Roger Bishop Jones
This document consists of the overheads for a presentation on ICL HOL and related topics at the 1989 HOL user meeting.
FOUNDATIONS and TOOLS for FORMAL VERIFICATION

PARTICIPANTS:

ICL Defence Systems

Program Validation Limited

University of Cambridge

University of Kent
MAJOR ICL OBJECTIVES

HIGHER ASSURANCE

HIGHER PRODUCTIVITY

BROADER APPLICABILITY

STANDARDISATION
HIGHER ASSURANCE

RE-IMPLEMENTATION USING
“GOOD S.E. PRACTISE”

• FORMAL SPECIFICATION of CRITICAL REQUIREMENTS

• CLEAR SEPARATION of CRITICAL CODE

• FORMAL or INFORMAL CORRECTNESS RESULTS
BROADER APPLICABILITY

ABSTRACT AWAY
from
DETAILS of CONCRETE SYNTAX

FORMAL SPECIFICATION
of
ABSTRACT HOL LOGIC

MAXIMISE
FLEXIBILITY and CHOICE
in CONCRETE SYNTAX

HOL SPECIFICATION LANGUAGE
(independent of metalanguage)

SPARK VERIFICATION
STANDARDISATION

ABSTRACT HOL LOGIC

CONCRETE SYNTAX
for
TYPES and TERMS

HOL SPECIFICATION LANGUAGE

CORE HOL SYSTEM INTERFACE
ABSTRACT HOL LOGIC
POINTS for DISCUSSION

VARIABLES

PERMISSIBILITY of CLASHES

DEFINITION of SUBST

CONSTANTS

CHECK on TERM FORMATION

TREATMENT of LITERALS

RULES for CONSERVATIVE EXTENSION

MODULARITY

CONTROLLING the SCOPE of NAMES

SCOPE

RECURSIVE DATA TYPES