Advancement – is Europe's premier co-operative R&D programme driving pre-competitive research on embedded and distributed software-intensive systems and services. As a EUREKA strategic Cluster, we support co-ordinated national funding submissions and provide the link between those who provide finance, technology and software engineering. Our aim is to mobilise a total of 20,000 person-years over the full eight-year period of our programme from 2006 to 2013.

ITEA 2-labelled projects are industry-driven initiatives building vital middleware and preparing standards to lay the foundations for the next generation of products, systems, appliances and services. Our programme results in real product innovation that boosts European competitiveness in a wide range of industries. Specifically, we play a key role in crucial application domains where software dominates, such as aerospace, automotive, consumer electronics, healthcare/medical systems and telecommunications.

ITEA 2 projects involve complementary R&D from at least two companies in two countries. We issue annual Calls for Projects, evaluate projects and help bring research partners together. Our projects are open to partners from large industrial companies and small and medium-sized enterprises (SMEs) as well as public research institutes and universities.

Σ! 3674

ES_PASS
(ITEA 2 ~ 06042) October 2009