ITEA 2

INFORMATION TECHNOLOGY FOR EUROPEAN ADVANCEMENT

ES_PASS Embedded SW Boarding Pass

INNOVATION REPORT

Static-analysis techniques ensure product-based quality assurance for safety-critical applications

Project leader: Maurice Heitz (CS Systèmes d'Information)

The ES_PASS project set out to overcome the limitations of quality-assurance systems that focus on embedded software complying with a qualified process. It has developed static-analysis technologies to ensure product-based quality assurance in industrial processes needed for safety-critical applications. The project adapted and enhanced methodologies and services to improve overall software quality while reducing verification and validation costs. Use was demonstrated in key domains such as aerospace, automotive and rail transportation. The success of the project is already serving as a driving force for the establishment of a European static-analysis community and marketing of the necessary verification tools.

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.

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 – essential as the use of embedded software is expected to grow by a factor of 10^6 over the next 40 years. A new and complementary approach was required that focused on the product – the software code itself – rather than the process.

Static-analysis techniques are the most promising alternative 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 had to be adapted to support deployment of these techniques.

The ES_PASS project was therefore started by Airbus France together with Ecole Normale Supérieure (ENS), the academic institution which developed the initial static-analyser prototype. Technology providers – tool editors and research organisations – and industrial end users joined to obtain the necessary support for full use of the new approach. ITEA played a major role in helping to define the original objectives of the project and enabling the partners to obtain national funding.

ITEA 2

INFORMATION TECHNOLOGY FOR EUROPEAN ADVANCEMENT

ES_PASS Embedded SW Boarding Pass

INNOVATION REPORT

Overcoming limitations of current tools

Most current verification and testing tools still rely on process-based techniques introduced in the 1980s. While they offer mature technology, they are no longer powerful enough to take up the challenge of verification of today's complex and safety-critical embedded software.

Static-analysis techniques have now matured and offer a formal means to enhance the overall quality of software and reduce verification-and-validation costs, while 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 domains – including aeronautics, space, automotive and rail – 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 a strong impact on assets or the environment.

Maximising the benefits of static analysis

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

Activities in the project included ensuring the technology transfer of static-analysis tools and techniques from academic to industrial sectors, and from the consortium partners to the entire community of highly dependable systems – such as in the medical, nuclear, transport, aerospace and automotive fields.

The ES_PASS project prepared the ground for the full-scale adoption of static analysis in industry by improving existing techniques and tools to account for the various specific needs and practices in the development of safety-critical real-time systems. In addition, it proposed adaptations of existing industrial processes and development standards to 'host' static-analysis techniques and tools.

Demonstrating in practice

Suitability of the methods and tools was demonstrated in a series of applications, and evaluated according to four main criteria:

1. Compliance with the dependability objective;
2. Compatibility with industrial standards such as Aerospace DO178B, Automotive IEC 61508 and CENELEC Railway EN50128;
3. Cost effectiveness; and
4. Industrial applicability.

Key results include:

- *Enhanced 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 requirements. This included the development and configuration of domain-specific, parameterised and locally tailorable static program analysers;
- *Improved engineering processes* integrating static analysis in industrial domains where confidence in the quality of software achieved is fundamental and must be shared with the relevant certification authorities; and
- *Dissemination of static-analysis technology* in both European and global industry.

INNOVATION REPORT

The project led to enhancements in static-analysis tools and their integration into tool suites such as Absint A^3 (AbsInt Advanced Analyzer) and the Esterel SCADE Studio to ease access and use. Moreover, it showed that static-analysis techniques which only require the final code represent a promising solution to major issues that have arisen with new automated software development methodologies, such as: introduction of commercial off-the-shelf (COTS) components; and use of automatically generated software

Pushing the spread of the technology

ES_PASS is now serving as the motivator for the static-analysis 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 project will push the spread of the technology in Europe. The outcomes of ES_PASS have made it possible for European editors to extend their static-analysis tools – enabling them to gain an advantage over US competitors. It has also helped develop new competences in static-analysis and supported its operation in industrial practice. It will thus create new service demands and jobs.

In addition, the success of ES_PASS is helping strengthen European scientific and technological excellence through a closer co-operation between research organisations and industrial end users. This will support the build up of static-analysis engineering know how and good practice by cross-fertilisation between researchers and industrial developers.

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

More information: http://www.es-pass.org/