An Experience of Using Event-B/RODIN in Japan
— DSF Activities —

Shin NAKAJIMA
National Institute of Informatics
Tokyo, Japan

The software industry in Japan, which has a strong need for new methods of development to achieve greater reliability, is more interested in formal methods than it was previously. Some major IT companies (NTT-Data, Fujitsu, Hitachi, NEC, Toshiba, and SCSK) got together to form a joint research group, DSF (Dependable Software Forum) [1] in December 2009. After an initial survey, DSF had chosen Event-B/RODIN as one of the methods to study how they would be used; the others include VDM++ and SPIN.

DSF has chosen Event-B/RODIN as a primary method to study because of its unique modeling approach with refinement and the advanced tool support provided by RODIN. In the first phase, we have given a series of lectures by using the materials that we developed so that the software engineers involved in DSF got to know the technology. Later, in February 2011, we invited Jean-Raymond Abrial to Tokyo to give us several lectures. He explained us the basic idea of Event-B and technical details so that we could refresh our understanding of it and made ourselves more familiar to the technology than before.

DSF has made public its activities in July 2011 [2]. A set of documents to describe "Guidelines to use Formal Methods" was reported, the major output of which was document on Event-B/RODIN. It is a first technical document on Event-B/.RODIN written in Japanese. We have "tailored" methodological aspects of the Event-B/RODIN, which includes a set of idioms and a guideline to make a plan for the refinement steps [3].

DSF, then, joined a working group organized by IPA to conduct further feasibility studies of using Event-B/RODIN. We applied the method to inspect a given set of design documents. The target is a kind of document management system, which had already been completed its development and is now used daily. The documents for the basic design were inspected to transform their contents into Event-B descriptions to be formally checked with RODIN.

This experimental activity is quite unique because all the “bugs” found in the original development process had been collected. We compared the results of the inspection with Event-B and the reported “bugs.” Some inspection results were actually missed in the development process although they were “magically” corrected by human engineers probably using appropriate domain knowledge. Furthermore, some reported bugs were re-captured by the inspection with Event-B. These findings have impressed those who had provided us the basic design documents. The result of this experiment was also made public in April 2012 [4].

The experience with DSF shows that Event-B/RODIN is definitely one of the industrial-strength formal methods today. The importance of refinement-based modeling and advanced tool support was recognized again by all the software engineers involved in the project. Simultaneously, we feel a strong need for tailored guidelines to use the technology appropriate for the characteristics of the target systems and a cultural aspect of the development organization/team although such tailoring is always important to have usable development methods.

We express our thanks to all the people working in RODIN project to make the technology publicly available, and to Jean-Raymond Abrial for inventing the B methods.

[1] DSF, http://www.nttdata.co.jp/dsf/en/
[2] DSF. http://www.nttdata.co.jp/dsf/
[3] S. Nakajima, A Refinement Planning Sheet, talk at RODIN User and Developer Workshop, Dusseldorf, September 2010.
[4] IPA. http://sec.ipa.go.jp/reports/20120420.html