Applications of Formal Methods

R.B. Jones
International Computers Limited, Eskdale Road, Winnersh, Wokingham, Berks RG11 5TT

tel: 0734 693131 x6536, fax: 0734 697636
email: uucp: rbj@win.icl.co.uk
Overview

- Applications Survey

- Applications in ICL Secure Systems
  - Business Motivators
  - Applications
  - Special Methods
  - Tools
Applications Outside ICL

• Praxis CASE tools project

• Praxis Z tools project

• Inmos T800 floating point unit

• IBM CICS project
Praxis CASE Tool Project

- Objective - to develop a complete CASE system for SSADM

- Team of 4-7 people (most were mathematicians)

- 345-page Z specification written

- 37,000 lines of code produced

- 25% of effort in specification phase

- Code productivity 50% higher than expected

- Better quality output
Praxis Z Tools Project

• Editor, parser, typechecker, cross-reference tool for Z documents.

• Team of 3 (with formal methods experience).

• Half of system specified in Z.

• 17,200 lines of code produced.

• 26% of effort in specification phase.

• “Productivity of 48 lines of code per day”.
Inmos T800 Floating Point Unit

- Silicon implementation delivered with only 3 faults (all due to errors in manual transcription).

- ‘Informal’ teams version contained more errors.

- A saving of 25% time to market, compared with that of the ‘informal’ team.
IBM CICS Project

- Z is being used to respecify key interfaces in 20 year old CICS (TP).

- Release 3.1 contains 268,000 lines of new code of which 37,000 have been specified in Z.

- Over 100 people trained in Z.

- 2000 pages of Z specification written.
CICS Project Benefits

• Errors found earlier in development where formal methods used.

• Error rate reduced to 61% of rate for informal development.

• 9% reduction in total development cost, though only 14% of code was formally specified.

• Further savings expected in support costs.
Applications Inside ICL

- “The Use of VDM within the Alvey Flagship Project”, VDM88, Springer LNCS 328.

- VDM and Essex

- Z in Office Systems

- Applications In ICL Defence/Secure Systems
Business Motivators

Quality

Regulatory framework for Secure (and Safety Critical) Systems

Strategic Need for Highly Secure Systems?

Professional Services Revenue
Security Certification Schemes

US Department of Defence Trusted Computer System Evaluation Criteria “Orange Book”

CESG Computer Security Memorandum No.3 “UK Systems Security Confidence Levels”

Harmonised Criteria Information Technology Security Evaluation Criteria “ITSEC”

Safety Critical

UK MOD interim defence standards 00-55/56
Applications In ICL Defence/Secure Systems

• Use of VDM on VDAP

• Z on various Design Study and Security Modelling contracts for CESG

• HOL/Z on CESG/ICL OWR project

• ICL HOL and Z proof tool

• Z for security modelling on UKAIR and CHOTS

• VDM/Z in various bids.
Use of VDM on VDAP Project

VDAP = VLSI Distributed Array Processor


- Run Time System

The CESG/ICL OWR Project

• A design-and-implement contract placed with ICL Defence Systems by CESG (Communications and Electronics Security Group, GCHQ)

• Design and make pre-production models of a ONE WAY REGULATOR to the highest achievable standards of assurance.

• Hardware only solution

• Full formal verification of detailed design against formal security policy.

• Product certified by HMG as “exceeding the requirements of UKL6”