



Australasian Certification Authority

AISEP Interpretation

AI No.	001
Author	Richard Helliwell
Issue Date	21 July 2005
Status	FINAL
Version	1.0
Summary	This AISEP Interpretation provides general guidance on semi-formal and formal styles and how they should be evaluated with EAL 5 – 7 methodologies.
Reference	EAL 5 – 7 Methodology.

Interpretation

This AISEP Interpretation provides general guidance on the specification of semi-formal and formal styles. This is particularly relevant to the application of the EAL 5 to EAL 7 criteria, where the requirements for semi-formal and formal styles in vendor and evaluator documentation are increased.

The levels of formality can be briefly described by:

- Informal Style: semantics defined by natural language
- Semi-formal Style: defined semantics with restricted syntax forms to well-defined expressions, which have a precise meaning.
- Formal Style: defined semantics, syntax and rules of inference based upon well-defined mathematical concepts.

Each style is considered to be hierarchical in nature. Thus a semiformal specification will meet the requirements for an informal style. Similarly, a formal specification will meet the requirements for an informal or semi-formal style.

It is an implicit requirement that where semiformal or formal style is required, that semiformal or formal methods are used to examine the content.

Semiformal Specification

A semiformal specification requires the use of a notation that is explicitly defined. It may be based on a restricted subset of the natural language, such as expressions used in a technical community. Alternatively, it may be based on accepted methodologies or diagrams, eg data flow diagrams, state transition diagrams or flow charts.

The advantage in using a semiformal style is that it reduces ambiguity of specifications, and strengthens the method of analysis.

An evaluator should examine the semiformal style to ensure that:

- The syntax rules are explicitly defined or referenced.
- The syntax rules are capable of expressing the desired security functions. Note however, that a single semi-formal notation may not be able to describe all required characteristics. It is acceptable to use a combination of notations to describe the security functions.
- The notation(s) used are in accordance with the syntax rules specified.
- It is supported by informal narrative descriptions where necessary.

Formal Specification

A formal specification is expressed within a formal system based upon well-established mathematical concepts. These mathematical concepts are used to define well-defined semantics, syntax and rules of inference.

There are two immediate benefits of using formal methods in any development process:

1. increased understanding of the system, at an early enough stage that inadequacies can be corrected cost-effectively.
2. assurance that any critical properties which have been stated and proved can be trusted.

The evaluator should examine the formal style to ensure:

- the notation is a recognised standard, or otherwise academically acceptable.
- the formal notations are supported by well defined syntax and semantic rules, with both being themselves expressed in formal notations.
- the syntactic and semantic rules define how to recognise constructs unambiguously and determine their meaning.
- that it is capable of expressing the security functionality or policies required.
- all formal arguments are correct and consistent with the formal notation syntactic and semantic rules.

- all formal arguments are supported by informal explanatory text

Formal Verification

Verification may be performed on specifications to prove that certain properties hold. The two main approaches to verification are model checking and theorem proving.

- **Model Checking:** A model is an abstraction of a system that simulates the system's behaviour whilst aiming to achieve certain requirements (often temporal) identified by a specification. Given such a model, model checking involves an exhaustive search for every possible trace of operations in order to examine whether the specified requirements always hold.

An exhaustive search is only possible if the state space is finite, otherwise the search would theoretically go on forever – in practice, model checkers run out of space and crash. Furthermore, for large finite models the checker may not have enough memory to complete the analysis or could take considerable processing time. These issues are caused by what is known as the *state explosion* problem.

- Theorem proving approach is popular due to its ability to reason with large and even infinite state spaces, as it does not suffer from the state explosion problem. Instead of analysing every possible trace of operations within a system model, a theorem prover conducts verification through inductive reasoning of the system's specification.

Model checking tools pose an issue when meeting the reporting requirements in Common Criteria evaluations. In general, model checking tools are unable to produce a formal proof that can be checked externally. That is, if a model satisfies its specification, then only a positive result will be returned. If it does not meet its specification, a counter example is usually presented, providing more information of how the specification fails.

To use a model checking tool evaluators need to have a level of confidence in the tool's implementation and ability to produce correct results. Two methods in which this may be achieved include:

- separate evaluation of the tool;
- performing checks against known weakened variants of models. However, as it is unlikely that every weakened variation will be able to be examined, it is necessary to describe how the subset of variations was selected.

The formal proof generated by theorem proving will meet the Common Criteria reporting requirements provided that it meets the requirements described for formal styles above. It is acceptable for the evaluators to follow a script provided by the vendor to assist in the verification.

Certifier Assurance Meetings (CAMs)

CAMs are held periodically throughout an evaluation to discuss technical aspects relating to the conduct of evaluation activities for a specific task. Given the meeting timeframes, it is not possible to verify formal evaluation proofs during these meetings. The expectation is that CAMs will be used to discuss the above aspects, together with an informal discussion of the proof and results. The actual examination of evaluation proofs by the ACA will be conducted outside the CAM process.