The QSL platform at LORIA

Mohamed El Habib, Claude Kirchner, Hélène Kirchner,
Jean-Yves Marion, and Stephan Merz
LORIA, Nancy, France
http://qsl.loria.fr/

April 30, 2003

Abstract

The QSL project aims at the development of concepts, methods, techniques, and tools to increase the reliability and the quality of software-intensive systems. Within this project, we are anticipating a platform of tools for validation and verification that ensures their availability, includes documentation and case studies, and eventually intends to foster the cooperation of different teams using different tools on common development projects.

1 The QSL project

The QSL (*Qualité et Sûreté des Logiciels*) project carried out at the LORIA laboratory in Nancy supports the development of concepts, methods, techniques, and tools to increase the reliability and the quality of software-based systems in a broad sense. Roughly a dozen teams within LORIA contribute to the project by pursuing operations on subjects such as the analysis of cryptographic protocols, verification by rewriting, the integration of UML notation and the B method of formal development, extreme programming, proof-based development of embedded systems, analysis of the implicit complexity, or the generation of proofs and counterexamples in substructural logics; some of these operations involve teams from other French laboratories. The project was launched in 2000 and is expected to continue in its present form until 2006.

A specific and federating goal of the QSL project is the creation of a platform of relevant tools, developed either within LORIA (such as ELAN [1] or CASRUL [2]) or elsewhere. During a first phase, the platform is intended to ensure the availability of these tools at a one-stop Web portal and to serve as a repository that provides associated documentation, course material, and case studies. Over a longer term, the platform is intended to serve as a nucleus to enhance the ability to carry out joint development projects by teams who are geographically distributed and use different tools, possibly based on different logical theories.

2 The current state of the QSL platform

A preliminary version of the QSL platform is accessible at the URL http://plateforme-qsl.loria.fr/. It presently hosts around 30 tools and libraries. For every tool, it provides a short summary and overall administrative information, including a classification according to the ACM categories, home URLs, installation instructions, examples of use, and a FAQ. This information can be accessed via a Web interface; similarly, the tool administrator, who does not need to be based at LORIA, can enter and update the required information over the Web and is responsible for its completeness and maintenance. Technically, the QSL platform is based on a 3-tier architecture model. The lowest tier uses the PostgreSQL database, which is freely available and quite powerful, allowing to check referential integrity. The middle tier is built around PHP scripts that access and manipulate PostgreSQL data and the server. The presentation tier is provided by the Apache Web server that allows users to connect to the QSL Platform.

In parallel, the tools are installed on a server that currently makes them available to users at the LORIA site. We are working on an interface that will make tools running in batch mode accessible over the Web, based on servlets (using JavaServer Pages) that provides a restricted interface, thus guarding our site against possible security breaches.

3 The intended evolution of the QSL platform

The version of the platform described in section 2 is but a first step towards the development of a useful repository for verified system development. We foresee its evolution along two main axes that we now describe.

3.1 A repository of tools and case studies

We hope that the platform will evolve into a one-stop Web portal as a repository of tools and developments relevant to the theme of quality and reliability of software-intensive systems. In this way, we aim at hosting not only tools and libraries, but also development projects and case studies, and this aspect is most closely related to the QPQ project. However, our focus is not primarily on archiving and peer review of deductive components themselves, but on building a repository of know-how in their application.

This axe should lead to a presentation of validation and verification methods and tools that will hopefully attract new users as well as allow for a comparison between different approaches. As an opportunity of disseminating formal methods, we encourage academics to make relevant course material available. Students will thus be able to use the QSL platform as a learning center that offers online courses.

3.2 A platform for cooperation

Based on a PROOFFORGE concept, we envision an environment that assists the cooperative development of proofs and verified components. Cooperation can be foreseen along two dimensions: firstly, joint projects can be established between geographically distributed teams. It will be even more challenging to enable cooperation involving different tools, possibly based on different logico-mathematical theories. While cooperation can obviously greatly enhance the capabilities of deductive software components (as an example, let us mention the ongoing work around the integration of COQ [3] and ELAN [1]), it is non-trivial to issue a correctness certificate based on certificates coming from different tools. (In the example mentioned above, the concept of "deduction modulo" offers a sound basis for a combined certificate.) In general, we can certainly not expect a "silver bullet" that would make underlying incompatibilities disappear. We plan to build upon the achievements of initiatives such as the MathWeb [4] and OpenMath [5] projects, on more sharply focused projects such as SAL [6] and VeriTech [7], and of course on the QPQ project.

¿From a technical point of view, the community should embrace the development of components and APIs to replace the prevalent development of stand-alone tools. Moreover, standardized middleware is required to facilitate communication between components. However, beyond these technological issues we also foresee the need for research into concepts and languages for user-assisted cooperation in order to tackle problems that are beyond the reach of fully automatic tools. The QSL platform is intended as a testbed to enable this kind of research, and to encourage developers to design their tools with cooperation in mind.

References

[1] http://www.loria.fr/equipes/protheo/SOFTWARES/ELAN/.

[2] http://www.loria.fr/equipes/cassis/softwares/casrul/.

[3] http://coq.inria.fr/.

[4] http://www.mathweb.org/.

[5] http://www.openmath.org/cocoon/openmath//index.html.

[6] http://www.csl.sri.com/projects/sal/.

[7] http://www.cs.technion.ac.il/Labs/ssdl/research/veritech/.