

New programming standard for safety-critical embedded systems

Introduction

Demand for greater intelligence and higher integrity in real-time components is increasing in the devices we depend on every day. As these embedded systems become increasingly ubiquitous, it's essential that there be an architecture neutral platform that allows components to be designed and to operate as high-integrity systems utilizing a broad range of hardware architectures.

The project has created a new real-time middleware platform that supports the development of architecturally neutral, high-integrity real-time systems (ANRTS), addressing both hard and soft application timing constraints and designed for safety-critical as well as business-critical and ambient intelligence applications, while delivering the platform flexibility inherent to Java™ based systems.

The HIJA environment specifically supports the development of ANRTS applications for safety-critical systems that must be verified as functionally correct. These applications can be deployed in a variety of operating environments and meet the needs of users and authorities requiring applications to be certified performing correctly.

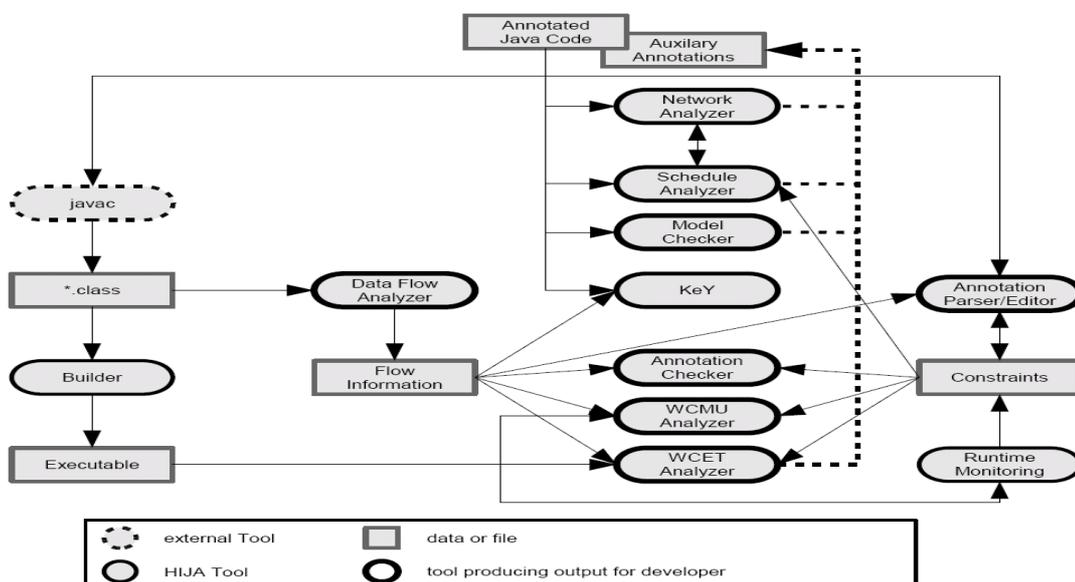
Standardization Challenge

The HIJA project was focused in the area of *Embedded*

Systems under the European 6th Framework Programme. The project faced the standardization challenge of developing new features and revisions to the well-established standard Java programming language that would enable a new generation of real-time safety-critical systems for applications including avionics, medical, energy, and transportation. One of the project research goals was to provide a framework that maintains the advantages of Java including portability, interoperability, object orientated design, and access to a large tool and library base, while providing a revised programming language reference that would allow Java based applications to be formally certified by government authorities for the most demanding safety-critical systems.

Standardization Path

The HIJA project included specific tasks to address standardization and in particular to participate in the Java Community Process programme, which establishes the formal specifications and revisions to the Java programming language. The Java Community Process is an open, participative process to develop and revise the Java technology specifications, reference implementations, and test suites. It involves over 700 members and seeks to foster the evolution of the Java programming platform in cooperation with the international Java developer community. A set of action steps was identified for the HIJA project to utilise the



existing infrastructure of the Java Community Process to standardize HIJA project results.

Step 1: Participate in ongoing standardization processes

From the start of the project the HIJA partners were active within the Java Community Process and used their participation to become both familiar with the standardization processes and to establish contacts and interact with developers as well as large end-users of embedded systems technologies for safety-critical systems.

Step 2: Understand existing features and validate proposed changes

The project invested resources to fully understand the features already implemented within the existing Java standards and to explore every possibility of supporting safety-critical requirements without any changes to existing specifications. Consultations with others outside of the HIJA project were used to validate amongst the Java development community that no techniques or workarounds to address safety-critical requirements using existing standard were overlooked, and the identified requirements of safety-critical systems were common to multiple industries.

Step 3: Build constituency for revisions

The project recognised that Java was a well-established standard and that changes might be resisted unless there was clear industry needs and new opportunities for the Java standard to be even more widely adopted. The project built a constituency of support for revisions to the standard by creating awareness of Java as a new and promising development environment for safety-critical real-time systems, while at the same highlighting the new requirements and implied changes needed to make Java genuinely suited for these new types of applications.

Step 4: Establish technical consensus for revisions

Demand for revisions to the Java language supporting safety-critical systems would not necessarily mean HIJA project results being adopted as standard unless the HIJA project could demonstrate the project results were the best technical solutions. The project established a team of experts to work within the Java development and user community to discuss and evaluate technical alternatives and to demonstrate the revisions from the project were the best technical choice and aligned with established Java principles.

Standardization results

The HIJA project has been successful in creating a new working group within the Java Community Process programme that includes HIJA project partners and other organisations from around the world interested in Java for safety-critical embedded systems. The new group known as the JSR 302 has voted to adopt the HIJA project results as the basis for a new safety-critical standard for the Java programming language that is expected to receive formal approval within the Java Community Process in 2007. The availability of a new industry standard specification is expected to accelerate the take-up of the real-time Java tools and technologies developed within the HIJA project.

Key Learning Points

The experiences and insights gained by the HIJA partners that may be of use to other projects include the following:

- Initiate the standardization actions early in the project. The HIJA project needed to work within ongoing standardization processes and some time was needed to synchronise the project schedules with the activities of the standards organisation. Waiting until later in the project would have eliminated the opportunity of making significant progress towards standardization while the project was operational.
- Provide sufficient resources to address technical issues that might arise during the standardization process. Several competing alternatives were submitted as part of the selection and consensus process and substantial resources were needed to understand and document the advantages provided by the HIJA project results.
- Include multiple project partners in standards making process. The different roles and perspectives of the partners involved created greater motivation for the need to revise the existing standard and greater support for the solutions being proposed by the project.
- Invest in collaborating with organisations involved in standards outside of the project consortium. The external validation of the HIJA technical proposals and additional inputs received not only helped in strengthening the technical specifications and achieving success in standardization, but they also improved the technical results developed by the HIJA project and expanded their applicability to a broader range of applications.