Analyzing the Requirements of an Access Control Using VDMTools and PVS

Georg Droschl

IST – Technical University of Graz, Austria *and*
Austrian Research Center Seibersdorf (ARCS).

droschl@ist.tu-graz.ac.at, <http://www.ist.tu-graz.ac.at>

SSD is an access control, which is part of a comprehensive security system developed by the Austrian Research Center Seibersdorf. SSD is being re-developed in a formal methods case study(cf Fig. 1). Since executable code has to be de-

Fig. 1. The Access Control and the Project Record of the Case Study.

veloped, a tool with an automatic code generator had to be chosen. VDMTools for VDM-SL is such a tool. When testing the specification, a test case indicating a contradiction in the requirements has been found. In order to achieve a better understanding of the nature of the contradiction, the theorem prover PVS has been used to formally prove properties of a certain aspect described by the requirements¹. The benefits of the PVS analysis include theorems which indicate inconsistencies in the requirements. Subsequently, linking VDM and PVS has been further investigated². There are VDM and PVS specifications which share the concept of events. However, they are used in a different manner in the two formalisms. Another aspect is using VDM for event-based systems.

¹ Droschl G. Using PVS for requirements analysis of an access control. Technical Report IST-TEC-99-05, IST, TU-Graz, Austria, February 1999. Available at <http://www.ist.tu-graz.ac.at/Publications>

² Droschl G. Events and Scenarios in VDM and PVS. To appear in the proceedings of 3rd Irish Workshop in Formal Methods, Juli 1–2, Galway, Ireland, 1999.