

Project Profile

Improving safety-critical engineering processes

Integrating static-analysis techniques into quality assurance processes for the transport industries



ES_PASS targets the needs of multi-domain safety critical systems

As current software quality-assurance processes reach their limits, the ES_PASS project is setting out to target the awareness, improvement, integration, deployment and dissemination of product-based static-analysis verification techniques for quality assurance in safety-critical embedded systems engineering. A range of industrial sectors is concerned, particularly aerospace, automotive and rail transport.

Conventional software quality assurance based on compliance with a qualified process is now reaching its limits. Moreover, current verification and validation methods that are mainly based on testing are almost impossible to scale up at acceptable costs for future systems. Therefore, a new and complementary approach is required, focusing on the product itself rather than the process involved.

Static-analysis techniques appear to be the most promising candidates to support this paradigm shift from process-based to product-based quality assurance at the European level. Two convincing arguments support this argument:

1. The excellence of European academic research in this area; and
2. The maturity of these techniques, which are already implemented in tools.

ES_PASS considers that static analysis represents a strong opportunity for Europe to guide and take the lead in this evolution.

The market for verification tools is now ready for the adoption of static-analysis techniques. So, the ITEA2 project is expected to serve as a driving factor for this critical market.

REACHING TEST LIMITS

Already, some safety and security problems cannot be detected by either exhaustive tests or exploring partial and imperfect models. In addition, some required properties can hardly be checked at all because the conditions for control and observation are simply not reproducible. In most cases, verification and validation usually requires the creation of costly additional hardware and software.

In this situation, static-analysis techniques now represent mature formal means to enhance the overall quality of software and reduce verification and validation costs, while remaining compatible with the usual skills and practices in industry.

Static-analysis techniques also represent a promising solution to tackle two major new issues: the introduction of commercial off-the-shelf (COTS) components and the use of automatically generated software. The key benefit is that static-analysis techniques only require the final code – the product; no other development artefact has to be considered.

The resulting cost effectiveness, reduced time to market and enhanced safety represent key success factors for safety-critical products in aeronautics, automotive, space and railways sectors. But these techniques may also have strong benefits for non-safety critical applications, where a software failure may have strong impacts – on assets, the environment, etc. – and for which current practices in safety-critical domains are too costly.

ES_PASS (ITEA 2 ~ 06042)

.....

■ Partners

AbsInt
Airbus France
Astrium
CEA LIST
Continental Automotive
CS Systèmes d'Information
Daimler
EADS Innovation Works
Ecole Normale Supérieure
Estrel Technologies
Fraunhofer FIRST
GTD
IFB
INPT-IRIT
ONERA
PSA
Saarland University
Technical University of Madrid
Technical University of Munich
Thales Avionics
Thales Transportation

■ Countries involved

France
Germany
Spain

■ Project start

September 2007

■ Project end

September 2009

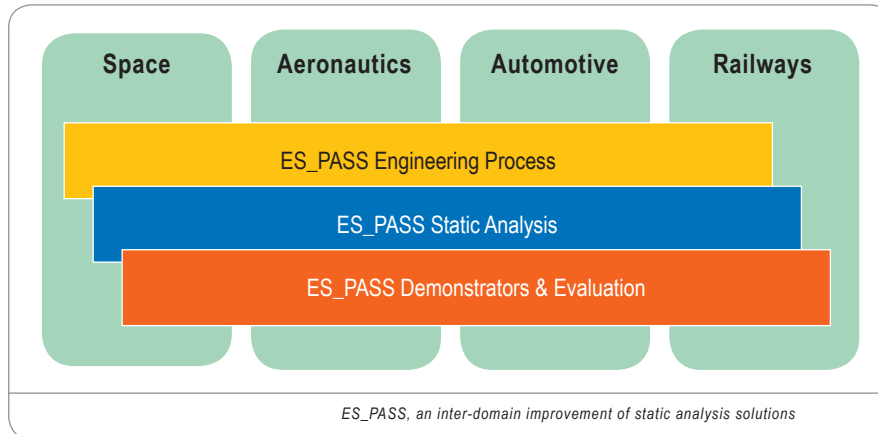
■ Contact

Project Leader :
Pierre Vielcanet
CS Systèmes d'Information, France

Email :
pierre.vielcanet@c-s.fr

Project website :
www.es-pass.org

Project Profile



ES_PASS is therefore located at the meeting point of three converging axes:

1. A strong research and development effort dedicated to the improvement of existing engineering methodologies and certification processes towards the integration of static-analysis techniques;
2. A strong research and development effort dedicated to the improvement of existing state-of-the-art static-analysis techniques and tools towards a better adequacy with industrial needs using domain-specific properties; and
3. A strong demonstration effort dedicated to the evaluation of these new processes, techniques and tools in real situations taking into account domain-specific improvements.

SETTING MAJOR GOALS

The ES_PASS strategy relies on the following major goals to support the introduction and dissemination of static-analysis techniques:

- **Ensuring the dissemination** of static-analysis techniques and tools from the academic domain to the industrial sector, and from the consortium members to the entire community of dependable systems – for example in the medical, nuclear and telecommunications fields;
- **Preparing the ground for the actual adoption** of static analysis in industry by improving existing techniques and tools to account for the various needs and practices in the domain of safety-critical real-time systems and, reciprocally, proposing adaptations to existing industrial processes and development standards to ‘host’ these techniques and tools; and

- **Evaluating the benefits** of static-analysis techniques and tools in various real industrial contexts.

OFFERING MAJOR BENEFITS

The major results of the ES_PASS project are expected to be:

- Improved engineering processes integrating static analysis in industrial domains where confidence in the quality of software is fundamental and must be shared with certification authorities; and
- Improved static-analysis methods and tools covering a spectrum of applications and properties – such as timing properties and floating-point calculation accuracy – compatible with the industrial expectations. This includes the development of domain-specific, parameterised and locally specialisable static program analysers.

Evidence of the suitability of these methods and tools will be obtained from real-life experiments. This suitability will be estimated according to four main criteria: compliance with the dependability objective; compatibility with industrial standards such as Aerospace DO178B, Automotive IEC 61508 and Railway Cenelec EN50128; cost effectiveness; and industrial applicability.

Overall, success in the ES_PASS project will strengthen European scientific and technological excellence through a closer co-operation between research capacities and end users. It will support the build-up of engineering know-how and good practices by cross-fertilisation between research and industrial teams. And it will offer new high added value job opportunities, balancing the increasing offshore outsourcing of low level testing.

ITEA 2 Office

High Tech Campus 69 - 3
5656 AG Eindhoven
The Netherlands
Tel : +31 88 003 6136
Fax : +31 88 003 6130
Email : itea2@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 2007