Aspects of High Assurance

Roger Bishop Jones

ICL Defence Systems
This document consists of the overheads for a presentation to
the IED project on Feb 9 1990.

QUESTIONS ABOUT HIGH ASSURANCE

HOW DO PROOF TOOLS CONTRIBUTE TO HIGH ASSURANCE?

HOW DO WE GET HIGH ASSURANCE ABOUT PROOF TOOLS?

HIGH ASSURANCE PROOF TOOLS

REQUIREMENT:

THAT ONLY VALID SEQUENTS ARE PROVABLE

HOW DO WE ESTABLISH THAT
OUR FORMAL SYSTEM IS CONSISTENT?

HOW DO WE ESTABLISH THAT
THE PROOF TOOL
CORRECTLY CHECKS PROOFS?

ESTABLISHMENT of CONSISTENCY

Formalise syntax

Formalise proof rules and axioms

Formalise semantics
(define validity)

Show that proof rules are sound
(preserve validity)

Show that axioms are valid

Show that "[]|-F" is not valid

Show that there exists a model?

LOGICAL FRAMEWORK
for
CONSISTENCY PROOF

All but last item
(existence of model)
could be done in HOL.

Last could be done in ZF-HOL
or else reduce to simplest form
and leave unproven.

GOEDEL's RESULTS?

Not a problem

METACIRCULARITY?

Either:

1 bottom line is informal

or:

2 formal circularity is introduced

or:

3 both

CORRECTNESS PROOF
for
PROOF CHECKER

Exercise in code verification

Formalise critical requirements

Factor out critical code

Formally embed part of SML in HOL

Informal and formal (partial) proof in HOL

METACIRCULARITY?

Same arguments as for logic

EMBEDDING of FRAGMENTS of SML into HOL

identify semantics domains
(need not have single type
per syntactic category)

simplified way of doing
denotational semantics

No need to formalise syntax