NAT'L INST. OF STAND & TECH R.I.C.
A11105 086776
NIST PUBLICATIONS

NISTIR 6068

Report on the TMACH Experiment

Ellen Flahavin (NIST)
Goswin Eisen (IABG)
Steve Hill (Logica)
Heribert Spindler (IABG)
Julian Straw (Syntegra)
Andy Webber (Logica)

U.S. DEPARTMENT OF COMMERCE
Technology Administration
National Institute of Standards
and Technology
Information Technology Laboratory
Gaithersburg, MD 20899-0001

July 1997

NIST

QC
100
.U56
NO.6068
1997

NISTIR 6068

Report on the TMACH Experiment

Ellen Flahavin (NIST)
Goswin Eisen (IABG)
Steve Hill (Logica)
Heribert Spindler (IABG)
Julian Straw (Syntegra)
Andy Webber (Logica)

U.S. DEPARTMENT OF COMMERCE
Technology Administration
National Institute of Standards
and Technology
Information Technology Laboratory
Gaithersburg, MD 20899-0001

July 1997

U.S. DEPARTMENT OF COMMERCE
William M. Daley, Secretary

TECHNOLOGY ADMINISTRATION
Gary Bachula, Acting Under Secretary for Technology

NATIONAL INSTITUTE OF STANDARDS
AND TECHNOLOGY
Robert E. Hebner, Acting Director

ABSTRACT

The evaluation of security in Information Technology products and systems has traditionally fallen to Government bodies. Each nation has devised criteria for such evaluation based on their own needs. In Europe, a number of nations realised that the objectives and methods of evaluation were sufficiently similar to make it worthwhile devising a single set of criteria and methods to suite the needs of the participant nations. This resulted in the ITSEC.

In the United States of America, it was felt necessary to understand the European approach to evaluation, and the commercial basis for evaluation that is used in some European nations. On this basis, a high assurance product was selected to undergo the evaluation process in the UK and Germany to learn about the process. The product in question was TMach, being developed by Trusted Information Systems Inc.

All trademarks are acknowledged whether shown within the text or not.

CONTENTS

REFERENCES

[CC] Common Criteria for Information Technology Security Evaluation (Parts 1 to 4), Version 1.0, 31 January 1996

[CONF-91] Apparent Differences Between the US TCSEC and the European ITSEC
M A Branstad, C P Pfleeger, D Brewer, C Jahl and H Kurth
National Computer Security Conference, October 1991

[ITSEC] Information Technology Security Evaluation Criteria, Version 1.2, June 1991.

[ITSEM] Information Technology Security Evaluation Manual, Version 1.0, September 1993

[JIL] ITSEC Joint Interpretation Library (ITSEC JIL), Version 1.0, July 1996

[NCSC-TG-002] Trusted Product Evaluations - A Guide for Vendors, 22 June 1990. (Bright Blue Book)
See also TPEP Procedures which supersedes parts of this document.

[NCSC-TG-005] Trusted Network Interpretation of the TCSEC (TNI), 31 July 1987. (Red Book)

[NCSC-TG-009] Computer Security Subsystem Interpretation of the TCSEC 16 September 1988. (Venice Blue Book)

[NCSC-TG-021] Trusted Database Management System Interpretation of the TCSEC (TDI), April 1991. (Purple Book)

[SADSEF] An Approach to the Definition of Semiformal Security Enforcing Functions
Ref. 234.20296.10.12, Issue 2, 22 November 1993

[TCSEC] DoD Trusted Computer System Evaluation Criteria, 26 December 1985 (Supersedes CSC-STD-001-83, dated 15 Aug 83). (Orange Book)

[TPEPP] TPEP Procedures

[UKSP05] UK IT Security Evaluation Scheme Manual of Computer Security Evaluation, Part III - Evaluation Techniques and Tools
Issue 1.0, June 1994
(*This document has restricted distribution*)

ABBREVIATIONS

ARPA	Advanced Research Projects Agency
CCEB	Common Criteria Editorial Board
CESG	Communications-Electronics Security Group
DTI	Department of Trade and Industry
EWP	Evaluation Work Programme
GISA	German Information Security Agency
ITSEC	Information Technology Security Evaluation Criteria
ITSEF	Information Technology Security Evaluation Facility
ITSEM	Information Technology Security Evaluation Manual
JIL	ITSEC Joint Interpretation Library
NCSC	National Computer Security Center
NIST	National Institute for Standards and Technology
NSA	National Security Agency
OSF	Open Software Foundation
RAMP	Ratings Maintenance Programme
SCSSI	Service Central de la Sécurité des Systèmes d'Information
SIN	Scheme Information Notice
SEF	Security Enforcing Function
TCSEC	Trusted Computer Security Evaluation Criteria (Orange Book)
TOE	Target Of Evaluation
TTAP	Trust Technology Assessment Program

1. INTRODUCTION

1.1 Purpose of Report

This report documents the findings of a multi-national evaluation experiment, funded by the U.S. Advanced Research Projects Agency (ARPA), to explore alternative approaches to security evaluation. The experiment focused on European ITSEC evaluations within the UK and Germany, using the Trusted Mach operating system (developed to target TCSEC B3) at a high level of assurance (E5). The report provides a description of the experiment, its aims and objectives, and provides insight into what has been learned and accomplished so far. (Note that this effort was performed over a number of years and the names of some of the organisations mentioned here may have changed.)

1.2 Purpose of the Experiment

In 1983, the U.S. Department of Defense published the Trusted Computer System Evaluation Criteria (TCSEC). Since that time, the National Security Agency (NSA) has been performing trusted system evaluations against the TCSEC within the United States. In 1990, the Commission of European Communities published a draft version of a European developed criteria, the Information Technology Security Evaluation Criteria (ITSEC).

Evaluations against the ITSEC were to be performed by IT Security Evaluation Facilities (ITSEFs) that were overseen by National Authorities. Considerable debate ensued on how the TCSEC and ITSEC compared but the debate remained at a philosophic level for want of hard evidence based upon comparative evaluation experience. Although claims were made that the criteria were compatible with one another, there appeared to be no real basis for discussing reciprocity of rating among the various countries. If ITSEC-rated systems were to be proposed for use within NATO, the United States would have little understanding of the rating.

The Trusted Mach (TMach) system, targeted at a B3 TCSEC rating, was being developed under the ARPA funding at this time. Evaluation of the TMach system against both the ITSEC and TCSEC was suggested as a means for understanding how the criteria and their accompanying evaluation processes compared. Although the TMach evaluations would not definitively answer how the criteria compared at all levels, it would move the comparison into a concrete rather than philosophic discussion. By actually evaluating TMach against the criteria, the different requirements of each criterion and evaluation process would become visible.

It is in the interest of the U.S. Government to understand how these two criteria differ in practice and how evaluations done under each may be compared. Efforts to reconcile the differences were therefore undertaken based upon detailed knowledge and understanding

gained thus far. North America and Europe subsequently agreed to develop the Common Criteria for Information Technology Security Evaluation [CC].

1.3 Target Audience

The purpose of this report is to inform on the results of the TMach trial evaluation project, and as such is intended primarily for use by the following groups:

- ARPA - The project sponsor;
- NIST (National Institute of Standards and Technology) - Which managed the project, and is the principal direct beneficiary of the research.

The stated objective of these organisations at the outset of the work was to raise awareness of the European evaluation process and to examine that process for features which could be used to develop further US initiatives in this area.

The results from the project are wide ranging and will also be of interest and relevance to the following groups:

- Vendors of high assurance products who wish to gain insights into those areas of ITSEC requirements which have proved challenging.
- European Scheme Managers with an interest in mutual recognition of evaluation results, who will wish to explore any identified differences in approach between the UK and German approaches.
- US evaluators who wish to gain awareness of the European process, and of the differences in approach from TCSEC evaluations.
- European evaluators without experience of high assurance evaluations, and those wishing to gain some understanding of differences from the US process.
- Those with the responsibility of developing the Common Criteria and Common Evaluation Methodology who wish to gain an understanding of the likely problems in applying and interpreting the criteria in high assurance evaluations.

1.4 Overview Of The TMach System

The Trusted Mach (TMach) system is a secure server-based operating system implemented as a message passing microkernel and a set of servers. TMach is intended as a highly portable operating system, capable of hosting other operating systems within domains and providing multi-level secure capabilities at high assurance.

The servers provided operating system functionality that is traditionally found in the operating system kernel. The TMach system is layered in accordance with generally accepted software engineering principles. These principles require that abstract layers

depend upon primitive layers and that the primitive layers shall not depend upon the abstract layers. TMach is designed to support information systems security and control requirements. Each protection layer provides abstractions and services to the layers above. Communication between the protection layers is performed over well-defined interfaces.

Each individual component defines a separate task. Layers of tasks are used in order to protect the trusted computing base (TCB). Dependencies between the components, whether microkernel modules or TCB tasks, is strictly downwards, with no component depending on a higher component for its functionality.

2. DESCRIPTION OF APPROACH

2.1 Roles and Objectives

2.1.1 Governments

ARPA - United States

ARPA's objective is to advance the technology of computer systems for the Department of Defense. The development of TMach began in the late-eighties with ARPA desiring a trusted operating system based upon the highly portable Mach microkernel. The intention was that, through the ITSEC evaluation of the TMach system, ARPA would gain the knowledge to understand how ITSEC and TCSEC evaluations compare, information that could be essential to determine the acceptability of candidate NATO systems. The project provided insight to guide decisions for evaluation reciprocity. It was also intended to result in a trusted operating system, TMach, that was evaluated against both criteria and thus should be acceptable for both the United States and European markets. Also, the trust characteristics of TMach would fit into ARPA's evolutionary operating system goals.

NIST - United States

NIST monitored the TMach evaluation contract performance for ARPA, and provided the contractual and management interface with the U.S. Government. In essence, NIST became the contractual "middle-man" for ARPA. NIST was responsible to ARPA as the U.S. Government agent for setting the evaluation tasks and co-ordinating the evaluation work.

The intended spin-offs from this exercise included understanding of the practical differences between the ITSEC and the TCSEC, the opportunity to compare the evaluations done under each, the creation of worked examples to the ITSEC style of evaluations, and exploration of the practical aspects of reciprocity with the U.S. gaining an understanding of the European Process and of any differences between the UK and the German evaluation processes.

CESG/DTI - United Kingdom

The Communications-Electronics Security Group (CESG) and the Department of Trade and Industry (DTI) in the UK operate a joint IT security evaluation and certification scheme certify the results of evaluations of systems and products to common technical standards. As the UK Certification Body, their interest in the TMach evaluation related both to the high assurance aspects and to the mutual recognition of evaluation results.

GISA - Germany

The two major project objectives for the German Information Security Agency (GISA)[1] were to perform a concurrent E5-evaluation and research on harmonisation aspects. GISA had already gained experiences with ITSEC-evaluations, however the TMach Project was one of the first to be targeted at an E5-level in a product evaluation, this would answer many questions concerning a common European interpretation of the criteria for concurrent evaluation.

2.1.2 Developer

TIS - United States

Trusted Information System Inc. (TIS) built the TMach system on a variant of the Mach microkernel, which was originally developed at Carnegie Mellon University and modified by the Open Software Foundation (OSF). TIS submitted the TMach system to the NSA for a B3 evaluation. Their TMach ITSEC evaluation was initiated to:

- evaluate the TMach architecture and trust strategy;
- evaluate the TMach development process and practices;
- determine whether a single set of documentation could satisfy both the TCSEC B3 and ITSEC E5 requirements;
- understand the similarities and differences between the evaluation criteria and evaluation process.

2.1.3 Evaluators

IABG in Germany, and Logica UK Limited and Syntegra (formerly Secure Information Systems Limited) in the UK were the ITSEFs chosen to perform the evaluations. Their goals were to gain:

- experience of performing an ITSEC E5 evaluation;
- an understanding of the TCSEC and the differences between TCSEC B3 and ITSEC E5/F-B3;
- an appreciation of the differences (if any) between the UK and German evaluation process and approach.

---

[1] Also referred to as the Bundesamt für Sicherheit in der Informationstechnik.

(Logica and Syntegra provided a joint UK evaluation team; it may be noted that this arrangement is unusual within the UK Scheme, where evaluation teams are normally drawn from a single ITSEF.)

2.1.4 Observers

Information from the project was shared with other organisations who were involved as observers.

NSA - United States

NSA agreed on the importance of achieving mutual recognition of different evaluation approaches and emphasised that no organisation wants to initiate a dozen different reciprocity agreements. Concern was expressed regarding the implications of government funded vs. commercially funded evaluations and the maintenance of certification quality.

OSF - United States

OSF is comprised of several international member companies, all interested in U.S./EC evaluations of OSF offerings. OSF's interest in the TMach evaluation centred on two questions:

- First, when developing very high security in an operating system, would the system meet adequate performance goals?
- Second, would adequate security meet market requirements?

SCSSI - France

The Service Central de la Sécurité des Systèmes d'Information (SCSSI) which became a certification body during the TMach Experiment, was interested in gaining a working knowledge of the UK and German certification processes. SCSSI was also interested in following a high assurance level (E5) evaluation of a non-trivial product, and in comparing the ITSEC and TCSEC approaches.

CSE - Canada

The interest of the Communications Security Establishment (CSE) in the TMach evaluation was in the harmonisation of criteria, and in the Mutual Recognition issues.

FMV - Sweden

Sweden's interest in the TMach evaluation was in gaining an understanding of the evaluation process in the UK and Germany.

2.2 Project History

2.2.1 Project Authorisation

In November 1990, James Burrows, the Director of the Computer Systems Laboratory of NIST, met with European officials and Stephen Walker of TIS to discuss initiating an evaluation of TMach against the ITSEC. As a result of this meeting, NIST finalised an agreement with the ARPA to co-ordinate and oversee the TMach evaluation work to be done by Germany and the United Kingdom (UK).

Under the agreement, NIST received funds from ARPA for the evaluations and negotiated the contracts with appropriate organisations in those countries.

2.2.2 Project Scope

On December 20, 1990, NIST published Commerce Business Daily (CBD) announcements notifying potential contractors of the solicitations for the TMach evaluation work. The intent of the contract work was to gain further understanding of the ITSEC and its evaluation process. The ITSEC evaluations of TMach began in September of 1991.

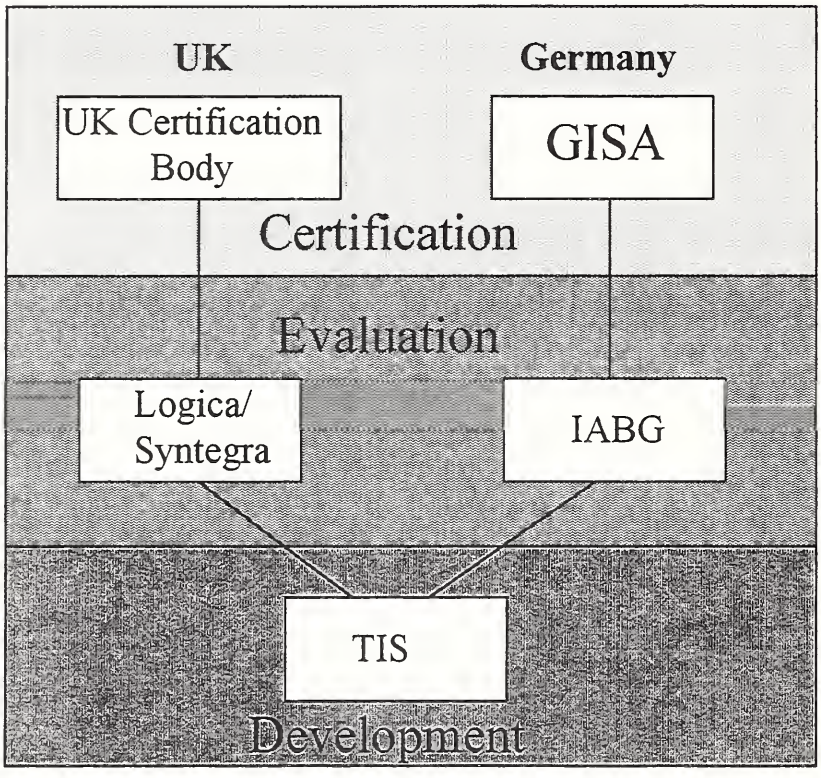
TMach, which was intended to provide users with both high level trust and a Unix interface, underwent evaluation by three different nations against two separate criteria. In the U.S., TMach was evaluated at the B3 level against the TCSEC, whilst in Europe there were concurrent evaluations of TMach at F-B3/E5 against the ITSEC. These multiple evaluations were undertaken with the objective of understanding the different criteria and evaluation processes by seeing how they relate to a single system.

The ITSEC evaluations of TMach were performed concurrently with the development of the product. This meant that the progress of the evaluation was critically dependent on the availability of evaluation deliverables (and in particular design documentation). It was not until September 1996 that TMach was in a sufficiently stable state for the evaluators to begin to plan the full set of evaluation activities required to complete the ITSEC E5 evaluation. TIS committed to provide the additional funding necessary to complete evaluation in the UK, with the evaluation team being built up to full strength in November 1996 for a target completion date of July 31st 1997. However, with the cancellation of the product development in January 1997, the ITSEC E5 evaluation was similarly brought to an end.

2.3 Evaluation Approach

Evaluation facilities in Germany and the UK are operated on a commercial basis under the control of national evaluation schemes. Scheme control covers both the technical review of evaluation methods and results, and adherence to a defined quality system which conforms to an international standard.

The TMach evaluation was conducted in parallel by evaluation facilities from each of the two countries, under supervision of the relevant national scheme bodies. These relationships are illustrated in the diagram below.



2.3.1 Evaluation phases

Evaluations in Europe are formally characterised as a three stage process as follows:

- Phase I - Preparation;
- Phase II - Conduct;
- Phase III - Conclusion.

The preparation phase has the following objectives:

- Ensure that all parties involved in the evaluation have a common understanding of the purpose and scope of the evaluation, and are aware of their responsibilities;
- Determine the suitability of the security target for evaluation;
- Examine available deliverables for their suitability for evaluation;
- Formalise the scope of the evaluation;

- Produce an Evaluation Work Programme (EWP) and a list of deliverables required.

The EWP describes the work which the evaluation facility proposes to undertake for the evaluation, and demonstrates that this is consistent with the chosen ITSEC assurance level (E5). It also provides and evaluation plan and details of the resources proposed.

The amount of work planned during this phase is flexible, particularly in relation to examination of deliverables. Sufficient work will provide all parties with some confidence in a successful outcome, and will allow the TOE to be formally accepted into the national evaluation scheme.

During the conduct phase the evaluators perform the technical evaluation work as defined by the EWP. As each work package is completed the results of the evaluation work performed are documented in the form of work package reports for inclusion in the Evaluation Technical Report supplied to the national evaluation authority. There may be one or more iterations involved if problem reports are raised which require updates to the evaluation deliverables, and hence examination of the updates by the evaluators.

In the conclusion phase the evaluation facility reports its findings and recommendations to the evaluation authority, which will examine these for compliance with scheme rules and will issue a certification report and certificate as appropriate.

The European schemes are characterised by continuous oversight of the evaluation process, achieved through regular progress meetings and early sight of results.

2.3.2 TMach approach

For the TMach evaluation the principal objective was to gain visibility of the evaluation process, rather than to achieve a successful evaluation result at minimum cost. The approach taken was therefore adjusted to provide a greater level of exposure to the European process. The German evaluation was undertaken in accordance with their standard practice, and began with an extended period of pre-evaluation work (Phase I). The UK team, however, determined to move quickly from Phase I into Phase II, to give exposure to the formal reporting processes required by that Phase. An additional perceived benefit of this approach was that a more formal application of the criteria and methodology would provide a better basis for the identification of underlying problems in the criteria and methodology. This latter approach required more formalised responses to draft deliverables than would have been made under Phase I.

2.3.3 Concurrent evaluation

The TMach evaluation was undertaken concurrently with the development of the product. This approach was appropriate for a number of reasons. Firstly, when the project was begun in 1991 the ITSEC had been published for only a short while, and there was little appreciation of the application of high assurance requirements. Therefore there was little

chance of a vendor being able to map the E5 requirements onto a set of design documents without assistance. This proved a correct assumption, since approaches to many of the ITSEC requirements had to be developed in parallel with the evaluation. Secondly, one of the objectives of the work (see section 2.1.2) was to establish whether a single documentation set could meet the requirements of both ITSEC and TCSEC evaluations, and, since a TCSEC B3 evaluation was already in progress, a parallel study was considered the best means of monitoring this and making appropriate adjustment to the content of deliverables.

2.3.4 Reporting

The project was operated within a structure of quarterly meetings. For most meetings a report was provided by both the UK and Germany, which described the results of the work performed. Since the UK had adopted a more formal approach to the process this report was structured as an interim ETR, providing a similar reporting level to that during any evaluation. The German report was a less formal report on progress and results.

As the UK was performing a formal evaluation throughout, any non-compliance with ITSEC requirements was also reported through the UK system of Evaluation Observation Reports. This enables each issue to be clearly identified and tracked through proposed response and resolution.

2.3.5 Evaluator independence

An important principle within the evaluation process is that the assessment of deliverables is independent of their production. The concurrent evaluation approach brings the evaluators closer to the development process, and requires discretion in the advice being provided. During this type of evaluation there is inevitable pressure from the developer for the evaluator to define an approach to meet the ITSEC requirements, which has the potential to compromise the independent assessment. Potential compromise was monitored during the project through the presence of German and UK certification body representatives at progress meetings, and by other regular contact with the certifiers. In the UK and Germany, this issue would normally be addressed by the use of separate teams for consultancy and evaluation, which, although it can lead to training overheads, removes the problem. For practical reasons this approach was not adopted on this project, and hence greater oversight was required.

2.3.6 Evaluation team

The evaluation team was retained almost in its entirety throughout the 5 year duration of the project. The German team retained 3 out of 4 evaluators over this period, and the UK team also 3 out of 4. This minimised the need for retraining of evaluation staff, and enabled relationships between evaluators and developers to be maintained over a long period.

3. KEY RESULTS

This section presents the key results of the TMach Experiment, describing:

- the differences observed between the US and European evaluation processes;
- the differences observed between the UK and German evaluation processes;
- the additional evidence the developer had to provide in order to satisfy the ITSEC E5 assurance requirements;
- the evaluation findings relating to the application of ITSEC F-B3/E5 requirements, and the interpretations that were necessary;
- the differences discovered between ITSEC F-B3/E5 and TCSEC B3;
- the impact the TMach evaluation had on the development of such initiatives as the ITSEM, the Federal Criteria, and the Common Criteria.

3.1 Differences in Evaluation Processes

A major benefit of the TMach Experiment for all participants has been to learn about the differences between evaluation processes in the US, UK and Germany. *Process* here means not only the formal organisation of an evaluation project (as shown in Figure 4.2.1 of [ITSEM]) but also how the single work items of an evaluation are conducted. This means that the approach and the philosophy are also addressed here. The goal of this exercise has not been to fight political battles by pointing out weaknesses in each others processes but rather:

- to come to a common understanding of the evaluation process and the underlying philosophy;
- to identify possibilities for misinterpretation and existing weaknesses that should be avoided when harmonising the evaluation process between North America and Europe;
- to identify strengths of each approach that could be used in a harmonisation process[2].

This section will provide an overview of the lessons learned within the TMach Experiment about differences and common points between the evaluation processes in the various countries.

---

[2] Three participants (Murray Donaldson, Chris Ketley and Gene Troy) and one observer (Steve LaFountain) in the project became CCEB members.

3.1.1 Comparison of Evaluation Processes in the US and UK/Germany

This section focuses on the comparison of the two processes, specifically pointing out the differences between them. Of course there are also many common points, e.g.:

- both processes are based on security criteria issued by the government;
- both processes lead to an independent assessment of the security of IT products;
- both processes are overseen independently by a government body;
- both processes lead to a government approved certificate.

Whilst this section does not go into the details of each of the processes, a brief overview is provided first in order to give some background. This comparison is drawn from the experiences in UK and Germany. There may be other differences with respect to other national schemes (e.g. the French scheme).

The US Process

The evaluation process in the US is documented in [NCSC-TG-002], partly superseded by [TPEPP]. The 'Trust Technology Assessment Program' (TTAP) was set up during the time span of the TMach Experiment and was partly influenced from the experience gained from that project.

The following overview shows the participants within the process with their actions and duties for the three phases Pre-Evaluation, Evaluation and Post-Evaluation (RAMP) described in [TPEPP]:

Pre-Evaluation

NSA:

- provides information on TPEP;
- reviews product proposal;
- participates in Technical Assessment (TA);
- gives advice to vendor;
- participates in Intensive Preliminary Technical Review (IPTR);
- prepares the Initial Product Assessment Report (IPAR);
- decides whether product should be evaluated.

Vendor:

- provides product proposal;
- participates in TA;
- participates in IPTR;
- provides deliverables for TA and IPTR.

Evaluation

NSA:

- signs Evaluation Agreement;
- implements evaluation team;
- implements the Technical Review Board (TRB);
- conducts evaluation;
- includes product into Evaluated Product List (EPL);
- issues a Final Evaluation Report.

Vendor:

- signs Evaluation Agreement;
- provides deliverables for evaluation;
- provides training for NSA evaluation team;
- provides Vendor Security Analyst as a member of the evaluation team;
- changes product / documentation as required by NSA.

Post-Evaluation - Rating Maintenance Phase (RAMP)

NSA:

- approves Rating Maintenance Plan (RM Plan);
- trains Vendor Security Analyst (VSA) for RAMP;
- holds RAMP boards;

- staffs Technical Point of Contact (TPOC).

Vendor:

- provides Rating Maintenance Plan (RM Plan);
- responsible for following Rating Maintenance Plan;
- staffs Vendor Security Analyst (VSA);
- presents analysis at RAMP boards;
- responsible for security analysis of changes.

The European Process

The European evaluation process based on [ITSEC] is documented in chapter 4 of [ITSEM]. The pre-evaluation and post-evaluation phases are not covered by [ITSEM]. For more details on the process see section 2.3 *Evaluation Approach*.

The following overview shows the participants within the process with their actions and duties in the evaluation process according to [ITSEM]:

Evaluation:

Developer / Sponsor:

- provides evaluation deliverables;
- makes changes required by the ITSEF.

ITSEF:

- provides Evaluation Work Programme (EWP);
- provides Problem Reports;
- provides Evaluation Technical Report (ETR).

Certification Body:

- 'shadows' evaluations;
- provides advice on writing security target;
- gives advice on criteria interpretations;

- issues certification report;
- issues certificate.

Accreditation and Licensing Body:

- accredits and audits ITSEFs.

Differences between the Processes and Approaches

The TMach Experiment, in performing three evaluations in three different countries in parallel, provided an optimal platform for comparing evaluation processes and approaches not only based on paper work but on real world experience. As stated above this section does not only take the formal process into account but also points out differences in evaluation approach and philosophy. Due to the limited information flow from the evaluation to the European evaluation team the picture on differences concerning the evaluation approach may be incomplete. The following sections are based on the evaluators' observations regarding the US evaluation process.

Transparency of the Evaluation Process:

While the formal evaluation procedures of the US and the Europe are both documented in detail (see above), only [ITSEM] gives information about how the real evaluation work is done. The description of the US process sticks with the formal process. Published documentation does not describe how an NSA Orange Book evaluation is performed in practice. This may create difficulties, for vendors in particular.

Commercial vs. Government Domination of the Process:

The US process is entirely controlled by the government (NSA) as opposed to the European process. In Europe the bulk of the work is performed by commercial companies (the ITSEFs). The government is involved in the certification and accreditation process by overseeing the commercial ITSEF's work, thus ensuring that the ITSEFs are working according to the principles of [ITSEM]. It is the evaluators' opinions that this government domination in the US process has the following impacts:

Negative Impacts:

- There is limited commercial pressure at NSA, which can lead to long evaluation time spans for the products. As a result, the products may be no longer up to date when the certificate is awarded (i.e. the product life cycle is shorter than the evaluation time). This hinders significantly acceptance in the commercial area.
- The NSA can refuse to evaluate a product based at its discretion whether the product is worth evaluating and has its marketplace. Therefore there is more freedom in the

European evaluation market where a vendor can choose an ITSEF, contract with it and perform the evaluation as long as he is willing to pay.

- The NSA tends to be prescriptive with respect to security architecture features. The NSA insists on special techniques that have to be used in order to achieve security (such as the reference monitor or the Multics-like ring architecture). With European evaluations, the architecture of security functions is not prescribed. As long as the implementation is correct and effective with respect to the Security Target, the evaluators do not mandate how the security functions are to be implemented.

- Practice in the TMach project suggested there is less stability in evaluator teams in US evaluations. US evaluation team members appear to use their gained security knowledge to take on better paid jobs. This can lead to additional delay in US evaluations. The European process allows commercial ITSEFs to pay their knowledgeable evaluators competitive salaries.

Positive Impacts:

- NSA's main goal is 'waterproof security'; they are not forced to speed up due to commercial pressure. This pressure allows European ITSEFs to do only what is required. NSA has resources to do a much wider assessment, which might lead to a more careful examination of the product security.

- The existence of a single evaluation body in the US (NSA) allows for a free exchange of ideas leading to highly consistent evaluation approaches and results. In Europe, where ITSEFs are in competition, such a free exchange is more difficult, and the task of national bodies to ensure consistency is harder.

Differences implied by Approach / Criteria Differences

The following paragraphs list differences between the two processes that are due to differences in the criteria on which the evaluation process is based and which also reflect different approaches in evaluation. Some of the items (such as separation of assurance and functionality) did not have immediate impact on the TMach Experiment work but are also listed.

- Separation of assurance and functionality in the European criteria [ITSEC]: This offers more flexibility than the US criteria (Orange Book) which couples assurance and functionality, both rising with the evaluation level. The [ITSEC] allow small products to be evaluated to high assurance levels. (This feature is strongly coupled with the next item.)

- Individual definition of Security Enforcing Functions (SEFs) in the European criteria [ITSEC]: Again, this approach is much more flexible. The vendor / sponsor / developer can specify exactly the security functionality that is implemented by the product, and

against which the product is evaluated, in the Security Target document. But ITSEC also allows the use of pre-defined functionality classes. The Orange Book approach ran into difficulties here because it is focused on operating system functionality. It took significant efforts to correct this bias by issuing "interpretations" that gave guidelines how Orange Book requirements can be applied in other contexts such as databases, networks etc. ([NCSC-TG-005], [NCSC-TG-009], [NCSC-TG-021]).

As a drawback of this flexible approach, practice (also in the TMach Experiment) showed that vendors can be overwhelmed by that flexibility and find it difficult to use. Whereas in the US process they only must state the intended evaluation level of the product, in Europe he has to provide a Security Target stating the SEFs as well as other details such as the intended method of use, threats and intended technical environment. Many vendors therefore need expert support to write the Security Target in a pre-evaluation activity. Within the TMach project, the ITSEC Functionality Class F-B3 was chosen to keep the experiment focused on TCSEC and ITSEC similarities and differences at B3.

- Evaluation of the Development Process in Europe: The European evaluation approach takes the development process of the product much more into account than the US. [ITSEC] puts many requirements on the development process which increase with higher assurance levels. The expectation here is that a product that is developed following "good" development and quality assurance practices can be more trusted to implement the SEFs stated in the Security Target.

- Focus on Evidential Process in Europe: The European evaluation process requires the vendor to provide documentation that is sufficient to give the evaluators the necessary evidence that the ITSEC requirements are fulfilled. The US process is less structured in the sense that evaluators have to extract evidence from whatever documentation is provided and out of interaction with the vendor (e.g. verbal explanations). However, US evaluators can (and do) request additional documentation from vendors concerning any item of interest or contention. So while the European process (at first sight) puts more workload on the vendor, this pays off in the long run. Evaluation costs on the vendor side tend to be lower under European schemes due to the better defined evidential process.

3.1.2 Comparison of Evaluation Processes in the UK and Germany

This section focuses on the comparison of the two processes, specifically pointing out the differences between them. Of course this focus should not hide the fact that they are essentially the same and that the differences between the processes are of minor significance.

In order to get some understanding why there are at all differences between the UK and German processes although they both evaluate according to [ITSEC] / [ITSEM] one has to consider the historical background. Both countries had set up their evaluation processes

before [ITSEC] / [ITSEM] was available and had experience in evaluation. From this starting point UK and Germany together with France and the Netherlands started a harmonisation effort to have common evaluation criteria. The result was the agreement on the [ITSEC], which was mainly an agreement on wording and not necessarily on the underlying philosophy. The preparation of [ITSEM] (which was significantly influenced by the TMach project) improved the situation by providing a common ground for evaluation methodology, although [ITSEM] is intended only to define the process to the level necessary for mutual recognition. Differences below this level arise from national approaches developed over a long period, but are deemed to have no impact on the validity of the results. Therefore UK as well as German evaluators still have their 'former approaches' and use these when evaluating according to [ITSEC] / [ITSEM]. This leads to some differences which are listed in the next section.

Differences between the Processes and Approaches

The TMach Experiment provided an optimal platform for comparing evaluation processes and approaches in the UK and Germany. One has to take into account the fact that an E5 evaluation of an operating system (i.e. a complex product) according to [ITSEC] was being performed for the first time. This meant there was little experience on either side (ITSEFs and Certification Bodies) although there was experience with high assurance evaluations prior to ITSEC. This parallel 'trial' evaluation effort revealed that there are differences but also that these differences did not affect evaluation results, thereby validating the ITSEM approach. Nevertheless the following list focuses on the differences identified.

Importance of the Development Process:

In the UK there is a greater emphasis on checking the development process (see above, differences between US and Europe). For example, according to the UK process the (semi-)formal specifications required by [ITSEC] should be used in the development process of a secure system in order to increase assurance, whereas according to the German process the (semi-)formal specifications required by [ITSEC] should be used in addition to informal specifications as a guide to get a higher level view and better understanding of the system in order to increase assurance. Nevertheless, both approaches lead to more assurance.

3.2 Development Process

This section describes the development process adopted by the developer and how it was adapted in response to meeting the ITSEC E5 requirements.

3.2.1 Security Target

The developer originally put forward the TMach *Philosophy of Protection* document as the Security Target for the ITSEC E5 evaluation. This approach was rejected by the

evaluators for the reasons stated in section 3.3 below. The developer therefore produced a separate Security Target document, but expressed the hope that this could be a 'generic F-B3 or B3 ST'. Whilst the evaluators considered that this was a reasonable aim, not precluded by ITSEC, and that much of the information relating to the threats and SEFs would be common to all Security Targets claiming strict conformance to ITSEC F-B3, it was also realised that ITSEC calls for a certain amount of product-specific information in the Security Target. The Philosophy of Protection was therefore referenced by the Security Target to provide appropriate background details.

The Security Target produced contained requirements that were additional to the requirements of the F-B3 functionality class. This approach was not strictly necessary in order to satisfy the ITSEC E5 requirements, but rather was a matter of choice by the developer (albeit subject to the evaluation of the Security Target as described in section 3.3 below).

ITSEC E5 requires the developer to use a *semiformal* specification of the SEFs. The developer considered use of the Claims Language as defined in ITSEC Annex B, but rejected this as unusable, even though a Claims Language version of F-B3 was available; instead they adopted the approach as described in [SADSEF]. The [SADSEF] approach requires security enforcing functions to be expressed in the form of predicate logic constructs, and uses a restricted set of English to represent the constructs used. In particular, the following are used:

- Universal and Existential Quantifiers;
- Logical connectives *and* and *or*;
- Logical connectives *if*, *only if* and *if and only if*.

During the course of the evaluation, the developer made some significant changes to the Security Target. These changes required the evaluators to re-examine the Security Target as described in section 3.3 below. The two most significant changes were:

- Removal of two SEFs following a major change to the system architecture. Both SEFs were additional to the requirements of F-B3, and were features that were specific to TMach, relating to the controls over the use of **setuid** functionality. These security features were no longer required following the change to the system architecture.
- The developer subsequently discovered that it was necessary to re-word some of the SEF specifications when they attempted to trace the SEFs into the design, so as to clarify their intended meaning. This was because in some specific cases the wording of a SEF was found to give rise to ambiguities.

3.2.2 Design

System Architecture

Part way through the project, the developer implemented a significant change in the architecture of TMach. A side effect of this change was that it was necessary for the developer to revise the Security Target by removing two SEFs which related to TMach-specific functionality that was no longer required. These changes required the evaluators to repeat their examination of the system architecture; however, the change to the system architecture did not, in itself, present any obstacle to TMach satisfying the ITSEC E5 architectural design requirements.

It should be noted that it would not normally be expected that a change to the system architecture would require changes to the Security Target.

Design Methodology

The developer adopted an Object Oriented Design approach for the development of TMach. This was compatible with the ITSEC E5 requirement for *significant use of layering, abstraction and data hiding* in the detailed design. The approach did not otherwise have any impact on the ability of the design to satisfy the ITSEC E5 requirements. However, the developer came to the conclusion (late in the project) that although the PDL satisfied the requirement for a semiformal detailed design (see below), it did not aid the understanding of an object oriented design.

A key issue for the design process was the ITSEC E5 requirement to provide semiformal descriptions of the architectural and detailed designs. This led to detailed discussion concerning the purpose served by the use of semiformal notations; this resulted in a number of interpretations being agreed, as described in section 3.3 below.

In response to the requirement, the developers created their own semiformal notation for describing the key interactions between architectural design components, and documented the syntax and semantics of this notation. This satisfied the ITSEC requirements for a semiformal notation.

At the detailed design level, the developer was already producing module specifications in PDL, which constituted a semiformal notation. The developer continued with this approach until late in the project when they modified their approach to documenting the detailed design so as to aid understanding of the design. Again, the developer created a semiformal notation for this level of design.

A more general issue for the design process was the question of whether ITSEC mandates or has a preference for one particular development methodology over another. Specifically, the developer expressed a perception that ITSEC was too biased towards the traditional 'waterfall' development methodology, and that this can present problems where

the developer adopts a cyclic/spiral development process in an evaluation carried out concurrently with the development.

In fact, the ITSEC does not 'prefer' any particular design methodology: ITSEC is a set of *evaluation* criteria and lays down requirements for the provision of *evaluation* evidence. The organisation and presentation of these criteria reflects the necessary order in which the evaluator actions are performed, which is 'top-down'. In other words, the evaluator's analysis has to begin with the security target, progressing through the design levels to the implementation, operation and testing of the TOE. ITSEC therefore defines the order in which the evaluators must *examine* the evaluation evidence; however, it does not prescribe the order in which a developer must *produce* the evaluation evidence.

Traceability Evidence

In order for the developer to satisfy the ITSEC E5 requirements in respect of demonstrating the tracing of the SEFs through the design representations, they had to provide additional documentation. The ITSEC requires the developer to demonstrate the instantiation of each security function through the design to the implementation, and at high assurance levels this traceability requirement must be met to a high level of granularity. In many cases the approach taken to design does not allow easy mapping of security functions, since each may be implemented by a combination of elements within different parts of the system. The ITSEC requires more explicit information in this area than does the TCSEC, the latter requiring more evaluator effort to achieve a similar end.

Security Mechanisms

ITSEC defines a *security mechanism* as *the logic or algorithm that implements a particular security enforcing or security relevant function in hardware and software.* ITSEC uses the term *mechanism* in a number of requirements applicable at ITSEC E5:

- in the Security Target a statement of *required security mechanisms* may be optionally included;
- in the detailed design there is a requirement for an identification and specification of security mechanisms, mapped onto functions and components, describing how the SEFs are provided;
- in the test documentation there is a requirement for an explanation of the security mechanisms identifiable in the source code and/or hardware drawings;
- in the binding analysis there is a requirement for an analysis of interrelationships between SEFs and mechanisms;
- in the strength of mechanisms analysis there is a requirement for analysis of the strength of *critical mechanisms*;

- in the ease of use analysis there is a requirement that human or other operational error which deactivates security enforcing functions or mechanisms is easily detectable.

There was much discussion of the meaning of the term *mechanism*. It was generally agreed that the term was used in different contexts with different meanings; a mechanism can be specified at any level of abstraction. For the detailed design, the interpretation agreed for this evaluation was that use of the term was a matter for semantics only: as long as there is traceability of the SEFs throughout the design levels it does not matter whether areas are explicitly identified as mechanisms or not. There was therefore no need for the developer to amend the design documentation to address this particular ITSEC E5 requirement.

Other discussions relating to the application of the term *mechanism* centred on the effectiveness analyses, as described in the following section and in section 3.3 below.

3.2.3 Effectiveness Analyses

The original approach adopted by the developer (in line with their stated objective of discovering whether the TCSEC evaluation deliverables could also satisfy the ITSEC requirements) was to present the TMach *Philosophy of Protection* document as fulfilling the ITSEC E5 requirements for a suitability analysis, binding analysis and strength of mechanisms analysis. As reported in section 3.3 below, the evaluators found that, although there was much in the document that was of relevance to these effectiveness analyses, it did not fully satisfy any of the applicable ITSEC requirements. Thus it was concluded that separate effectiveness analyses would be required to meet these criteria.

The developer did not attempt to provide these analyses until some time after a (relatively) stable Security Target had been produced. However, the developer did produce an 'Effectiveness Analysis Plan' to describe the intended approach, and presented this to the evaluators for assessment. For the binding and strength of mechanisms analyses in particular, this centred on a defined list of security mechanisms within TMach which would be used as a basis for these analyses.

A significant part was to be played by the developer's covert channel analysis; specifically, this was to go a significant way to satisfying the requirement for a list of known vulnerabilities in the construction (i.e. specification, design and implementation) of TMach. Indeed, the developer stated an intention to remove all known vulnerabilities other than covert channels, in which case the covert channel analysis would have fully satisfied this particular ITSEC requirement.

During discussions on covert channel analysis, the evaluators queried how the developer was intending to handle different hardware platforms. The developer explained that the plan was to provide a hardware independent analysis, with 'top-up' analyses provided for different hardware platforms. This was considered appropriate for ITSEC E5.

Towards the end of the TMach Project, the developer observed that the effectiveness analyses had had no tangible impact on the development of the product. However, it should be noted that the ITSEC, in calling for the six effectiveness analyses, is requiring the developer to present a case as to why the product contains no (known) vulnerabilities that can be exploited within the intended environment. A developer who has developed a product based on sound security principles should be able to construct such a case with relative ease, and not have to revise the TOE design or implementation as a result. Of course, it should also be pointed out that the evaluators did not have the opportunity of completing *their* effectiveness analysis and penetration testing, and may therefore have discovered vulnerabilities which *would* have required changes to TMach.

3.3 Evaluation Findings

This section documents the evaluator's findings in relation to the application of the ITSEC E5 requirements, and describes the interpretations of those requirements as agreed between the UK CB, evaluators and developer. It should be noted that not all of these interpretations represent official UK or German policy, although some have subsequently been reflected in the ITSEC Joint Interpretation Library [JIL] (which documents agreed interpretations of the ITSEC raised by the UK, Germany, France and the Netherlands).

A full summary of the evaluation results is provided in the Final ETR produced by the UK evaluation team, which has restricted distribution. The overall result was that TMach had not satisfied the ITSEC E5 requirements. This verdict does not, however, mean that the evaluators considered TMach to be an insecure product, but rather is a reflection of the fact insufficient evidence had been provided to the evaluators, by the time the product development was cancelled, to enable the evaluators to complete their analysis and perform functional and penetration testing.

This section is structured according to the standard ITSEC evaluation approach which was adopted for the TMach evaluation. The principal evaluation activities (at ITSEC E5) are as follows:

- The evaluators first examine the Security Target and the formal model of the underlying security policy to determine that the security requirements against which the TOE will be evaluated form a clear, coherent and consistent specification.

- The evaluators then analyse the design and source code implementation to establish assurance that the SEFs specified in the Security Target are correctly provided. A significant part of this activity is that of *traceability analysis*, in which the evaluators attempt, using the evidence provided by the developer, to trace each SEF through the design representations into the source code. This not only establishes confidence in the correctness of the SEFs, but also provides the evaluators with a level of understanding of the TOE design and implementation necessary for their independent vulnerability analysis and penetration testing.

- The evaluators examine the developer's test evidence to check the coverage achieved, and perform their own functional testing of the TOE based on a combination of repeating a sample of the developer's tests (to provide corroboration of the reported results), and of performing additional tests to those specified by the developer.

- The evaluators also examine the environment in which the TOE was developed (the Development Environment) and the environment in which the TOE is to be used (the Operational Environment).

- The evaluators examine the sponsor's effectiveness analyses to determine whether they concur with the case put forward by the sponsor that the TOE is free from any known exploitable vulnerabilities.

- Finally, the evaluators perform their own independent vulnerability analysis, drawing on the understanding of the TOE they have gained from all other evaluation activities, and on the results of those activities with a view to identifying potential vulnerabilities in the TOE. These are then converted into penetration tests which the evaluators perform as the final evaluation activity (apart from, of course, reporting the results) in order to confirm or disprove whether the potential vulnerabilities identified are exploitable.

3.3.1 Security Target

As described in the preceding section, the developer originally put forward the TMach *Philosophy of Protection* document as the Security Target for the ITSEC E5 evaluation. However, the evaluators found that this document did not satisfy the ITSEC E5 requirements for a Security target because:

- it gave no clear statement of the SEFs, and in particular did not include a semiformal specification of the SEFs;

- it did not include a product rationale.

The developer therefore produced a separate Security Target document containing the required details. The Philosophy of Protection was referenced to provide appropriate background details, such as the definitions of subjects and objects.

There was discussion as to what constituted a 'Security Enforcing Function' (SEF) in the Security Target. The developer put forward the argument that there were 5 SEFs in the Security Target: Identification and Authentication, Access Control, Audit, Trusted Path, and Security Administration. The evaluators pointed out that the generally accepted interpretation was that the SEFs were the individual functional requirements that were specified under each SEF group heading.

The developer accepted this argument, and revised the Security Target accordingly. However, they expressed concern that there could be problems when tracing the SEFs

into the architectural design, since some of the details specified in the SEFs (e.g. information recorded in the audit trail) might not be visible at this representational level. The evaluators did not (because of the incompleteness of the evidence supplied) have the opportunity of determining whether there were any such traceability problems in practice.

The TMach Security Target specified requirements relating to covert channels (in terms of acceptable bandwidth and auditing of their use), but in so doing followed an unofficial interpretation of the TCSEC. This was not considered a problem with respect to compliance with ITSEC F-B3, since the F-B3 requirements are somewhat vague and in any case the intent of ITSEC F-B3 is to be consistent with the TCSEC B3 requirements. It was considered acceptable to follow the NSA guidelines providing these were properly documented. The evaluators noted, however, that this would introduce an inconsistency in the Security Target, which the developer resolved by excluding covert timing channels from the statement of threats. This was accepted by the evaluators insofar as the ITSEC E5 requirements for a Security Target were concerned; they did not, however, have the opportunity to determine whether this exclusion resulted in any problems when the ITSEC effectiveness requirements were fully applied.

The changes made to the Security Target during the course of the evaluation (as described in the preceding section) required the evaluators to examine the changes to ensure that the modifications to the SEFs did not either:

- introduce any ambiguities or conflict with other SEFs; or
- introduce any vulnerabilities as a result of any of the identified threats being inadequately countered by the SEFs.

3.3.2 Formal Model

ITSEC E5 calls for a formal model of the underlying security policy, but does not require that the model cover all SEFs in the Security Target [ITSEC 2.82]. The agreed interpretation for this evaluation was that the formal model for TMach provided adequate coverage of the F-B3 requirements by modelling only the access control SEFs (i.e. MAC and DAC). However, it was necessary, in order to satisfy the ITSEC E5 requirements, for the developer to provide an informal interpretation of the formal model in terms of the Security Target.

There was some discussion concerning the ITSEC requirement that the model be 'capable of proofs', and whether this required formal proofs to be provided. The developer updated the model to include full proofs in some cases, with an indication of how the proofs could be generated in the other cases. The proofs were examined and found to be acceptable.

3.3.3 Architectural and Detailed Design

There were two key aspects to the evaluators' assessment of the architectural and detailed design against the ITSEC E5 requirements, namely:

- validation of the semiformal descriptions (which comprised the use of semiformal notations with supporting informal descriptive text);
- traceability analysis of the SEFs.

Semiformal Design

Discussions relating to the requirements for the use of semiformal notations in the design, and their purpose, resulted in the following interpretations being agreed:

- It is acceptable to use more than one notation in the development, providing the ITSEC requirements are met for each notation.
- If one of the design levels (architectural or detailed) is broken down into layers, it is not necessary to provide a semiformal representation for each intermediate layer.

  (Note: ITSEM 4.5.56 indicates it may, however, be necessary to make use of more than one semiformal notation to provide a complete picture of the architectural design.)
- The Interface Specifications, because they follow a restricted notation or format, can be considered as a semiformal representation.
- The mapping from one level of design to the next (i.e. traceability information) does not have to be semiformal. However, if this mapping is provided in the form of a table, this can be regarded as semiformal.

Ambiguity was noted in the ITSEC E5.5 and E5.8 requirements. Both make use of the word 'it', which could be interpreted as referring to either the semiformal description of the design, or the design as a whole. After much discussion, it was eventually agreed that this apparent ambiguity was not a problem in practice, as the two interpretations are effectively the same. It is difficult to gain a full understanding of the design by examination of the semiformal specification alone: a semiformal design will therefore normally include some accompanying informal text. Therefore, a design which incorporates the use of semiformal notation(s) together with informal prose is considered to constitute a 'semiformal description' (subject to the note regarding ITSEM 4.5.56 above). Each of the individual requirements of ITSEC E5.5 and E5.8 that are preceded by 'It shall' are therefore to be satisfied by some part of that description.

Evaluation proceeded on the basis of these interpretations, but progress was restricted by the incompleteness of the architectural and detailed design evidence provided to the evaluators during the course of the project.

Later discussions between the developer and evaluators concerned the completeness of the semiformal architectural diagrams; in other words, which were the 'key' interactions that needed to be represented semiformally. The evaluators took the position that completeness would be judged with respect to the tracing of the SEFs: where two or more components interact to provide a SEF, this should be shown by use of the semiformal notation. The evaluators did not, however, have the opportunity of applying this approach in practice.

Traceability Analysis

ITSEC defines requirements for the traceability of SEFs. It was generally agreed that the evidence did not have provide a mapping at each level back to the Security Target (as might be thought from a literal reading of the ITSEC requirements), but rather that a step-by-step mapping through each representational level was acceptable. This established the principle of the transitivity of the tracing of the SEFs.

Again, the incompleteness of the architectural and detailed design evidence severely constrained the amount of work the evaluators could perform in this area (traceability analysis traditionally gives rise to a significant proportion of the problem reports raised in an ITSEC evaluation). In the limited number of cases where the evaluators were able to perform traceability analysis, they found a small number of problems in the application of the developer's approach to documenting how the SEFs were provided, but no significant problems in the approach itself.

3.3.4 Source Code Examination

The evaluators were able to examine a sample of the source code (not the definitive version) for two of the servers within TMach. This did not identify any significant problems, although some observations were made concerning the correspondence between the detailed design and source code.

3.3.5 Developer Testing

The evaluators were able to assess the developer's test plans as a basis for meeting the ITSEC E5 requirements. However, the evaluators were not provided any test specifications or results during the course of the TMach evaluation, and were therefore not in a position to validate the approach in practice.

There was discussion as to whether ITSEM mandates 100% test coverage at the source code level at ITSEC E5. The agreement reached was that as ITSEC E5 calls for a *rationale* for the test coverage achieved, 100% coverage cannot be an absolute requirement (if 100% coverage is achieved then there is no need for a rationale, other than justifying the claimed level of coverage). ITSEC E5 does not require testing of every branch or statement within the source code: ITSEM 4.5.72 is not a mandatory requirement.

Rather, the intent is that 100% coverage is a goal; where 100% coverage is not achieved a rationale is required from the developer. If the evaluators can subsequently show that some security enforcing interfaces are not tested, and that it is possible for them to be tested, then they will request the developer to perform more tests.

The following related interpretations were also agreed:

- Although module testing is one way of satisfying the ITSEC requirements in respect of code and detailed design coverage, these requirements can also be met through testing at the TCB interface, providing there are sufficient tests to cover the internal interfaces to security enforcing components. An explanation (rationale) must be provided as to why the coverage is sufficient, and also why any routes through the code that are not tested cannot be tested.

- Documented code reviews may be considered as a form of module testing, and thus may be presented as a contribution to satisfying the source code coverage requirements.

The developer did not, however, provide the intended evidence, and so the feasibility and validity of their proposed approach to meeting the ITSEC E5 requirements were not demonstrated.

3.3.6 Development Environment

The evaluators visited the TMach development environment to check the application of configuration control and security procedures. The only significant issue raised related to developer's security: ITSEC E5 calls for an explanation of the security procedures and how they protect the integrity of the TOE and the confidentiality of its associated documents. However, for TMach, the confidentiality of the documentation was not a significant concern; indeed some design documents were intended for the public domain. The following interpretation was agreed:

- The essential requirement is that the integrity of the TOE is protected. It is acceptable (in this particular evaluation at least) for the developer to have no confidentiality requirements, provided the information on developer's security explains what the policy is. (Note that there may be cases where confidentiality *is* a legitimate concern.)

3.3.7 Operation

The evaluators were able to examine draft copies of the Security Features User Guide (SFUG) and Security Administrator's Guide (SAG). No significant problems or issues were found.

No evidence was provided during the course of the project relating to the operational environment procedures. However, discussion of the requirements relating to the

installation of the product (system generation) led to the following interpretation being agreed:

- Generation of an audit record at boot time recording the security configuration is sufficient to meet the ITSEC E5.32 requirement. The developer should keep a record of how the system was built (e.g. 386/486 make options) to meet the generation requirements. There is no requirement for an audit record of configuration options selected at the customer's site: a manual record of sysgen options would be adequate, as per ITSEM 6.3.60(b).

3.3.8 Effectiveness

As noted in section 3.2 above, the developer put forward the Philosophy of Protection as the ITSEC suitability analysis, binding analysis and strength of mechanisms analysis. However, the evaluators' assessment of this document against the relevant ITSEC E5 concluded that it did not fully satisfy any of these requirements. The developer therefore produced (or undertook to produce) separate analyses to satisfy the ITSEC E5 requirements.

Suitability Analysis

The developer presented a suitability analysis which the evaluators assessed against the ITSEC requirements. No significant problems or issues were raised, and no significant interpretations were necessary.

Binding Analysis

The developer presented a binding analysis based wholly on interactions between the SEFs identifiable at the level of the Security Target. The evaluators raised concerns about the lack of use of design details in the analysis. It was expected that use would be made of the architectural design in particular to identify and analyse interrelationships between SEFs and mechanisms. Indeed, according to ITSEC figure 4, the detailed design and implementation levels would also have to be used in the analysis at ITSEC E5. After some discussion, the following agreed interpretation was reached:

- The effectiveness analyses as a whole must address all the information specified in ITSEC figure 4. However, some flexibility is allowed as to which effectiveness analysis covers any particular aspect. For example, it would be acceptable for the binding analysis to confine itself to analysing dependencies at the architectural design level (cf. ITSEM 0.2.39), provided that the construction vulnerability assessment addresses any vulnerabilities arising from dependencies introduced at the detailed design or implementation levels, e.g. covert channels.

It was also noted that ITSEC figure 4 refers to a 'vulnerability analysis', which according to ITSEC 3.4 is the sum of the effectiveness analyses. Thus the requirement to consider

information in ITSEC figure 4 applies to the effectiveness analyses as a whole rather than to individual analyses. This apparent error in ITSEC is, to some extent, mitigated by 'revised' definitions of suitability analysis and binding analysis in ITSEM 0.2.66 and 0.2.39 respectively.

The developer responded with an updated analysis which went some way to addressing these concerns, although some specific issues remained. The evaluators did not have the opportunity of assessing the binding analysis based on their understanding of the product as gained from a complete evaluation of the architectural design.

Strength of Mechanisms

There was considerable discussion of the concept of strength of mechanisms and how it was intended to be applied in practice. The following agreed interpretations were made:

- For the purposes of the strength of mechanisms analysis, security mechanisms should be considered at a high level of abstraction.

- The strength of mechanisms analysis needs only consider the strength of critical *Type A* mechanisms[3] (evidence presented to the evaluators indicated that the password mechanism was the only such mechanism within TMach). However, a justification must be provided as to why other critical mechanisms are categorised as *Type B*.

With regard to the second interpretation, it should be noted that much of these discussions preceded the ITSEM which introduced the concept of *Type A* and *Type B* mechanisms. Indeed, it was largely as a result of the TMach evaluation that these concepts were recognised and introduced[4].

A strength of mechanisms analysis was presented for evaluators. No significant issues or problems were raised. The evaluators did not, however, have the opportunity of validating the claimed rating by penetration testing.

Covert Channel Analysis and Effectiveness

---

[3] Type A mechanisms are those that can be defeated by direct attack, and for which a strength rating can be assigned. Type B mechanisms cannot be defeated by direct attack, although they could be defeated by indirect attack.

[4] The JIL subsequently modified the definition of *critical mechanism* so as to exclude *Type B* mechanisms, i.e. only *Type A* mechanisms are now considered to be *critical*. This does not, of course, mean that the concepts are any less valid, because the developer and evaluator still have to decide which mechanisms could be defeated by direct attack even if they are perfectly conceived and implemented; in other words they must still identify which are the *Type A* mechanisms (and, by inference, which are *Type B*), even though the *Type A / Type B* labels may no longer be used.

There was some discussion as to how the developer's covert channel analysis related to the ITSEC effectiveness requirements. The analysis of the bandwidth and disposition (by elimination, reduction or auditing) of identified covert channels was unanimously seen to be part of the Construction Vulnerability Assessment. The question remained as to whether the *analysis* for covert channels fell under the heading of binding analysis (the general UK view) or Construction Vulnerability Assessment (the German view). This apparent difference in view was, however, simply a further manifestation of the ITSEC Figure 4 problem (see above); the heading under which the analysis is placed is, ultimately, of no importance: what matters is that covert channel analysis is addressed in an ITSEC evaluation where covert channels are identified as a threat.

Discussion also led to the following agreed interpretations:

- Exploitation of covert channels is a form of indirect rather than direct attack. Therefore, covert channels do not have to be addressed by the strength of mechanisms analysis.

- No full covert channel analysis of the formal model is required.

The developers did not complete their covert channel analysis during the course of the project, and therefore the evaluators did not have an opportunity of validating the developer's analysis.

3.4 Comparison of TCSEC B3 with ITSEC E5/F-B3

One of the objectives of the TMach project (see section 2) was to gain a practical understanding of the differences between TCSEC B3 and the equivalent ITSEC rating, namely E5/F-B3. This section presents the results of this examination. In particular, it considers the ITSEC E5 requirements which were found not to be satisfied by existing documentation produced by the developer for the TCSEC B3 evaluation of TMach.

In a sense, this section provides a practical validation of the paper presented at the 1991 National Computer Security Conference which looked at the differences between TCSEC B3 and ITSEC E5/F5 [CONF-91]. However, it should be pointed out that [CONF-91] was based on the contents of the draft ITSEC version 1.0 rather than the definitive version 1.2 of ITSEC which is addressed here. It may be noted in particular that version 1.2 of the ITSEC contained some significant differences which the 1991 paper was not in a position take into account of, but which quickly became apparent as the TMach evaluation progressed. In particular:

- ITSEC version 1.2 provided a much clearer distinction between the correctness and effectiveness aspects of assurance. For example, version 1.0 of the ITSEC included vulnerability analysis - including covert channel analysis - as part of the correctness criteria, whereas now this activity is defined to be part of effectiveness.

- ITSEC version 1.2 introduced the term *semiformal* into the definition of the E5 architectural and detailed design requirements. In contrast, version 1.0 of the ITSEC used the phrase *some form of rigorous approach and notation* which conveys the same meaning as *semiformal*, but which is more open to interpretation; in the context of an E5/B3 comparison this phrase could be interpreted as being satisfied by the B3 documentation.

3.4.1 Requirements

As described in the preceding two sections, an essential document for the ITSEC E5 evaluation (and indeed for any ITSEC level) is the Security Target, which is required to contain details that were not found to be provided by any existing documentation such as the Philosophy of Protection. It was therefore necessary for the developer to produce a separate document containing an informal and a semiformal specification of the SEFs, together with details about the intended environment, the assumed threats, and assumptions about that environment. The Philosophy of Protection was referenced to provide additional explanatory details about the SEFs.

The formal model produced for the B3 evaluation was generally considered acceptable for ITSEC E5, but additional supporting information had to be provided to satisfy the E5 requirements in full, namely:

- example formal proofs of the model;

- an informal interpretation of the model in terms of the Security Target, showing that no SEF conflicted with the model.

3.4.2 Architectural Design

The documentation produced for the TCSEC B3 evaluation was insufficient to satisfy the ITSEC E5 requirements. This information had to be augmented as follows:

- Provision of a *semiformal* description of the architecture. Although the existing interface specifications were considered acceptable as semiformal specifications of the external interfaces of TMach, there was still a requirement to provide, using some form of restrictive notation, a specification of significant interactions between architectural design components (i.e., the kernel and the servers) in the provision of the SEFs. A separate document was produced, although it was the developer's intention to integrate this into the existing system architecture document.

- Provision of SEF traceability evidence. A separate mapping document was provided to identify which components were responsible for each SEF.

3.4.3 Detailed Design

Similar observations were made at the detailed design level. However, at the lowest (least abstract) level, the PDL specifications were considered acceptable as semiformal descriptions of the detailed design. However, some concern was expressed by the evaluators that, in tracing from the (semiformal) architectural design to the (semiformal) PDL via the (informal) intermediate representations, there could be a loss of rigour. Insufficient evidence was provided to permit the evaluators to validate this particular approach.

Late in the project, the developer switched from PDL to another style of specification, with the intention of making the design (and in particular the interrelationships between different modules) easier to understand. This was also considered acceptable as a semiformal notation.

As with the architectural design level, the developer had to provide additional documentation to provide evidence of how the SEFs were traced to the detailed design levels. The developer's intention was to further refine the component mapping documents by including mapping onto subsystems and modules.

3.4.4 Implementation

At this level of representation (source code, hardware drawings and test documentation) the most significant difference was in the area of test coverage. ITSEC E5 requires an explanation of the correspondence between the tests and the SEFs, security relevant functions at the detailed design level, and security mechanisms at the implementation level, with a rationale for the coverage achieved. The developer undertook to provide this additional evidence, but the existing approach of testing at the TCB interface, supplemented by documented code reviews, was accepted in principle as satisfying the ITSEC E5 requirements.

A further difference observed was that whereas at ITSEC E5 the evaluators are allowed to sample the developer's tests, sampling is not permitted at TCSEC B3.

3.4.5 Development Environment

The principal differences for this aspect of the evaluation were:

- ITSEC E5 is more stringent than TCSEC B3 in respect of configuration control requirements, in that it requires the configuration control tools to have the capability of identifying which configuration control items are security enforcing or security relevant, and also of identifying which items are affected by a change to a given item.

- ITSEC E5 required the evaluators to visit the development environment to check the application of the configuration control and security procedures.

- Additional information was required by ITSEC E5 to document the developer's security procedures, explaining how these maintained the integrity of the product.

3.4.6 Operation

The existing operational documentation for the TCSEC B3 evaluation (Security Features User Guide, Security Administrator's Guide, and associated manuals) were considered acceptable as the basis for satisfying the ITSEC E5 User Documentation and Administrator Documentation requirements.

With regard to the ITSEC E5 Operational Environment requirements, the major difference was in the additional requirement (as compared with TCSEC B3) to document the product delivery procedures, demonstrating how the integrity of the product was maintained whilst in transit between the development and the environment in which it is to be installed, configured and used. The developer undertook to provide this additional evidence, although they did not do so during the course of the TMach project.

3.4.7 Effectiveness

The whole area of effectiveness represents a significant difference between ITSEC E5 and TCSEC B3, since TCSEC B3 does not require the developer to provide a set of effectiveness analyses as required by ITSEC. There are two basic reasons for this difference:

- TCSEC B3 is presented as a 'given' solution to a particular security problem. Although there is clearly an underlying rationale as to why this solution is appropriate, this is not made explicit by the TCSEC (at least in terms that can be mapped onto the ITSEC effectiveness analyses). By contrast, the ITSEC allows the sponsor the flexibility of specifying the security functionality to be evaluated, but a consequence of this is that the sponsor must demonstrate there is an *effective* solution to the security problem as defined by the Security Target.

- ITSEC E5 places a greater burden of evidence on the developer than TCSEC B3[5]. Much of the work done by the developer in generating the effectiveness analyses is work that would be done by the evaluators in a TCSEC B3 evaluation. Therefore, although at the end of the evaluation processes similar work has been carried out, the division of work between developer and evaluator is different in the two cases.

---

[5] However, it does not necessarily follow from this that the ITSEC evaluation process is more burdensome for a developer. In fact, the TMach developer observed that a positive feature of the ITSEC was that it identifies in advance the materials that are required. By contrast, the TCSEC imposes requirements as the evaluation proceeds; this is a problem for the developer, who is thus unable to anticipate or plan what will be needed.

The developer produced, or undertook to produce, additional documents to satisfy the ITSEC requirements for the six effectiveness analyses. However, it was recognised that the developer's covert channel analysis would play a major role in satisfying the Construction Vulnerability Assessment requirements. Furthermore, it was not clear whether TMach would have any known vulnerabilities in its operation, and hence whether a separate Operational Vulnerability Assessment would be required.

The developer produced at least one version of the remaining four effectiveness analyses for evaluation. Their relationship to the TCSEC B3 requirements is discussed below.

Suitability Analysis

ITSEC requires an analysis that shows that the SEFs in the Security Target are suitable to counter the threats, this being necessary because of the flexibility ITSEC allows in the specification of security functionality in a Security Target. Where the Security Target is based on a standard set of functionality such as F-B3, there should be associated with this a standard set of threats the functionality is designed to counter, and hence a standard suitability analysis. Neither the ITSEC version of F-B3, nor TCSEC B3, includes such information (see the discussion above), and hence it was necessary for the developer to derive the suitability analysis from the threats and SEFs in the Security Target. The effort required of the developer could have been significantly lessened had ITSEC F-B3 provided this information (this is indeed the approach taken in the UK Scheme's version of F-B3 in the draft Scheme Information Notice (SIN) 067).

Binding Analysis

ITSEC requires the provision of a binding analysis which addresses all interrelationships or dependencies between SEFs and mechanisms. Some of these dependencies are apparent at the level of the Security Target. It therefore follows that for a standard set of functionality such as F-B3 there will be a common set of SEF-SEF dependencies and associated analysis. However, ITSEC also requires consideration of interrelationships between mechanisms, and ITSEM expects the analysis to be largely based on the architectural design, which will identify dependencies that are not apparent at the level of the Security Target.

A separate analysis was therefore required. The evaluators observed that the Philosophy of Protection contained much information that was of relevance to the binding analysis, but what was needed was a comprehensive analysis covering all SEFs and mechanisms, and the interrelationships between them.

At ITSEC E5, there is significant evaluator effort required to validate the developer's binding analysis by in particular examining whether there are dependencies between SEFs and mechanisms not considered by the developer, and whether these give rise to potential vulnerabilities. (This work may be performed as the evaluator's validation of the binding analysis or as part of the evaluator's independent vulnerability analysis.) Particular interest

will be directed at the detailed design and source code. By performing this analysis, the evaluators focus on the weaker areas of the TOE and target their penetration testing accordingly. This contrasts with TCSEC B3 where the evaluators focus more on penetration testing and less on analysis.

Strength of Mechanisms Analysis

TCSEC B3 does not have a similar concept to strength of mechanisms as defined in the ITSEC. It was therefore necessary for the developer to produce a separate analysis which (as with most products and systems evaluated against ITSEC) addressed the strength of the password mechanism, the only mechanism breakable by direct attack.

Again, as with the binding analysis, significant work is performed here by the evaluators in validating the developer's analysis, and in identifying and performing penetration tests to confirm or disprove the developer's analysis.

Ease of Use Analysis

TCSEC B3 does not have any analysis analogous to the ITSEC ease of use analysis. It was therefore necessary for the developer to provide an additional document to contain the required information.

3.5 Impact on Criteria and Methodology Development

3.5.1 Impact on ITSEC and Associated Methodology and Interpretations

The TMach Project adopted the draft versions of ITSEM at an early stage to validate their usability. The TMach Project established links with the ITSEM Working Group during 1992, and was therefore able to influence its development. UK and German evaluators presented at the ITSEM Workshop held in Brussels, September 1992, drawing at least in part on their experience from the TMach evaluation.

When the draft versions of ITSEM were used in practice, it soon became clear that there was a need for the ITSEM to clearly distinguish between those parts of the document that were intended to be prescriptive, and those that were intended to be descriptive. This recommendation was implemented in ITSEM version 1.0 which (in Part 4) highlights the mandatory requirements on evaluators.

The most obvious influence of the TMach Project on the development of the ITSEM was in the new area of effectiveness. Much of the content of ITSEM annex 6.C, which provides guidance on the interpretation of the effectiveness requirements, was directly influenced by the TMach evaluation. In particular, the recognition that with respect to strength of mechanisms there are two types of mechanism [ITSEM 6.C.2-6.C.8]:

- those that are breakable by direct attack and have an associated strength (*Type A*);

- those that are unbreakable by direct attack if perfectly conceived and implemented (*Type B*).

The example given in [ITSEM 6.C.9-6.C.11], illustrating how this categorisation (and the strength analysis) is independent of how the developer chooses to identify the mechanisms involved, came directly from the TMach evaluation, representing an agreed UK-German interpretation.

Many of the significant interpretations were, however, reached after ITSEM was issued as definitive in September 1993. These have, nonetheless, been reflected in UK Scheme documentation, as follows:

- The TMach evaluation provided an early contribution to the understanding of ITSEC evaluations in the UK by contributing two case studies to UKSP 05 Part IV (Evaluation Case Studies). These concerned the evaluation of a security target at ITSEC E5, and the evaluation of the architectural and detailed design at E5.

- The interpretations with respect to application of the ITSEC requirements for semiformal architectural and detailed design documentation were recorded in a UK SIN.

- The UK Evaluation Manual, UKSP 05 Part III, (which supplements the ITSEM in the UK) now contains the agreed interpretations relating to:

    - development methodologies ('waterfall' versus 'spiral')

    - the transitivity of tracing of SEFs

    - test coverage requirements

    - developer's security (TOE integrity being the key issue)

    - effectiveness and the application of ITSEC Figure 4.

3.5.2 Impact on Federal Criteria

The findings from the TMach Project were also fed into the development of the Federal Criteria by NIST and the NSA. The importance of the security target concept was accepted. The concept of the 'generic security target' which was floated during the early stages of the project (this being in turn a logical extension of the ITSEC Functionality Class) was realised in the form of the Protection Profile concept introduced in the Federal Criteria, and carried forward into the Common Criteria.

3.5.3 Impact on Common Criteria

The TMach Project benefited from having, as UK Certifier, one who was also a member of the Common Criteria Editorial Board (CCEB). (Indeed, three of the participants and one observer in the project became CCEB members.) The interpretations of the ITSEC and ITSEM arising from the TMach evaluation have had a knock-on effect on development of the Common Criteria (CC). Two of the main influences have been as follows:

- The TMach evaluation has shown that there can be a significant amount of discussion between developers, evaluators and certifiers as to precisely what particular requirements or terms actually mean. The approach taken in the CC development to document the technical rationale behind the criteria and provide 'application notes' for the requirements is intended to avoid this problem in CC evaluations.

- The presentation of the ITSEC effectiveness criteria has led to the perception that the ITSEC requires additional documentation to provide the required set of analyses. This has proved, in many cases, to be a burden on the evaluation sponsor. By contrast, the approach taken by the CC is to retain the effectiveness criteria whilst integrating the requirements into the correctness evidence. The CC's aim has been not to require additional deliverables, but rather to get the developer to point out where in the existing documentation the requirements are addressed (which was arguably the original intent of the ITSEC).

4. CONCLUSIONS

4.1 Benefits

4.1.1 Benefits to NIST and ARPA

The following benefits have resulted from the TMach project:

1. The project has enabled NIST and ARPA to gain a detailed understanding of the whole European approach on computer security evaluation, covering:
    - The application in practice of ITSEC for a high assurance level, which has resulted in learning strengths and weaknesses of the ITSEC
    - The application of new (compared to the TCSEC) assurance concepts in ITSEC (effectiveness in particular) in a high assurance evaluation
    - The study of the evaluation method as described in the ITSEM
    - Support of understanding the new concepts of
        - separation of functionality and assurance
        - traceability
        - security target.
    - Understanding of the two most advanced European evaluation schemes (UK, Germany)
    - Learning about the procedures taken for criteria interpretations
    - Gaining an insight into the commercial evaluation process and the issues involved.
2. The project has supported of the development of:
    - Common Criteria, by feeding the experiences made within the TMach project back into the CCEB
    - TTAP, by gaining experience in the work of European ITSEFs.

4.1.2 Benefits to National Certification Bodies

The following benefits have resulted from the TMach Project:

1. The project has provided a deeper understanding of the ITSEC E5 requirements in relation to:

    - their application in a real evaluation
    - differences between ITSEC and TCSEC.

2. The project has made valuable contributions to the development of the evaluation criteria and methodology.

3. The project has supported mutual recognition between the UK and Germany by allowing both certification bodies to have visibility of evaluation results in the other country.

4.2 Problems Identified

A number of problems of interpretation and application of specific requirements have been noted, and these are described (with their agreed resolution) in section 3. However, two key problems are worthy of mention here.

1. A set of evaluation criteria does not, on its own, constitute a suitable basis for a smooth evaluation. This problem is magnified in the case of ITSEC, where the authors were drawn from countries speaking four different languages. It is necessary for the criteria to have an accompanying explanation of what the requirements mean, and what their intent is. Otherwise, there is a significant risk of developers, evaluators and certifiers wasting considerable time discussing the meaning of particular terms and requirements.

2. From the perspective of a commercial evaluation, it is not sensible to attempt to perform an evaluation concurrently with a rapid prototype development. Had the principal goal of this project been to perform a complete evaluation of TMach, then a different approach would have been adopted. A more fruitful and cost-effective option (where successful evaluation was the principal project goal) would have been to provide pre-evaluation consultancy to the developer, and progress to formal evaluation only when the product and its documentation were stable. (Note that the evaluators adopted the approach they did in order to provide visibility of the process.)

4.3 Recommendations for Common Criteria Development

Many of the lessons learnt from the TMach Project are of direct relevance to the development of the Common Criteria (CC) and the Common Evaluation Methodology.

Those involved in the development of these documents should take particular note of the following interpretations (as described in section 3 of this report):

1. The interpretations relating to the content of the Security Target (e.g. specification of SEFs, handling of covert channels) are of direct relevance to application of the CC Security Target assurance requirements (class ASE).

2. The interpretations concerning the content and scope of the formal security policy model are of relevance to the CC Functional Specification requirements defined by the components ADV_FSP.3 to ADV_FSP.6 (which feature at EAL5 to EAL7).

3. The interpretations relating to the use of semiformal notations in the design representations are of direct relevance to CC Development assurance requirements (class ADV), and specifically the components ADV_FSP.3 to ADV_FSP.5, ADV_HLD.3 to ADV_HLD.4, ADV_LLD.2 and ADV_RCR.2 (which feature at EAL5 to EAL7).

4. The interpretations relating to demonstrating test coverage at the detailed design and implementation levels are of direct relevance to CC Tests assurance requirements (class ATE), and specifically the components ATE_DPT.3 and ATE_DPT.4 (which feature at EAL5 to EAL7).

5. The interpretations relating to developer's security are relevant to the Development Security (ALC_DVS) requirements.

6. The interpretations relating to strength of mechanisms are of direct relevance to the Strength of Function (AVA_SOF) requirements.