ITEA
INFORMATION TECHNOLOGY FOR EUROPEAN ADVANCEMENT

Spices

INNOVATION REPORT

Ensuring fast verification of mission-critical embedded systems using model-based development/ engineering

Project leader: Vincent Seignole (Thales)

The SPICES project developed modelling, verification and code-generation tools for fast verification of software designs in mission-critical applications such as avionics, aerospace and communications. The project made use of two standards: the architecture analysis and design language, which enables precise modelling of embedded real-time systems, and Object Management Group component technology. The resulting model-driven development/engineering approach enables early analysis of systems and ensures consistency between software architecture and implementation structure in terms of component technology. The tools are being integrated in an open-source Eclipse platform.

Overall engineering efforts for embedded software have risen markedly with the increasing complexity of mission-critical systems. Design costs are significantly higher for systems with certification constraints – such as in the avionics sector to meet DO178B Airborne Systems and Equipment Certification criteria. When developing and integrating such systems, the cost of fixing design problems found late on is very high.

However, there is a lot of room in such applications to cut costs by making integration more predictable. SPICES set out to verify design decisions as soon as they are made, and guarantee consistency between design decisions and the actual system.

Assembling critical mass of experts

The ITEA project brought together experts in analysis, verification and software engineering of real-time and embedded systems from the avionics and communications sectors to reduce the costs and efforts of building mission-critical systems. It developed use of model-driven engineering based on the architecture analysis and design language (AADL), making it possible to conduct verification and analyses early in the design process, and to provide support for integrating software subsystems of critical software-intensive embedded capabilities.

INNOVATION REPORT

The project was initiated by a small team of industrial partners in the avionics and communications domains that identified the main principles for approaching the problem of integration of mission-critical system. Research organisations and tools providers joined because of their interest in the research opportunities and tools development, and the ability to reach a critical mass and so impact standardisation.

Partners ranged from large industry and major research centres to small and medium-sized enterprises (SMEs). The particularity of the industrial partners is that they mainly make business out of contracts, instead of providing offers to a large consumer base. These partners dealt with demonstrators and technology experiments, sometimes building the technology required themselves. The latter aspect was also important in initial stages of technology definition, for the purpose of direct relevance and usability.

The research centres and SME partners focused on either reusing their background on tools to augment their functionality with new features or make them match the standards selected by the project. Beyond project-wide co-operation, more focused collaborations were established to provide greater in-depth focus on some challenges.

Co-operation in the SPICES project made it possible to achieve an adequate size to gather partners of different natures, and to propose an appropriate balance between addressing current industry problems and mid-term ones by experimenting with promising techniques needing additional steps to maturity.

Building on established standards

AADL is an architecture description language dedicated to embedded, critical, real-time systems in many domains, including avionics, space, transportation and industry. It enables the precise description of software components such as process, thread and data, and the execution platform supporting them – processor, bus, memory, etc. It also enables the definition of extensions to support additional information and use of AADL into systems and software development processes.

SPICES built on AADL and the CORBA Component Model (CCM) standard component- based technology from the Object Management Group (OMG) to set up a spectrum of innovative tools covering several types of activities. These included: verifying real-time constraints; state exploration; estimating performance; power consumption analysis based on high-level designs; and determining worst-case execution time.

It also extended the capabilities of advanced component-based technologies towards new targets – such as reconfigurable hardware and partitioning kernels used in avionics or secure systems.

The technological developments were validated in a series of demonstrators that provided an ideal framework to gain experience in the use of tools early in the development cycle. These included:

- Software radio;
- Avionics flight warning system;
- Use of AADL model-creation and simulation tools in the space domain;
- Avionics software in an air traffic control application; and
- Use of AADL to model a direct memory access (DMA) subset in avionics hardware.

INNOVATION REPORT

High level of confidence required

While project results do not bring new features as such to end users of the systems involved, the SPICES approach facilitates and speeds the creation of high-integrity systems. Companies adopting this approach can thus deliver better product quality at lower cost.

The markets targeted initially are avionics, aerospace and radio communications. Such domains require a high level of confidence in the final system. In addition, with the increased use of software in all areas of industry, there is a significant trend to being able to support high-integrity developments in other domains – such as healthcare systems. The main challenge lies in the ability to provide adequate cross-industry solutions.

Today's market for tools in the area covered by SPICES is fragmented. A key shift from the current market offer is the perspective of open source for a substantial number of tools, which will contribute to democratisation of use of the techniques promoted by the project.

Initial applications through consultancy and support

While the topic of SPICES is strategic, the appropriate business model is more delicate. The traditional software-tool vendor model may be difficult to sustain in the medium term. SPICES is following a long-term trend; however adopting such technologies for mission-critical systems in a generalised way will still necessitate time. This is due to the inherently intricate development process for mission-critical systems and the peculiarities of each product-line candidate.

The short-term business opportunities of the project results are in the area of consultancy and support to industries to introduce such techniques, and identify the technologies integration path with them. Further opportunities will be at the level of tool evolution and integration into industrial developments at large.

A major outcome of the SPICES project has been support for a proactive European stance in worldwide standardisation efforts in the field of embedded software engineering.

More information: http:// www.spices-itea.org