
VDM and the Verified Software Challenge

John Fitzgerald¹, Hugo Macedo and
Miguel Ferreira

Zoe Andrews, Jeremy Bryans, John Hughes, Peter Gorm Larsen,
Jose Oliveira, Richard Payne, Ken Pierce, Sander Vermolen,...

¹ Centre for Software Reliability,
Newcastle University

Some theorem provers ...



VDM and the Verified Software Challenge

1. VDM and VDM Tools Today
 2. Mondex
 3. Pacemaker (Hugo)
 4. Posix (Miguel)
-

VDM and VDM Tools

- Vienna Development Method (from 1970s!)
 - Basic modelling language was VDM-SL:
 - Model-oriented; abstraction in type definitions & functionality specification
 - British School: implicit pre/post-specification
 - Danish School: executable functional models
 - British & Danish Schools unified by Fitz. & Larsen in mid 1990s
-

VDM and VDM Tools

- Mid 1990s: Significant tools development at IFAD (Denmark)
 - 1992 – 1994: ESPRIT-III project AFRODITE: start of VDM++ (o-o) and an initial toolset
 - 1994 – 2004: toolset and VDM++ taken up by IFAD
 - Large customer base established: over 1000 users worldwide
-

VDM and VDM Tools

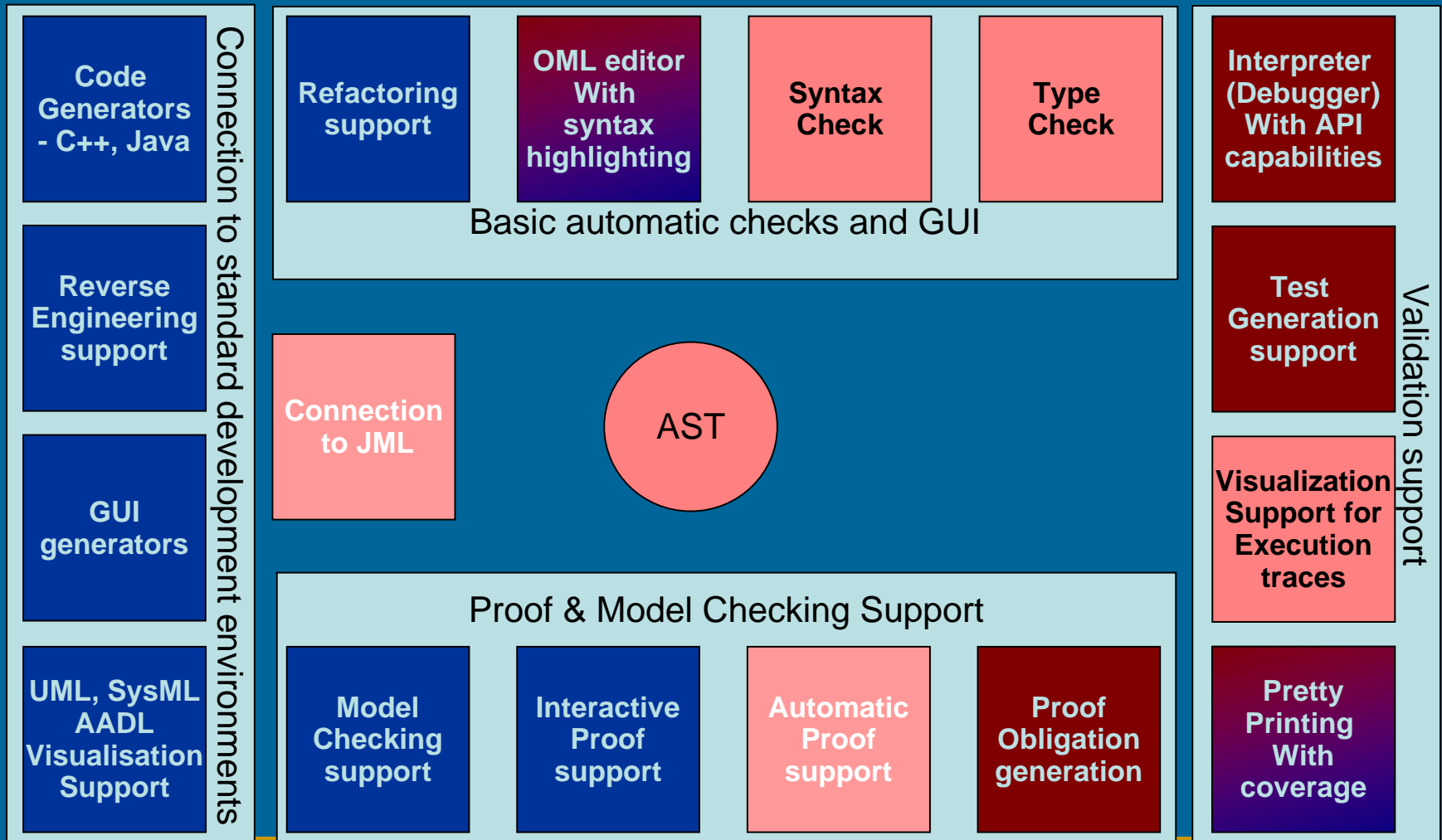
- 2004: IFAD went out of business!
 - 2004: VDMTools taken over by CSK, Japan
 - recently: VICE Extensions (distribution, RT)

 - 2004: Overture:
 - Open source movement
 - New thinking, new technology in the area of IDEs and user interfaces
 - Eclipse plug-in approach to encourage a variety of tools
-

VDM and VDM Tools

- Philosophy– lowering barriers to industry use
 - Recently, emphasis on modelling over refinement or code verification
 - Major tools development effort
 - Good record of industry experience, much in public domain.
 - www.vdmportal.org
-

VDM/Overture Tools



Shows current, under development and planned components

Engagement with challenge problems

- Mondex: benchmarking validation capabilities
- Pacemaker: exploring extensions for embedded and real-time systems design
- Posix: tool chains and interoperability

Mondex

- Newcastle team, many new to VDM in depth, few old-timers
- Fully modelled
- Broadly as in the Z monograph
- Full range of V&V techniques used:
 - Systematic test (executable subset)
 - Scenario-based test (via GUI for non-VDMer)
 - Proof obligation generation
 - Auto-discharging in HOL (subset)
 - Manual refinement proofs

Pacemaker (Hugo Macedo)

- Full paper in the symposium procs.
 - Study in VDM++ “VICE” extensions (real-time and distributed)
 - Extensions motivated by the need for:
 - Early phase identification of bottlenecks in embedded systems
 - Validation of timing behaviour by examination of test traces
 - (Ultimately interested in co-simulation)
-

Posix (Miguel Ferreira)

- Focus on tools interoperability
 - Working on Intel Flash File System Core in
 - VDM++
 - Alloy
 - HOL
-

VDM and the Challenge Problems

Further information:

- Overture Tools Initiative: www.overturetool.org
 - VDM in general www.vdmportal.org
 - CS-TR-1099 at www.cs.ncl.ac.uk/research:
Fitzgerald, Larsen, Sahara, “Modelling and Analysis in VDM: Proceedings of the Fourth VDM/Overture Workshop”
-