An Overview of the ISO/VDM-SL Standard*

Nico Plat†

Delft University of Technology
Faculty of Technical Mathematics and Informatics
P.O.Box 356, NL-2600 AJ Delft, The Netherlands
nico@dutiaa.tudelft.nl

Peter Gorm Larsen†

IFAD
The Institute of Applied Computer Science
Forskerparken 10, DK-5230 Odense, Denmark
peter@ifad.dk

Abstract

VDM-SL, the notation incorporated in the formal method VDM, is currently being standardized under auspices of the International Standards Institution (ISO) and the British Standards Institution (BSI). It is one of the few formal languages of which the syntax and the semantics have been completely formally defined. In this paper we present an overview of the standard, including a report on the current status of the standardization effort.

1 Introduction

The acceptance of the importance of formal methods for software development, and the industrial application of formal methods are becoming increasingly widespread. Formal methods provide a mathematical approach to the specification and subsequent development of software, thus allowing unambiguous specifications and development steps which can be proved to be correct.

One of the most mature formal methods, primarily intended for the formal specification and development of functional aspects of software systems, is the *Vienna Development Method (VDM)* [**?**, **?**]. A central element of VDM is its specification language: *VDM-SL*. VDM-SL is a wide spectrum specification language: it can be used for highly abstract specifications as well as for specifications at a very low level of abstraction. In fact, an executable subset of the language can be defined [**?**, **?**], such that the language is suitable for prototyping.

The increasing use of VDM and the growing number of dialects in use have led to the recognition of the need for a standard for VDM-SL. The standardization effort is carried out under the flag of ISO/IEC JTC1/SC22/WG19. It is expected that an internationally recognized standard for VDM-SL will lead to:

- An increase in the use of VDM. The standard provides a reference document for VDM-SL, serving as an agreed document defining the exact meaning and format of VDM-SL specifications.

- An increase in the tool support for VDM. The availability of a standard will increase the possibility for specifications to be communicated between tools, which will make the development of such tools more attractive for tool vendors.

- A deeper insight into the problems occurring with the complete formal definition of formal languages. Virtually all aspects of VDM-SL have been formally defined, natural language merely being used for annotation purposes. To the authors' knowledge, the only other language for which this is being done (in the context of ISO standardization) is Modula-2 [**?**].

*Submitted for publication to ACM SIGPLAN Notices

†The authors are official delegates to ISO/IEC JTC1/SC22/WG19 for The Netherlands and Denmark, respectively. Both authors are also active members of BSI IST/5/-/19.

In this paper we will present an overview of the standard for VDM-SL. A reference guide for the language following the standard (to be) as closely as possible is [**?**], another recent text book illustrating the language is [**?**]. Earlier status reports of the standardization process have been published in [**?**] and [**?**].

This paper is organized as follows: in the next section we will give a short overview of the history of the language which has led to the initiative for standardization. In section **??** we will briefly describe some essential characteristics of the language. In section **??** we will give a condensed overview of the structure of the standard and a short description of each of the elements. We will conclude the paper by reporting on the current status of the standardization effort.

2 History

'VDM' is a generic term: the development of VDM has given rise to several VDM 'dialects'. The development of VDM started back in 1970, when in the IBM laboratory in Vienna a group formed by Heinz Zemanek worked on formal language definition and compiler design. They built on ideas of Elgot, Landin and McCarthy to create an operational semantics approach capable of defining the whole of PL/I, including the parallel features of the language. For this purpose they used a meta-language which was called *Vienna Definition Language (VDL)*. The approach taken was successful, but it also showed that operational semantics could complicate formal reasoning in an unnecessary way. A new approach was taken, called *denotational semantics*, in late 1972. A PL/I compiler was designed using a meta-language called *Meta-IV*. Due to external reasons the compiler was never finished, but the formal definition of PL/I in a denotational style is generally seen as the birth of VDM.

The diversion of the IBM group to handle more practical problems led to its dissolution. From then on, further development mainly took place at two geographical locations: in Lyngby, Denmark (Prof. Dines Bjørner) and in Manchester, UK (Prof. Cliff B. Jones). The Danish VDM research has concentrated on systems software specifications, which has led inter alia to a complete formal definition of the Ada language, whereas the English research has mainly concentrated on algorithm and data structure refinement. VDM proof obligations are one of the major results of the latter research. Thus, the main reason for the existence of different VDM dialects is the different areas of application VDM can be used for. Unfortunately, such a diversion does not stimulate industrial acceptance of VDM, and therefore, in 1986 work started on the establishment of a standard version of VDM-SL.

The standardization effort was initiated by the *British Standards Institution (BSI)*, establishing a Panel (BSI IST/5/-/50) whose membership was also open to members from foreign organizations. In 1991 the need for a VDM-SL standard was also recognized by *ISO/IEC JTC1*[2] by the formation of a Working Group, SC22/WG19. The actual work on the standard is still being done by the members of the BSI Panel (since the official recognition by ISO known as BSI IST/5/-/19).

3 An overview of the language

VDM is a model-oriented formal method based on a denotational semantic setting, intended to support stepwise refinement of abstract models into concrete implementations. The method includes a formal specification language, VDM-SL, which supports various forms of abstraction.

Representational abstraction is supported through data modeling facilities. These facilities are based on six mathematical data structuring mechanisms:

[2] Joint Technical Committee 1 of the International Standards Organization and the International Electro-technical Commission.