ICL Defence Systems Formal Methods Unit

Roger Bishop Jones
ICL Defence Systems

ABSTRACT

This document consists of the overheads for a presentation to the STC Technology Panel on DS Formal Methods Work.
Agenda:

<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
<th>Presenter</th>
</tr>
</thead>
<tbody>
<tr>
<td>09:30</td>
<td>Introduction</td>
<td>Myer Morron</td>
</tr>
<tr>
<td>09:40</td>
<td>Overview</td>
<td>Roger Jones</td>
</tr>
<tr>
<td>10:00</td>
<td>GCHQ Design Studies</td>
<td>Frank Womack</td>
</tr>
<tr>
<td>10:20</td>
<td>Compiler Development Using VDM</td>
<td>Tom Lake</td>
</tr>
<tr>
<td>10:40</td>
<td>Formal H/W Test Case Extraction</td>
<td>Geoff Scullard</td>
</tr>
<tr>
<td>11:00</td>
<td>Coffee and comfort break</td>
<td></td>
</tr>
<tr>
<td>11:10</td>
<td>One Way Regulator</td>
<td>Alan Walton</td>
</tr>
<tr>
<td>11:20</td>
<td>Security Modelling</td>
<td>Myer Morron</td>
</tr>
<tr>
<td>11:30</td>
<td>Square Root Box (the movie) training</td>
<td>Myer Morron</td>
</tr>
<tr>
<td>11:40</td>
<td>Critical Factors</td>
<td>Roger Jones</td>
</tr>
<tr>
<td>12:00</td>
<td>Tour of Facility</td>
<td>Myer Morron</td>
</tr>
</tbody>
</table>
OVERVIEW
of
DS FORMAL METHODS WORK

Roger Jones
Leader, DS Formal Methods Unit
FORMAL METHODS
is about
QUALITY ASSURANCE

In Defence market:

ASSURANCE
is
ADDED VALUE

customer requirements go
BEYOND ZERO DEFECTS

customer (DOD, GCHQ/MOD) precisely defines
LEVELS of EVALUATION
(vide Orange book)
in which HIGHER LEVELS
DEMAND FORMAL VERIFICATION

use of FORMAL METHODS to achieve
HIGHER LEVELS of ASSURANCE
gives COMPETITIVE ADVANTAGE and
creates NEW MARKETS
Formal Methods Work in Defence Systems

Formal Hardware Test Extraction

Compiler Development using VDM

GCHQ Design Studies

One Way Regulator

Formal Methods Consultancy

Security Modelling

VDM Standardisation

Training
OWR FORMAL METHODS CONTENT

WORLD FIRST
commercial hardware verification
A1+ evaluation

Security Requirements Specified in HOL
(Higher Order Logic)

Design in HOL

Design will be
FORMALLY PROVEN
to satisfy security requirements
(using the Cambridge HOL
proof development system)
SECURITY MODELLING

Invitations to tender now frequently contain requirements for formal security models.

The DS Development Unit provides formal presentations of security requirements for inclusion in tender documents.

Further formal security modelling may be provided after award of contract.

Projects supported in this way include:

- VME Security Option
- UKAIR
- CJ2
- CHOTS
- TRAWLERMAN
CRITICAL FACTORS

PEOPLE

Very high calibre of staff required Customer specifies PhD level staff.
Staff difficult to recruit, and difficult to retain.

LANGUAGES, METHODS and TOOLS

The technology is still immature. Considerable productivity benefits could be expected from improved tooling.
Higher levels of evaluation require better languages, methods and tools.