

Project: DRA FRONT END FILTER PROJECT

Title: Proposal for Phase 2

Ref: DS/FMU/FEF/018 *Issue: Revision : 1.2* *Date:* 5 December 2009

Status: Draft *Type:* Proposal

Keywords:

Author:

<i>Name</i>	<i>Location</i>	<i>Signature</i>	<i>Date</i>
G.M. Prout	ICL		
R.B. Jones	ICL		

Authorisation for Issue:

<i>Name</i>	<i>Function</i>	<i>Signature</i>	<i>Date</i>
R.B. Jones	HAT Manager		

Abstract: The revised proposal for Phase 2 of the DRA front end filter project RSRE 1C/6130.

Distribution: HAT FEF File
Simon Wiseman

0 DOCUMENT CONTROL

0.1 Contents List

0	DOCUMENT CONTROL	2
0.1	Contents List	2
0.2	Document Cross References	2
0.3	Changes History	2
0.4	Changes Forecast	2
1	GENERAL	3
1.1	Scope	3
1.2	Introduction	3
2	PROPOSAL FOR PHASE 2	4
2.1	Item Number 3 - Formalisation and Proof	4
2.2	Item Number 4 - Report on Proofs	5
3	WORK PLAN	6

List of Tables

1	Tasks in Phase 2	6
2	Deliverables for Phase 2	6

0.2 Document Cross References

- [1] DS/FMU/017. *Secure Database Technical Proposal*. High Assurance Team, ICL Secure Systems, WIN01, 21st January 1992.
- [2] *Invitation to Tender RSRE 1c/6130*. DRA, December 1991.

0.3 Changes History

Changes made as a result of discussions with DRA-ED on December 22nd 1992.

0.4 Changes Forecast

None.

1 GENERAL

1.1 Scope

This document provides a revised proposal for Phase 2 of the DRA front end filter project RSRE 1C/6130.

1.2 Introduction

In the original proposal for this project, [1], it was stated that a firm price costed proposal for the supply of items 3, 4, 5 and 6 of the ITT schedule, found in [2], would be provided at the end of Phase 1.

Some problems arise in making a quotation for the Phase 2 work:

- The specifications for the system about which proofs will be conducted are still substantially incomplete. It is apparent that these specifications when complete will be significantly more complex than those supplied with the original invitation to tender for this contract. This particularly concerns the specifications for the filter, but the specifications for the SSQL database have also been modified since the Phase 1 proof work was started and have not yet been reformalised.
- It appears likely, judging by the information currently available, that the full correctness and security proof for the database as implemented using the filter would be prohibitively costly.

The contract for Phase 1 was based on the premise that the specifications were well formed and secure, and called for a security proof. A significant number of errors were discovered in the specifications, and the extra costs arising had to be dealt with by amendments to the contract. We are therefore costing Phase 2 on the assumption that ICL will be given a larger amount of discretion in the formalisation of the models, and in the resolution of problems discovered in these models. This should substantially reduce the probability of contract amendments being required during Phase 2.

As a result of the experience in Phase 1 it would seem more appropriate to regard the objectives as:

- To use the proof process to discover flaws in the specifications.
- To evolve the specification during the course of the proof as necessary to render it satisfactory.

The main purpose of the requirement for Phase 2 in the original ITT was to verify the design of the Front End Filter. The most important (if not the only) concern was that the filter would result in a secure database.

This proposal for Phase 2 therefore attempts to provide the most effective way of employing formal modelling and proof to improve confidence in the security of the Front End Filter.

2 PROPOSAL FOR PHASE 2

The work proposed for Phase 2 is based on items 3 and 4 of the ITT schedule of requirements in [2]. In discussion with DRA-ED it has been decided to delete items 5 and 6 from the schedule of requirements. In addition, it was agreed to formalise the SSQL query transformations in standard ML. The purpose of this formalisation is to increase confidence in the correctness of the query transformations and to facilitate the maintenance of the specifications by DRA-ED. Because of the present state of the relevant specifications considerably more work is involved in the formalisation of the propositions to be proven than originally envisaged, and the cost of any proof work is more difficult to establish.

2.1 Item Number 3 - Formalisation and Proof

We propose initially to formalise the SSQL query transformations in standard ML. The next step in Phase 2 is the formalisation of the models of the relevant systems and of the propositions to be proven. This may involve re-structuring the specifications in a way which focuses on the security aspects. The propositions offered for proof will be chosen to yield best assurance of security of the filter within the proposed cost limits for Phase 2.

The remainder of item 3 consists in developing the formal proof of the selected propositions. It is proposed, by contrast with the arrangements for Phase 1, that when errors in the models or in the propositions are discovered, ICL will have discretion, in consultation with DRA, to make appropriate modifications to the specifications and to the propositions, so as to yield best results from the remaining work within the original cost profile.

Item 3 is described in greater detail as follows:

Initial Formalisation of the SSQL query transformations

The informal specifications of the SSQL query transformations will be formalised in standard ML. This will necessitate the formalisation of the datatypes of SSQL and TSQL in standard ML.

Formalisation of the TSQL abstract machine

The supplied abstract syntax of TSQL (known as standard SQL in [2]) is intended to be based on the semantics of SSQL. DRA have supplied a revised abstract syntax of SSQL which differs from that on which the Phase 1 formalisation of the semantics of SSQL was based. Formal modelling of the TSQL database undertaken during Phase 2 will focus on those aspects of the underlying database which are essential to the security of the database resulting from the addition of the filter, and may omit any details not essential to the proposed proof work.

Formalisation of the SSQL query transformations

We propose to re-structure the query transformations so as to minimise the costs of the subsequent formal proofs (which should have a beneficial effect on their intelligibility). Details which are immaterial to the security proofs may be omitted, and features of the models which are particularly problematic from the point of view of the security proof may be omitted or simplified. All such points will be clearly documented in the accompanying informal text.

Formalisation of SSQL implementation behavioural model

A mathematical model will be constructed of the behaviour of the SSQL system as implemented using the TSQL abstract machine and the specified filters. This should be a routine construction.

Formalisation of security propositions

It is our present view that a full functional correctness proof for the SSQL database as implemented using the filter is not feasible within cost limits acceptable to DRA. It is therefore proposed to focus the proof effort in Phase 2 on the security of the SSQL database. The state of the specifications at this time does not allow a reliable estimate of the cost of a full security proof for the SSQL database.

It is proposed that on completion of the specification work, ICL will identify the proposition or propositions, relating to the security of the filter implementation of the SSQL database, the proof of which will most effectively improve assurance of security within the proposed cost limits for Phase 2. DRA will be consulted during this process to facilitate agreement on the propositions to be proven.

Proofs

Machine checked formal proofs of the agreed security propositions identified above will be developed and delivered to DRA.

In the event of any of these propositions proving to be false or intractible ICL will consult with DRA with a view to identifying corrective actions which maximise benefits within the proposed cost limits.

Issue 1.2 Removed dependency on ICL logo font

2.2 Item Number 4 - Report on Proofs

This is as in section 2 of the original proposal for this project, [1].

3 WORK PLAN

It is anticipated that the overall duration of Phase 2 be twelve months. Table 1 shows a first level decomposition into subtasks of the work for Phase 2 described in Section 2 above.

Code	Description
WP3	Formalisation of SSQL Implementation Model and Proof of Security Propositions
WP4	Report on Phase 2 Proof

Table 1: Tasks in Phase 2

Table 2 shows the major deliverables for Phase 2. Two estimated delivery dates are shown where appropriate. The first is the date (from the start of Phase 2) for a draft for review by DRA-ED, the second is the date for the final version.

WP	Code	Description	Draft	Final
WP3	D8	Query Transformation Specifications in SML	wk6	wk8
WP3	D9	TSQL abstract machine specifications	wk18	wk50
WP3	D10	Query Transformation Specifications in HOL	wk6	wk50
WP3	D11	SSQL Implementation Model Specifications	wk18	wk50
WP3	D12	Specification of Security Propositions	wk34	wk50
WP3	D13	Phase 2 Proof Scripts	-	wk50
WP4	D14	Report on Phase 2 Proofs	-	wk50

Table 2: Deliverables for Phase 2