A VDM specification of the steam-boiler problem Abstract and Evaluation

Yves LEDRU, Marie-Laure POTET*

November 14, 1996

Abstract

A model-based formal specification of the steam boiler problem is presented, using VDM-SL. The development of the specification follows an environment-based approach. First, the physical boiler is specified, then its interface with the control system and finally, the control system itself. The integration of the interface and of the controller in the specification of the boiler take the form of successive refinements. The approach has several advantages: it provides a methodological guidance to the specification activity and tends to avoid over-specification and premature design decisions, by focusing later on the control aspects of the problem.

This specification had to face several challenges. VDM is mainly aimed at the description of transformational systems and does not provide support for real-time or reactive aspects. Also, the size of the resulting specification mandates the use of modular constructs. This solution tries to handle these reactive and real-time aspects in the standard VDM-SL language, and provides an evaluation of the modular extensions of VDM-SL proposed by the IFAD toolbox. Still, the main result of this work is the specification which helped locating imprecisions in the original statement, improved the detailed understanding of the problem by the specifiers and provides a precise reference for the subsequent design and implementation activities.

Evaluation and comparison (draft)

1. *Which parts of the system are specified at which level and in which way? (verbally, rigorously, formally?)*

   The specification covers the behaviour of the boiler, how it can be perceived through the available captors, or influenced by the available actuators. These provide a context for the implicit specification of the controller. These specifications are formal.

   The specification of the possible failures of the boiler has not been expressed formally, but sketched verbally. Several consistency properties of the specification have been considered verbally.

2. (a) *Does the solution comprise an implementation of a control program?*

[0]Laboratoire Logiciels Systèmes et Réseaux - Institut IMAG (UJF - INPG - CNRS), BP 53, 38041 Grenoble Cedex 9 (FRANCE) - Tel + 33 76827214 - Fax + 33 76827287 - e-mail Yves.Ledru@Imag.fr, Marie-Laure.Potet@imag.fr

No, it only addresses the specification activity. Still some parts of the specification are executable, but they correspond to a modelisation of the boiler, and not of the controller.

(b) *Has the control program been linked to the FZI simulator?*
No, but the simulator helped clarifying some imprecisions in the original statement of the problem.

(c) *Has some experimentation been done with the control program?*
No.

3. *What are the comparable other solutions and what are the major differences wrt them? What other solutions complement the given solution and in which respect?*

The main characteristics of our work are: a model-based language, the modelisation of the environment, and the fact that it is limited to the specification phase. The solutions that use B, Z, or RSL also use a model-based specification language.

- The solution proposed by Abrial using the B language mainly focuses on the design and verification activities and does less address the problem of stating the specification. To some extent, it addresses the activity that follows the specification activity covered by our work and can be considered as complementary. Also, the fact that it uses a model-based formalism may allow an easy transition between these phases.
- The work proposed by Buessow and Weber seems closer to our contribution. The use of the Statecharts formalism in combination with Z is a good way to address the reactive aspects of the problem.
- The work of Schinagl using RSL seems to be more object-oriented than our VDM specification. Also, it tends to be more closer to an implemented solution. One objective of our approach was to avoid over-specification and premature design decisions which may appear in the very explicit style of specification adopted in Schinagl's work.

4. (a) *How much time has been spent on producing the solution? Give the number of person months, if possible for the various parts of the solution.*
Two persons worked part-time on the problem during 3 months. The total amount of time spent is estimated to 1.5 man*month, but it definitely benefited from the "idle" time to mature the solution.

(b) *How much preparation is needed to become sufficiently expert of the used specification framework in order to be able to produce a solution to such a problem in that framework? Indicate the number of weeks of training which you believe is needed for an average programmer to learn the method.*
An average programmer needs 2 weeks of training for the VDM method and tools, but the production of a similar specification needs a deep understanding of the method which can only be reached after several months of practice under the supervision of an expert.

5. *What are the premises for a good understanding of the proposed solution?*

(a) *Is a detailed knowledge of the used formalism needed?*
No. The paper assumes a basic knowledge of the principles and concepts of VDM, corresponding to the level of a one-day tutorial.

(b) *Can an average programmer understand the solution?*

The goal of the document is mainly to specify the problem. Not to propose a solution. An average programmer can understand the solution provided he has a basic knowledge of VDM.

(c) *How much time do you believe is necessary for the average programmer whithout knowledge of the used specification method to learn what is needed to be able to understand the solution?*

One week to understand the specification.